COPYRIGHT AND CITATION CONSIDERATIONS FOR THIS THESIS/ DISSERTATION

o Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

o NonCommercial — You may not use the material for commercial purposes.

o ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

How to cite this thesis
TrustCV: Supporting reputation-based trust for collectivist digital business ecosystems

by

Donovan Anthony Isherwood

Dissertation submitted in fulfilment of the requirements for the degree

Magister Scientiae in the subject of Information Technology

in the Faculty of Science at the University of Johannesburg

Supervisor Professor Marijke Coetzee

December 2013
Declaration

I, Donovan Anthony Isherwood, hereby declare that:

- The work in this dissertation is my own work;
- All sources used and referred to have been documented and recognised;
- This document has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institution.

Donovan Anthony Isherwood
Acknowledgements

I would like to acknowledge the support and encouragement I have received throughout my academic career. I would like to thank my supervisor Prof. Marijke Coetzee for her continued support and guidance. Her drive for excellence and perfection ensured I always did my best and delivered to the best of my abilities. This dissertation would not be possible without her motivation and belief in me.

I would like to thank SAP Research Pretoria and everyone involved for their experience, assistance, and the opportunities they created for me. I would like to thank the University of Johannesburg and the National Research Foundation (NRF) for their financial support for the duration of my research.

I owe many thanks to my family and friends who always supported me and believed in me. To my parents, whose constant belief in my ability has made me achieve many things which I never thought possible. A special thank you to my girlfriend, Ekaterina for her support when times were tough and my motivation was low.

Last, but not least, I would like to thank God for everything.

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the NRF.
Abstract

In Africa, the economy is largely dominated by SMMEs that represent 90% of private businesses and contribute to more than 50% of employment and GDP. However, these SMMEs struggle to sustain their businesses in the current economic climate. To address this, advancements in mobile and cloud technology introduce new possibilities such as digital business ecosystems to support environment where small, micro, and medium enterprises can interoperate. The fundamental challenge for SMMEs in a digital business ecosystem is the selection of transaction partners. SMMEs are interested to transact with other SMMEs that will benefit their business through successful transactions. This leads to the sustainability and growth of SMMEs and consequently the economy. However, not all SMMEs behave as predicted and therefore, being able to trust another SMME in the digital business ecosystem is important.

Trust is an essential part of business and personal life. The social nature of trust makes trust very personalised and for each individual, trust is interpreted, understood and perceived according to past experience and social behaviour. These factors are largely influenced by cultural norms and behaviours that individuals conform to. In African and some other regions, collectivist cultural norms and behaviours are common whereas in Westernised regions, individualist cultures are common. Therefore, it is not enough to just consider trust from a technical perspective but also from a cultural perspective. For small businesses in Africa and other regions in the world, this is especially true. Compared to larger companies in developed economies, SMMEs in Africa are more informal and operate in a more personal manner. This implies that trust decisions are largely influence an owner or employee’s cultural norms and behaviour.

The research conducted in this dissertation proposes a trust model, known as Trust\textsubscript{cv} that supports the cultural norms and behaviours of collectivist cultures for trust in a digital business ecosystem. Digital business ecosystems, trust, culture and social network analysis provide the literature foundation for Trust\textsubscript{cv}. The effectiveness of Trust\textsubscript{cv} is measured through simulations of a digital business ecosystem in Africa, which provides interesting results compared to an existing trust model. The results indicate that Trust\textsubscript{cv} could be used to support trust in collectivist digital business ecosystems used by collectivist cultural SMMEs.
Table of Contents

Table of Contents .................................................................................................................. 5
List of Figures ....................................................................................................................... 12
List of Tables .......................................................................................................................... 14

PART I

Chapter 1: Introduction

1.1 Introduction ..................................................................................................................... 16
1.2 Description of problem area ......................................................................................... 18
1.3 Motivation ....................................................................................................................... 18
1.4 Problem statement .......................................................................................................... 18
  1.4.1 Research objectives ................................................................................................. 18
  1.4.2 Research questions ................................................................................................. 19
1.5 Important terms ............................................................................................................. 21
1.6 Research methodology ................................................................................................. 22
1.7 Layout ........................................................................................................................... 23
1.8 Conclusion ...................................................................................................................... 25

Chapter 2: Digital business ecosystem for Africa

2.1 Introduction ..................................................................................................................... 27
2.2 The digital business ecosystem (DBE) ......................................................................... 28
2.3 Network architecture of a digital business ecosystem .................................................. 29
  2.3.1 Properties of a digital business ecosystem ............................................................. 30
  2.3.2 Peer-to-peer architecture for the digital business ecosystem ................................. 32
2.4 The state of small businesses and ICT in Africa ......................................................... 35
Chapter 3: Trust and reputation for digital business ecosystems

3.1 Introduction ........................................................................................................... 46
3.2 Trust ..................................................................................................................... 47
  3.2.1 Properties of trust .......................................................................................... 49
  3.2.2 Constructs of trust .......................................................................................... 50
3.3 Reputation ............................................................................................................ 53
3.4 Trust and reputation computation for the digital business ecosystem .............. 55
  3.4.1 Trust and reputation metrics .......................................................................... 56
  3.4.2 Scope of trust and reputation metrics ............................................................. 57
  3.4.3 Architectures for trust and reputation computation ......................................... 59
  3.4.4 Approaches to trust computation .................................................................... 61
3.5 A comparison of relevant trust and reputation systems ...................................... 63
  3.5.1 Trust and reputation systems ......................................................................... 63
  3.5.2 Evaluation criteria for trust and reputations systems for the digital business ecosystem ........................................................................................................... 64
  3.5.3 A comparison of trust and reputation systems for the digital business ecosystem 66
  3.5.4 A trust and reputation system for the digital business ecosystem for Africa ... 73
3.6 PeerTrust system for the digital business ecosystem ............................................ 74
  3.6.1 PeerTrust system ........................................................................................... 74
  3.6.2 PeerTrust algorithm ....................................................................................... 77
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.6.3</td>
<td>Trust and reputation for the digital business ecosystem</td>
<td>78</td>
</tr>
<tr>
<td>3.7</td>
<td>Conclusion</td>
<td>79</td>
</tr>
</tbody>
</table>

**Chapter 4: The influence of culture on trust and reputation**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>81</td>
</tr>
<tr>
<td>4.2</td>
<td>Culture</td>
<td>82</td>
</tr>
<tr>
<td>4.3</td>
<td>Individualist vs. Collectivist cultures</td>
<td>84</td>
</tr>
<tr>
<td>4.4</td>
<td>Cultural influence on trust</td>
<td>85</td>
</tr>
<tr>
<td>4.4.1</td>
<td>Use case for trust in individualist cultures</td>
<td>86</td>
</tr>
<tr>
<td>4.4.2</td>
<td>Use case for trust in collectivist cultures</td>
<td>88</td>
</tr>
<tr>
<td>4.4.3</td>
<td>Culture and it’s relation to trust</td>
<td>90</td>
</tr>
<tr>
<td>4.5</td>
<td>Collectivist cultures and their trusting behaviour</td>
<td>92</td>
</tr>
<tr>
<td>4.5.1</td>
<td>Trust grows as group harmony increases.</td>
<td>93</td>
</tr>
<tr>
<td>4.5.2</td>
<td>Recommendations from in-group members are trusted more.</td>
<td>94</td>
</tr>
<tr>
<td>4.5.3</td>
<td>Trust grows with an increase in social position</td>
<td>94</td>
</tr>
<tr>
<td>4.5.4</td>
<td>Trust in outsiders is formed by recommendations from in-group members</td>
<td>95</td>
</tr>
<tr>
<td>4.6</td>
<td>Trust and reputation properties for the digital business ecosystem</td>
<td>96</td>
</tr>
<tr>
<td>4.6.1</td>
<td>Trust and reputation properties for collectivist cultures</td>
<td>96</td>
</tr>
<tr>
<td>4.6.2</td>
<td>Summary of trust properties for collectivist digital business ecosystems</td>
<td>98</td>
</tr>
<tr>
<td>4.7</td>
<td>Collectivist digital business ecosystem</td>
<td>100</td>
</tr>
<tr>
<td>4.8</td>
<td>Conclusion</td>
<td>100</td>
</tr>
</tbody>
</table>

**Chapter 5: Social network analysis for collectivist digital business ecosystem trust and reputation**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>102</td>
</tr>
<tr>
<td>5.2</td>
<td>Benefits of social network analysis for the collectivist digital business ecosystem</td>
<td>103</td>
</tr>
<tr>
<td>5.3</td>
<td>Social graph of the collectivist digital business ecosystem</td>
<td>105</td>
</tr>
<tr>
<td>5.4</td>
<td>Social graph views for social network analysis</td>
<td>107</td>
</tr>
</tbody>
</table>
5.4.1 Socio-centric view ............................................................... 108
5.4.2 Ego-centric view ............................................................... 108
5.5 Social network analysis for trust and reputation .................. 110
5.6 Analysis of centrality measures for the collectivist digital business ecosystem .... 113
  5.6.1 Degree Centrality ............................................................ 113
  5.6.2 Tie Strength ..................................................................... 114
  5.6.3 Shortest Path ................................................................. 115
  5.6.4 Density ........................................................................... 116
  5.6.5 Clustering Coefficient ..................................................... 117
  5.6.6 Closeness centrality ....................................................... 119
  5.6.7 Betweenness Centrality ................................................... 120
  5.6.8 Summary of centrality measure analysis ......................... 121
5.7 Review of state-of-the-art research for trust and reputation systems supported by centrality measures .......................................................... 123
5.8 Motivation of centrality measures for trust and reputation for the collectivist digital business ecosystem ............................................................. 125
  5.8.1 Centrality measures identifying groups, influential nodes, and group leaders 126
  5.8.2 Members of a group that maintain group harmony are trusted more ........... 128
  5.8.3 Members of a group trust in-group members more than out-group members 128
  5.8.4 Influential nodes such as group leaders are trusted more ............................. 129
  5.8.5 Out-group members can be trusted if they are recommended by in-group members ................................................................................. 129
  5.8.6 Summary of centrality measures for trust and reputation for the collectivist digital business ecosystem ............................................................... 130
5.9 Conclusion ............................................................................. 131
PART II

Chapter 6: Introducing Trust\textsubscript{cv} – a trust and reputation model for the collectivist digital business ecosystems

6.1 Introduction ......................................................................................................... 134
6.2 Trust\textsubscript{cv} architecture ........................................................................... 135
6.3 Trust\textsubscript{cv} components ........................................................................... 137
   6.3.1 Trust Manager ............................................................................................. 137
   6.3.2 Data Locator .............................................................................................. 138
   6.3.3 Trust Data .................................................................................................... 138
   6.3.4 Transaction Tool .......................................................................................... 138
6.4 Trust\textsubscript{cv} use-case design ...................................................................... 139
6.5 Conclusion .......................................................................................................... 141

Chapter 7: Trust\textsubscript{cv} model

7.1 Introduction ......................................................................................................... 143
7.2 Trust\textsubscript{cv} model properties ..................................................................... 144
7.3 Basic trust model constituents and operations .................................................... 144
   7.3.1 Trust environment ........................................................................................ 145
   7.3.2 Trust model constituents and operations ...................................................... 146
   7.3.3 Trust computation ........................................................................................ 150
7.4 Trust\textsubscript{cv} model social graph constituents ................................................ 151
   7.4.1 SMME’s ego-network social graph ............................................................... 151
   7.4.2 Centrality measure calculations ................................................................. 154
7.5 Trust\textsubscript{cv} model operations and algorithms ........................................... 156
   7.5.1 Use case for Trust\textsubscript{cv} ...................................................................... 157
   7.5.2 Recommendations for Trust\textsubscript{cv} ..................................................... 158
   7.5.3 Reward and punish for Trust\textsubscript{cv} ..................................................... 165
Chapter 7: Trust<sub>cv</sub>

7.5.4 The final Trust<sub>cv</sub> algorithm ................................................................. 168
7.5.5 Trust<sub>cv</sub> support for collectivist cultural trust properties ......................... 169
7.6 Conclusion ........................................................................................................... 170

Chapter 8: Trust<sub>cv</sub> Simulation and Evaluation

8.1 Introduction ......................................................................................................... 172
8.2 Simulation Environment ...................................................................................... 173
  8.2.1 NetLogo environment ................................................................................... 173
  8.2.2 NetLogo for the Trust<sub>cv</sub> and PeerTrust models ........................................... 173
8.3 NetLogo Simulations ........................................................................................... 174
  8.3.1 Simulation scenarios for evaluation .............................................................. 174
  8.3.2 Common scenario settings ........................................................................... 175
  8.3.3 Scenario evaluation metrics ........................................................................ 177
8.4 Standard PeerTrust scenario simulation and evaluation ..................................... 179
  8.4.1 Peer-to-Peer simulation environment ........................................................... 179
  8.4.2 Standard PeerTrust simulation ..................................................................... 183
  8.4.3 Standard PeerTrust simulation evaluation .................................................... 183
8.5 Collectivist culture PeerTrust scenario simulation and evaluation ....................... 187
  8.5.1 Peer-to-peer environment according to collectivist cultures ....................... 187
  8.5.2 Collectivist culture PeerTrust scenario simulation ....................................... 189
  8.5.3 Collectivist culture PeerTrust scenario evaluation ....................................... 189
8.6 Trust<sub>cv</sub> scenario simulation and evaluation ............................................. 193
  8.6.1 Collectivist digital business ecosystem simulation environment .................. 193
  8.6.2 Trust<sub>cv</sub> scenario simulation .................................................................. 197
  8.6.3 Trust<sub>cv</sub> scenario evaluation .................................................................. 199
  8.6.4 Scenario simulation summary and conclusion ............................................. 203
8.7 Conclusion ........................................................................................................... 205
Chapter 9: Conclusion

9.1 Introduction............................................................................................................... 207
9.2 Revisiting the research objective............................................................................... 208
9.3 Limitations of the research ...................................................................................... 214
  9.3.1 Limitations regarding the Trust_{cv} trust computation ....................................... 214
  9.3.2 Limitations regarding the simulation environment .............................................. 214
  9.3.3 Limitations regarding the evaluation of Trust_{cv} ................................................ 215
9.4 Further research ..................................................................................................... 215
  9.4.1 Optimising the Trust_{cv} trust computation ......................................................... 215
  9.4.2 Implementing the Trust_{cv} model in a real world scenario .................................. 215
  9.4.3 Verification of the simulation environment.......................................................... 216
  9.4.4 Collectivist digital business ecosystem implementation ..................................... 216
  9.4.5 Trust_{cv} for other regions .................................................................................. 216
9.5 Conclusion.................................................................................................................. 217

References....................................................................................................................... 219

Appendix A. Simulation Environment for PeerTrust and Trust_{cv} ................................. 228
Appendix B. Papers Presented Based on this Research .................................................... 236
List of Figures

Figure 1.1 Dissertation layout................................................................. 25
Figure 2.1 Example of a P2P architecture.................................................. 33
Figure 2.2 Digital business ecosystem P2P Overlay Network ..................... 34
Figure 2.3 Digital business ecosystem for Africa consisting of SMMEs .......... 42
Figure 3.1 Trustee, trustor and trust level scenario ..................................... 48
Figure 3.2 Constructs of trust..................................................................... 51
Figure 3.3 Determining reputation example.............................................. 54
Figure 3.4 Digital business ecosystem for Africa with communities .......... 57
Figure 3.5 Process and components of trust and reputation systems.......... 64
Figure 3.6 PeerTrust system architecture.................................................. 74
Figure 3.7 PeerTrust DataLocator with routing tables............................... 76
Figure 4.1 Adapted constructs of trust including culture ............................. 92
Figure 5.1 Social Overlay Network for the collectivist digital business ecosystem ..... 106
Figure 5.2 The collectivist digital business ecosystem social graph............ 107
Figure 5.3 Ego-centric view from SpazaShop S perspective ....................... 109
Figure 5.4 Direct trust relationship.......................................................... 111
Figure 5.5 Indirect trust relationship........................................................ 112
Figure 6.1 Trustcv architecture............................................................... 136
Figure 6.2 Trustcv UML use-case............................................................ 139
Figure 7.1 SpazaShop S Ego-network ..................................................... 152
Figure 7.2 Adjacency list representation of SpazaShop S ego-network social graph.... 153
Figure 7.3 SpazaShop A’s ego network.................................................... 157
Figure 8.1 PeerTrust NetLogo simulation environment............................. 180
Figure 8.2 Standard PeerTrust result P2P network .................................. 184
Figure 8.3 Standard PeerTrust output results........................................... 185
Figure 8.4 Collectivist culture PeerTrust result P2P network ............................................. 190
Figure 8.5 Collectivist culture PeerTrust output results ...................................................... 191
Figure 8.6 Trust_{cv} NetLogo simulation environment .......................................................... 193
Figure 8.7 Trust_{cv} result for the collectivist digital business ecosystem .............................. 200
Figure 8.8 Trust_{cv} output results ........................................................................................ 201
Figure 8.9 Average Trust Value graph for all simulation scenarios ........................................ 203
Figure 8.10 Percentage of Successful Transactions graph for all simulation scenarios ..... 204
List of Tables

Table 3.1 Trust and reputation system evaluation summary .................................................. 72
Table 4.1 Difference between individualist and collectivist culture in terms of trust ............ 91
Table 4.2 Trust properties for collectivist cultures .............................................................. 99
Table 5.1 Analysis of centrality measures for the collectivist digital business ecosystem .. 122
Table 5.2 Centrality measures to satisfy collectivist cultural behaviour .............................. 131
Table 7.1 Centrality measures calculation summary ............................................................ 156
Table 7.2 Difference between recommended values and transaction feedback ................. 166
Table 7.3 Trust satisfaction of collectivist cultural properties ............................................. 169
Table 8.1 Common scenario simulation settings ................................................................. 176
Table 8.2 Standard PeerTrust scenario simulation settings .................................................. 183
Table 8.3 Standard PeerTrust evaluation metric results ....................................................... 186
Table 8.4 Collectivist culture PeerTrust scenario simulation settings ............................... 189
Table 8.5 Collectivist culture PeerTrust evaluation metrics results ................................. 191
Table 8.6 Trust scenario simulation settings ..................................................................... 197
Table 8.7 Trust scenario collectivist cultural settings ....................................................... 198
Table 8.8 Trust evaluation metrics results ....................................................................... 201
Table 8.9 Scenario simulation summary evaluation metrics results ................................... 204
Chapter 1

Introduction

1.1 Introduction

Initiatives by the European Commission (EC, 2007) have resulted in the establishment of a digital business ecosystems (DBEs) for micro-, very small, small or medium enterprises (SMMEs). The purpose of digital business ecosystems is to support SMMEs to co-evolve in a competitive, but at the same time collaborative environment. Through this, the entire ecosystem and economy can benefit, providing SMMEs with business opportunities. In Africa, the economy is largely dominated by SMMEs that represent 90% of private businesses and contribute to more than 50% of employment and GDP (NCR, 2011). However, SMMEs in Africa, particularly very small enterprises (VSEs) struggle to sustain their businesses in the current economic climate. This is due to a low financial liquidity, making small purchases at a time, lack of credit or ability to negotiate discounts, and the transport costs associated with many small purchases (Kew and Herrington, 2009, Friedland et al., 2008). Empowering SMMEs through business opportunities, a digital business ecosystem for Africa could contribute to the economy and sustainability of SMMEs.

Advancements in mobile and cloud technology introduce new possibilities for SMMEs in Africa. Initiatives have been made to encourage SMMEs in Africa to adopt mobile and cloud technology to run their day-to-day business activities (Ngassam et al., 2011) using a digital business ecosystem. Currently, digital business ecosystems are made possible through the use of Internet technologies and peer-to-peer (P2P) architectures where SMMEs are represented by software agents (Nachira et al., 2007) capable of interacting with other SMME agents.

To support the growth of such business ecosystems and the economy, SMMEs need to be supported to collaborate with others through business transactions. The characteristics of a digital business ecosystem such as its decentralised and dynamic nature, and open environment make it challenging to support businesses through technological means. Furthermore, relationships are established, maintained, and dissolved in a digital business ecosystem. This creates additional challenges since relationships, whether personal or
business, are built upon the foundation of trust (Bachmann, 2001, Buskens, 1998, Lewis and Weigert, 1985, Mayer et al., 1995, McKnight and Chervany, 1996). Without SMMEs knowing the extent to which they can trust another SMME, they cannot be confident that another SMME will behave as predicted. Therefore a digital business ecosystem would have to support SMMEs to determine the level of trust they can place in other SMMEs.

SMMEs in Africa, particularly very small SMMEs, conduct business in an informal manner whereby business owners make personal decisions as to which SMME to transact with (DTI, 2008, Africa, 2011). The personal nature of such a decision and therefore interpretation, understanding, and perception of trust can be largely influenced by cultural norms and behaviours (Doney et al., 1998, Lane, 1997, Sia et al., 2009). Research has shown that there are real differences between the environment and cultures of Africa and the residents of developed economies in the Western world (Doney et al., 1998, Zaheer and Zaheer, 2006, Chong, 2003, Botha, 2007, Isherwood et al., 2012). For example, members of African cultures are more concerned about the reputation of their group over their individual reputation, and therefore classified as collectivist cultures (Hofstede, 1980). Additionally, cultures in Africa consider social standing as an indication of a member’s level of trust and influence over the community (Botha, 2007). Considering cultural differences, and the nature of a digital business ecosystem, a digital business ecosystem for Africa would require a trust model capable of facilitating trust in a decentralised peer-to-peer environment for collectivist cultures.

The goal of this research is to propose a trust model for collectivist cultures that can support trust in a digital business ecosystem for Africa. To achieve this, the challenges previously mentioned need to be addressed. Therefore, the research attempts to gain an understanding of a digital business ecosystem and how such a digital ecosystem can be used in Africa, based on the behaviour of SMMEs in Africa. A comprehensive study of trust in computer science and a comparison of selected existing trust models are conducted in this research. Understanding the cultural differences between the collectivist cultures, particularly in Africa, and other cultures, and how they approach trust is required. The research identifies trust properties for collectivist cultures which are explored further and satisfied through the use of social network analysis. The final result of this research is the proposal and evaluation of the Trust\textsubscript{cv} model. The Trust\textsubscript{cv} architecture and model is proposed and simulated in a digital business ecosystem for Africa environment to demonstrate its effectiveness.
1.2 Description of problem area

Digital business ecosystems have properties that need to be addressed by its technical implementation. A peer-to-peer architecture is capable of satisfying many of the properties of a digital business ecosystem. However, this implies that a peer-to-peer trust model is required to support trust and reputation in the digital business ecosystem. Trust is essential where SMMEs need to decide whether to select a transaction partner or not. The selection of an unreliable transaction partner can have a detrimental effect on a business, particularly if money and reputation are at stake. Therefore, it is imperative to make use of trust to assist SMMEs to select transaction partners so that successful transactions can be concluded. As the digital business ecosystem is used by people in a specific African cultural environment, the subjective and social nature of trust requires that the collectivist cultural norms and behaviour are taken into account by a trust model.

1.3 Motivation

The prevalence of mobile and cloud technology in Africa makes the implementation of a digital business ecosystem for Africa a real possibility. This can have a beneficial impact on the economy of Africa as SMMEs are exposed to more business opportunities. For a digital business ecosystem for Africa to be successful, SMMEs need to conclude business transactions successfully, supported by a digital business ecosystem. The implementation of an appropriate trust model can significantly contribute towards this success, by enabling SMMEs to select better transaction partners.

1.4 Problem statement

A number of trust models exist that support a peer-to-peer architecture, making it useful for a digital business ecosystem. However, there are no trust models that specifically support the collectivist cultural behaviour of African cultures, in conjunction with P2P architectures. By defining such a trust model, a contribution can be made towards the success of a digital business ecosystem for Africa. Given the problem statement, this section further introduces the objectives and research questions.

1.4.1 Research objectives

The primary objective of this research is to propose a trust model for collectivist cultures that can support trust in a digital business ecosystem for Africa. The focus of this research is to
provide background on digital business ecosystems, trust and reputation, the role of culture in
trust and particularly the collectivist African cultural approach to trust.

1.4.2 Research questions

This research aims at addressing the following specific research questions:

1. **How can SMMEs be supported by technology to grow their business?**

In order to address this research question, an understanding of digital business ecosystems
is required. The current state and behaviour of SMMEs in Africa needs to be considered to
determine how digital business ecosystems and related technology can be applied to support
SMMEs. To address this research question in more detail, the following secondary research
questions are defined:

   a) What is the state of SMMEs in Africa and how do they conduct business?
   b) What are the properties of a digital business ecosystem?

2. **How can trust be supported by a collectivist digital business ecosystem?**

For a digital business ecosystem to grow, trust between participants needs to be supported to
ensure that SMMEs make informed decisions when a transaction partner is selected. In order
to understand the role of trust in a collectivist digital business ecosystem, the following
secondary research questions are defined:

   a) What are the constructs and properties of trust?
   b) Which existing trust models are appropriate to be used by a collectivist digital business
      ecosystem?

3. **How does cultural behaviour influences trust in a collectivist digital business
   ecosystem?**

Cultural norms and behaviour can influence the formation, understanding, and interpretation
of trust. Therefore, the specific cultural behaviour for SMMEs in Africa needs to be identified
and understood. This leads to the following secondary research questions:

   a) What is the dominant culture in Africa and how does it differ from other cultures?
   b) Which specific norms and behaviour of this culture influences the formation of trust?
c) Can a set of trust properties be identified to support trust in a collectivist digital business ecosystem?

4. How can identified trust properties be implemented in a collectivist digital business ecosystem?

This research question follows directly from the previously stated one. Even though the identifications of trust properties can be done, it only becomes viable if a technical solution can be found for its implementation. In order to address this, the researcher investigates the role of social network analysis, which leads to the following secondary research questions:

a) What are the benefits of using social network analysis when implementing trust?
b) How can social network analysis be applied in a collectivist digital business ecosystem?
c) Which social network analysis measures influence trust?
d) What is the state-of-the-art when social network analysis measures are applied to trust models?
e) How can social network analysis measures be used to implement the identified trust properties?

5. How can trust be incorporated by a collectivist digital business ecosystem?

In current digital business ecosystems, trust is implemented according to the cultural norms and behaviours of individualistic cultural groups. To support the growth of a collectivist digital business ecosystem, participants need to feel comfortable with the manner in which trust is supported. In order to achieve this, the identified trust properties need to be implemented. Therefore, the following secondary research questions are proposed:

a) What are the architectural components of such a trust model?
b) How are the identified trust properties modelled and implemented using social network analysis?

6. Does the trust model proposed by this research in fact support collectivist behaviour?

In order to determine this, the proposed trust model needs to be evaluated. The use of multi-agent computer simulation techniques is useful to evaluate complex behaviour where real-
world experiments are difficult. Therefore, the following secondary research questions are defined:

a) Which multi-agent simulation tool can be used to simulate the use of trust in the collectivist digital business ecosystem?

b) What simulation scenarios and evaluation criteria can be used to assess the effectiveness of the proposed trust model?

c) To what extent does the proposed trust model meet identified evaluation criteria and which deficiencies can be identified?

The proposed research questions define the direction of the research conducted in this dissertation. The most important contribution of the research is the defining of a trust model for collectivist cultures and subsequently the digital business ecosystem for Africa.

1.5 Important terms

In order to avoid any misunderstanding, it is important to correctly interpret the terminology used in this dissertation. The researcher now provides a brief definition of what is meant by the terms SMME, digital business ecosystem, trust, and culture.

a) SMME
A micro-, very small, small or medium enterprise (SMME) is a separate and distinct business entity such as small shops; suppliers; construction companies; artisans; accountants; marketing businesses; hair salons; beauty salons; dentists; doctors; other cooperative enterprises and non-governmental organisations (DTI, 2008). SMMEs are managed by one owner or more. Such an entity can be categorised as micro-, very small, small or medium enterprises.

b) VSE
A very small enterprise (VSE) is simply a specific subset of SMMEs that make up a large portion of the economy (DTI, 2008). The definition of VSE follows the definition of SMME but implies further constraints than larger SMMEs such as size, informal operation and cultural adaptation that need to be further considered.
c) Digital business ecosystem

A digital business ecosystem (DBE) is a specific type of digital ecosystem designed to support SMMEs, where SMMEs transact with each other SMMEs in a competitive yet collaborative environment (EC, 2007, Lurgi and Estanyol, 2010). The digital business ecosystem aims to facilitate the growth of SMME members so as to enhance the market value of the entire digital business ecosystem and its members. This is achieved through a digital means whereby SMMEs are represented and supported by software agents.

d) Trust

Trust is the extent to which one entity, in the form of an agent or business or both, is willing to enter into a transaction with another entity in the digital business ecosystem, with the acceptance of being vulnerable to the actions of the other entity, whether negative or positive, without being in control of the other entity’s actions (Mayer et al., 1995, McKnight and Chervany, 1996).

e) Culture

Culture is the collective programming of the mind that distinguishes the members of one group or category of people from another (Hofstede, 1980). This is the collective norms and behaviours that categorise a group of people and in particular, for this research, influence the constructs of trust.

1.6 Research methodology

The research conducted in the dissertation begins with the formulation of a problem statement and research questions to justify the purpose of the dissertation. The proposed research makes use of a strategy discussed in Olivier (2009), with the aim of developing a model. This strategy consists of a detailed investigation of the literature, followed by a critical analysis and review, to motivate the proposed model based on the findings in the literature. A literature review is conducted in the fields of digital business ecosystems, trust and reputation, culture and trust, and social network analysis. The literature review determines the current state-of-the-art and gains insight into existing methods, techniques, and approaches which have previously been proposed to address the problem statement. The research questions are addressed throughout this process and the development of the model and architecture of the system. A formal model is proposed by the author to address the problem statement. The formal model makes use of techniques and knowledge that was identified in the literature study (Ramesh et al., 2004). A multi-agent simulation of the proposed model is finally performed and used to further validate the model (Olivier, 2009). Experiments determine the
performance of the proposed trust model against an existing model using evaluation criteria identified in the literature review and analysis. Multi-agent simulation is a useful methodology to estimate the performance of complex social interactions, as it offers the possibility to investigate the trust model outside of the experimental domain.

The next section describes the layout of the dissertation and is derived from the methodology used.

1.7 Layout

This dissertation consists of two parts with both Part I and Part II consisting of several chapters. Figure 1.1 depicts the layout of this dissertation. Part I provides a background and literature overview to the reader, which is essential to the formulation of the model. Important concepts are developed in this section and provide a foundation for the model that is finally presented. The current chapter, Chapter 1, presents the research topic and provides background information to define the problem.

Chapter 2 provides comprehensive background on the digital business ecosystem and SMMEs in Africa. The definition and properties of a digital business ecosystem identify the architecture of a digital business ecosystem which needs to be considered when implementing a trust model in the digital business ecosystem. The properties of a digital business ecosystem for Africa are defined based on the characteristics and behaviour of SMMEs, particularly very small enterprises (VSEs) in Africa. These properties, together with the digital business ecosystem properties, direct the research in the following chapters.

Chapter 3 provides an extensive study on trust in computer science. The properties, constructs, and computations of trust are discussed. An analysis is performed on existing trust models to determine an appropriate trust model which can be extended for the digital business ecosystem for Africa. The evaluation of the trust models is based on the research conducted in the chapter and the properties identified in Chapter 2.

Chapter 4 studies the influence of culture on trust. This chapter identifies two types of cultures which have different approaches towards trust. A case study is provided which specifically describes the behaviour of collectivist cultures in Africa, leading to the proposal of four trust properties for collectivist cultures. These properties introduce the next chapter which identifies an approach to supporting these properties.
Chapter 5 introduces social network analysis as a means of supporting the trust properties for collectivist cultures. An extensive analysis is performed on social network analysis measures that can be used in the digital business ecosystem for Africa. Three measures are then proposed for implementation in the trust model for the digital business ecosystem for Africa. This chapter concludes the background research of this study.

Part II of this dissertation sets out to develop a trust model for collectivist cultures and evaluates this model through simulations.

Chapter 6 introduces the Trust\textsubscript{cv} model and proposes the architecture for this trust model based on an existing trust model known as PeerTrust.

Chapter 7 presents the contribution of this study. The chapter formally defines and models the Trust\textsubscript{cv} model. Detailed definitions and algorithms are defined as the Trust\textsubscript{cv} model attempts to address trust properties for collectivist cultures based on the research conducted in this study.

Chapter 8 evaluates the effectiveness of the Trust\textsubscript{cv} model. Simulations of the Trust\textsubscript{cv} and PeerTrust model are performed according to scenarios defined for each model. The results of the simulations are evaluated according to their support for trust in a digital business ecosystem-like environment. These models are compared against each other to determine if the Trust\textsubscript{cv} model can be considered as a trust model for the digital business ecosystem for Africa through its support of collectivist cultures.

Chapter 9 revisits the research questions and ensures that the research does meet the objectives it set out to achieve. The dissertation is summarised, key aspects are highlighted, and the final conclusions with further research possibilities are provided.

Appendix A provides extra information relating to the PeerTrust and Trust\textsubscript{cv} simulation environments.

Appendix B gives the papers presented at conferences which are based on the research conducted in this study.
1.8 Conclusion

The introduction chapter provides background information, defines the purpose and motivation for the study and sets the tone for the chapters that follow. The key concepts are introduced and the remainder of the dissertation is organised and discussed.

The digital business ecosystem for Africa can be beneficial for SMMEs in Africa and consequently the economy of Africa. However, trust needs to be facilitated in this environment for SMMEs to conduct successful business transactions. Identifying trustworthy and reliable members in a digital business ecosystem is not without its challenges thanks to the nature of digital business ecosystems. In Africa there are cultural differences, compared to other regions
that can influence trust in the digital business ecosystem for Africa. Therefore, this study proposes a trust model, suitable for the digital business ecosystem for Africa through support of collectivist cultures in Africa.

The chapters that follow all contribute towards the development of a trust model for the digital business ecosystem for Africa. Information regarding digital business ecosystems, trust, and culture begin with a background study and investigation into the digital business ecosystem for Africa, which is discussed in the next chapter.
Chapter 2

Digital business ecosystem for Africa

2.1 Introduction

In Africa, micro-, very small, small or medium enterprise (SMMEs) represent 90% of private businesses and contribute to more than 50% of employment and GDP (NCR, 2011). In South Africa alone, there are approximately 5 979 510 small businesses which are considered as SMMEs (Finscope, 2010). A valuable SMME sector can contribute to the economy, particularly in developing countries where it can provide an engine through which growth objectives can be achieved (NCR, 2011). However, in developing countries there is a low rate of SMME sustainability. The challenges of conducting business in developing countries differ from, and are more significant, than those in developed countries (Kew and Herrington, 2009) as SMMEs are not able to adopt technologies that are successfully used in developed economies.

In recent years, the uptake of mobile devices, particularly in developing economies, has resulted in a focus shift (Bornman, 2012) for businesses. Opportunities to provide mobile applications to SMMEs and very small enterprises (VSEs), to help them to manage the day-to-day running of their business are being investigated. In this context, the adoption of new forms of e-business by VSEs and SMMEs is identified as a key priority for fostering innovation and competitiveness (Nicolai, 2003). The concept of a digital business ecosystem (DBE) is identified to support VSEs and SMMEs to grow their business and form collaborations with others.

In this chapter, a background on the digital business ecosystem is given where a definition for digital business ecosystems, network architecture and associated properties of a digital business ecosystem are discussed. Insight into the state of SMMEs is given followed by a detailed introduction to very small enterprises (VSEs) and their role in the economy. A use case demonstrates common tasks that VSEs accomplish on a day to day basis to indicate how mobile ICT solutions and the digital business ecosystem can be used to aid VSEs and other SMMEs. This is followed by the challenges that need to be addressed for the digital business ecosystem for Africa to provide a foundation for the remaining research. Finally, the chapter is concluded.
2.2 The digital business ecosystem (DBE)

In 2002, the European Commission (EC) began a multidisciplinary research initiative to establish a complete and comprehensive digital business ecosystem (EC, 2007). In this section, existing definitions for digital ecosystem and digital business ecosystem are provided. A definition for the digital business ecosystem for Africa, which is used by the author of this dissertation, is proposed.

a) Digital ecosystem

A digital ecosystem is an open socio-technical infrastructure aimed at creating a digital environment for networked organisations that supports cooperation, knowledge sharing, the development of open and adaptive technologies, and evolutionary business models (Briscoe and Wilde, 2006, EC, 2007). A digital ecosystem exploits the properties of natural biological ecosystems and is therefore self-organising, scalable, and robust. The concept of digital ecosystem was born through the common discovery of extending the networking model to the knowledge and social models (EC, 2007).

b) Digital business ecosystem

A digital business ecosystem (DBE) is a specific type of digital ecosystem that simulates and implements an environment where small, micro, and medium enterprises (SMMEs) can interoperate (EC, 2007, Lurgi and Estanyol, 2010). The aim of a digital business ecosystem is to support its participants to co-evolve in a competitive, but at the same time collaborative environment (EC, 2007). This is achieved through the sharing of knowledge and information transfer between SMMEs in the digital business ecosystem, thereby forming collaborations. These collaborations ensure that the entire digital business ecosystem's market value is increased by providing growth opportunities for SMMEs (EC, 2007, Lurgi and Estanyol, 2010). For VSEs in Africa, such growth opportunities are vital. As VSEs are at the bottom of the economic pyramid in developing economies in Africa they consequently find it challenging to compete and collaborate with larger enterprises (NCR, 2011).

Generally, digital business ecosystems are supported by diverse technologies to allow SMMEs to offer their services in the digital market place (Lurgi and Estanyol, 2010). Each enterprise or entity in the digital business ecosystem is represented by a software agent, which has the main purpose of facilitating collaborations with other SMMEs in the digital business ecosystem (Lurgi and Estanyol, 2010). Software agents facilitate collaborations at service level using components such as business services, software services, and knowledge representation of the economy. (EC, 2007).
c) Digital business ecosystem definition

For the purpose of this research, a digital business ecosystem, to be applied in an African context, is now defined as follows:

A digital business ecosystem is an environment where entities such as SMMEs interoperate and collaborate with each other through digital means via transactions. Transactions occur among software agents of SMMEs when a SMME provides a service to another SMME and/or vice versa. This service is in the form of knowledge exchange, goods exchange, or expertise exchange.

In order to be able to support a digital business ecosystem applied in an African context, the network architecture of digital business ecosystem is explored next, to understand technology requirements from an architectural perspective.

2.3 Network architecture of a digital business ecosystem

Digital business ecosystems are made possible through the use of Internet technology and the convergence of knowledge networks, ICT networks, and social networks (Nachira et al., 2007) and continue to evolve. They build upon established professional, social, business and collaborations networks used by government, companies, researchers, and friends. As these networks develop, they encourage the distributed sharing of resources and use of distributed architectures, thereby resulting in the growing popularity of the peer-to-peer (P2P) network model.

Digital ecosystems thrive naturally on peer-to-peer (P2P) networks, supported by Internet-based communication technologies such as HTTP (Parameswaran et al., 2001, Nachira et al., 2007), and applications based on specific products or platforms such as instant messaging, chats, and content delivery. However, they lack the ability to make sense of the context of economic life and individual economic players (Nachira et al., 2007). A digital business ecosystem attempts to address this challenge by using relevant software technologies that can accurately reflect the social and economic behaviour and relationships between individuals and economic actors that are easily adoptable by SMMEs in various contexts.
As a digital business ecosystem solution is not elementary, it requires an understanding of the underlying environment, both from a techno-social and economic system point of view. This section discusses the properties of a digital business ecosystem that are to be considered for implementation purposes and the underlying P2P architecture.

### 2.3.1 Properties of a digital business ecosystem

Five common properties of a digital business ecosystem, derived from its implementation (EC, 2007, Nachira et al., 2007, Péntek and Herdon, 2011, Ion et al., 2008, Dini and Nachira, 2004), are now discussed. These properties provide insight into the characteristics and behaviour of a digital business ecosystem, leading to requirement for modelling a digital business ecosystem.

**a) Open environment**

The interaction and collaboration among different SMMEs over the Internet lead to an open environment (EC, 2007, Nachira et al., 2007, Péntek and Herdon, 2011) with the following characteristics:

- unreliability - connections over the Internet can be very unstable, leading to dropped connections, messages getting lost, and message delays due to network traffic.
- dynamic network structure - a diverse range of SMMEs across many locations can join and leave the network at any time resulting in a disruption to the network structure (Dini and Nachira, 2004, Nachira et al., 2007).
- evolving self-organising network structure - the changing network structure requires that the digital business ecosystem has to evolve and self-organise constantly.

These properties naturally lead to the requirement for a decentralised architecture, discussed in the next point.

**b) Decentralised architecture**

A centralised model promotes the possibility of single points of failure, and single points of control, making it a poor choice for implementation. The most fundamental property of a P2P network is decentralisation (EC, 2007, Nachira et al., 2007). The digital business ecosystem thus requires a decentralised P2P architecture due to the following properties (Nachira et al., 2007, Ion et al., 2008):

- There cannot be a single point of failure or control.
The digital business ecosystem should not be dependent upon a single instance or actor. These properties imply the need for balanced and decentralised governance models.

c) Scalability
A decentralised digital business ecosystem implementation must scale well to handle an increased number of nodes, transactions, services, as SMMEs join the ecosystem. (Péntek and Herdon, 2011). A centralised architecture would not be efficient in a situation where the digital business ecosystem grows substantially and operates for an extensive duration. The central node would be overloaded and eventually fail, resulting in a single point of failure for the entire digital business ecosystem. Fortunately, decentralised P2P systems have proven to be very scalable, as demonstrated by millions of users accessing file-sharing systems such as BitTorrent, simultaneously (Péntek and Herdon, 2011).

d) Robustness
A decentralised digital business ecosystem implementation should be robust (EC, 2007, Nachira et al., 2007, Péntek and Herdon, 2011). The scaling, as well as the open environment of a digital business ecosystem both increase the likeliness of errors. When errors occur, the system should be able to continue to function and not let a single fault cause a complete system failure. The digital business ecosystem implementation should also guard against malicious nodes joining the network as fake or real entities that can disrupt the network.

e) Self-organising
A decentralised digital business ecosystem implementation should be able to self-organise (EC, 2007, Nachira et al., 2007, Péntek and Herdon, 2011). As nodes leave and join the network, from various locations across the globe, and interactions occur between human and digital entities, it becomes more complex for a system administrator to manage the entire digital business ecosystem. Therefore, the system should be able to adapt to changes in its dynamic environment. For example, if a malicious node joins the digital business ecosystem, the system should ensure that this node is detected and removed from the network or suspended from collaborating with any other member.

These properties of a digital business ecosystem make its implementation complex. In the next section, the underlying P2P architecture of the digital business ecosystem is discussed in order to determine if it can satisfy many of the properties discussed above.
2.3.2 Peer-to-peer architecture for the digital business ecosystem

Digital business ecosystem communities require direct interaction between participants or peers, in order to perform transactions or exchange information. Such communities can be represented by P2P applications that are implemented by an abstract overlay network, defined at the application layer, over a physical P2P network topology. Next, definitions of a P2P network, an overlay network and P2P overlay network architecture are given and challenges of unstructured P2P overlay network architectures for digital business ecosystems are identified.

a) Definition: Peer-to-peer (P2P) network

A P2P network is a distributed application architecture where peers are used by their owners to communicate information, share or consume services and resources with other peers whom they are aware of (Stoica et al., 2001, Saroiu et al., 2001). A peer is a network-addressable computing element such as a mobile device, desktop computer, or network server (Klemm et al., 2003, Saroiu et al., 2001, Stoica et al., 2001). Peers can be both clients and servers respectively, by supporting resource sharing and allowing access to resources.

Figure 2.1 depicts the PeerTrust (Xiong and Liu, 2004) architecture, which is an example of a reputable well-known P2P network. In this architecture, each peer is responsible for maintaining its own computational system, known as an agent. In a P2P network, peers communicate with other peers directly. There is no central entity controlling the communication between them. Each peer has to make its own decision as to which peer it communicates with and potentially transacts with. In order to deal with strangers, trust is thus important to maintain in a P2P network.

A peer in the P2P network maintains a record of all the other peers it has transacted with to be able to communicate and compute the trust level of other peers. Communication and trust computation are therefore functions controlled by the agent.
b) Definition: Overlay network

An overlay network consists of virtual or logical links that interact with physical links in the underlying network (Eng Keong et al., 2005). Such networks are not dictated by the underlying physical presence, which is usually static, but rather by the logical relationships between peers (Voulgaris et al., 2005). P2P overlay networks overlay Internet Protocol (IP) networks that support a number features such as robustness and scalability (Lua et al., 2005).

Systems that implement P2P overlay networks require fault-tolerance, self-organisation, and scalability properties. These requirements are in line with those required by digital business ecosystems, and thus P2P overlay networks are suited to the implementation of these digital business ecosystems.

Figure 2.2 gives the P2P overlay network (EC, 2007) that models the overall architecture of a digital business ecosystem. Peers are software agents that represent entities such as businesses in the digital business ecosystem. For example, a business entity such as SpazaShop A in Figure 2.2 is a peer in the digital business ecosystem P2P overlay network,
and is supported by a software agent running on a machine connected to the Internet or some other network.

A peer such as SpazaShop A collaborates with other peers through knowledge exchange, goods exchange, or expertise exchange and acts as either a client or a server in a particular transaction. The overlay network provides the digital business ecosystem with the possible guarantee of no single point of failure, robust knowledge transfer and service provision through a set of collaborative nodes.

**Figure 2.2 Digital business ecosystem P2P Overlay Network**

c) **P2P overlay network architecture**

Based on how the nodes in the overlay network are linked to each other, P2P networks can be classified as either structured or unstructured.

- structured P2P networks make use of Distributed Hash Table (DHT) to locate specific peers using a key-value mapping (Voulgaris et al., 2005, Lua et al., 2005, Aberer et al., 2003). This imposes a specific linkage structure between nodes.
unstructured P2P overlay networks allow peers to join the network without any predefined deterministic scheme for linking nodes (Voulgaris et al., 2005). Therefore, peers have no prior knowledge of the network topology, making the task of locating specific peers more challenging (Lua et al., 2005). Unstructured implementations are aimed at systems to provide rapid information dissemination and content-based searching in distributed environments that are highly dynamic (Voulgaris et al., 2005).

For the digital business ecosystem, an unstructured P2P architecture is applicable, as peers have no prior knowledge of the network topology. This introduces challenges, described next.

d) Challenges of unstructured P2P overlay network architectures for digital business ecosystems

The challenge of using unstructured P2P overlay networks is that peers are not always aware of other peers in the network. This makes it challenging to find specific peers since there is no central peer who has knowledge of the entire network and other peers. For example, should SpazaShop A in Figure 2.2 want to collaborate with the SpazaShop B in Figure 2.2, it needs to ask the peers that it is connected to, to provide a “route” from SpazaShop A to SpazaShop B.

Another challenge is that peers often interact with strangers and thus need to manage the risk involved with each interaction. Peers thus need to have the ability to decide how and when to interact with others, which is an important focus of this research. SpazaShop A thus needs to be able to determine if SpazaShop B can be trusted before SpazaShop A interacts with SpazaShop B.

To further motivate this research with respect to the manner in which trust between peers in unstructured P2P overlay networks should be addressed, the next section discusses the state of SMMEs and ICT (Information Communication Technology) in Africa.

2.4 The state of small businesses and ICT in Africa

SMMEs are the backbone of the economy in Africa according to the Economic Report on Africa (2011). This section provides an indication of the state of SMMEs and ICT (Information Communication Technology) in Africa, followed by a description of very small enterprises (VSEs) and their difference in nature to other businesses.
2.4.1 The state of SMMEs and ICT in Africa

A definition for SMMEs that identifies the types of businesses that participate in the digital business ecosystem for Africa is now given. The current state of ICT acceptance among SMMEs is then discussed, identifying the challenges that exist in developing economies such as Africa.

a) SMMEs

The definition of SMME proposed by National Small Business Amendment Act of 2004 is (DTI, 2008):

“…a separate and distinct business entity, including cooperative enterprises and non-governmental organisations, managed by one owner or more. Businesses are categorized as micro-, very small, small or medium enterprise (SMME).”

According to the definition there are a number of businesses which fall into the SMME category. Examples include small shops; suppliers; construction companies; artisans; accountants; marketing businesses; hair salons; beauty salons; dentists; doctors; and many others. Many of these businesses can benefit from collaborations where small shops form cooperatives to purchase bulk supplies from suppliers at discounted prices.

A key factor in achieving business success and growth is the forming of cooperatives among SMMEs (Mabuza, 2009). However, in a competitive environment it is vital to select the appropriate collaboration partner due to the risks involved (Kew and Herrington, 2009). If collaboration fails, there is great financial or time loss for SMMEs. This negatively impacts a small business more than it would a larger enterprise that has the capacity to plan better for such situations.

This research now identifies that SMMEs can perform better if they are supported to collaborate with each other. Unfortunately, the process of selecting appropriate or trusted partners is a major stumbling block.

The next subsection considers the state of ICT in Africa to be able to understand which technology is viable to support digital business ecosystems for this research.
b) The state of ICT in Africa

The constant uptake of mobile devices and improved telecommunication infrastructure connects many people and businesses in Africa (Bornman, 2012). Although ICT provides the opportunity to enable collaborations, many SMMEs in Africa have not adopted such ICT solutions according to the Economic Report on Africa (2011). The main reason for the low acceptance is the community’s suspicion of ICT usage (Maier and Nair-Reichert, 2007). This is a result of lack of ICT training and awareness for small business owners and employees (Kew and Herrington, 2009). Without confidence in the technology, businesses are less willing to trust ICT solutions to assist with their business operations and choice of partners.

According to the Economic Report on Africa (2011) there is a large subsection of SMMEs known as very small enterprises (VSEs) that have found it even more challenging to accept such ICT solutions and conduct business using these solutions. This is unfortunate as ICT has a direct impact to their business. In the next section, a description of VSEs is provided.

2.4.2 Very small enterprises (VSE) in the digital business ecosystem

VSEs follow the definition of SMMEs discussed in the previous section, but have a few characteristics such as size, informal operation and cultural adaptation that need to be further considered. Furthermore, people in charge of VSEs have a high adoption of mobile usage. Therefore it is possible that digital business ecosystem solutions may be applied to enhance growth and collaboration between VSEs. In this section these aspects are further discussed.

a) VSE size:

VSEs consist of fewer than 10 paid employees in most industry sectors, formal and informal. VSEs contribute to about 45% to 64% of SMMEs throughout South Africa and similarly in Africa (DTI, 2008) making them a majority among Africa SMMEs and the economy. Examples of VSEs include very small retail shops (known as spaza shops in South Africa), plumbers, builders, hair salons, tour guides, and taxi drivers.

b) Informal operation:

Among VSE, there is a large number of businesses that operate informally (DTI, 2008, Africa, 2011). Informal businesses are those that are not registered in any way and seldom operate from business premises. They are usually run from home, street pavements, very small buildings, or other informal arrangements, particularly in rural areas (DTI, 2008). The value of the informal sector should not be underestimated since it plays a large role in the economy of Africa (Finscope, 2010, DTI, 2008, Africa, 2011).
Informal businesses often provide services and products to the formal economy, and vice versa. For example, informal retail shops purchase products from the formal suppliers. The informal sector also provides a safety net for many people who would otherwise not be supported by the formal sector. In the 1990s, most of the jobs in urban Africa were dominated by the informal sector (DTI, 2008).

c) **Conduct business according to cultural norms and behaviour:**
Due to the size of VSEs and their informal nature, these businesses are more personal. Owners tend to run the business and make business decisions based on personal relationships and understandings. Their personal behaviour is in turn influenced by their cultural norms and behaviour (Hofstede et al., 1991). This highlights the fact that it is important to consider the role of culture when a digital business ecosystem for VSEs is implemented. Culture would affect how collaborations are formed and supported since it involves committing to and trusting another business.

For example, many African cultures place emphasis on group loyalty (Moliea, 2007) and social position (Cramer, 2010). Should a negative comment about the work of a group member lead to a decrease in the reputation of the group, other group members would refrain from making this comment public. They would also ensure the group member does not jeopardise the group’s harmony in the future. Also, recommendations from people with a high social standing tend to have more weighting than recommendations from people with a lower social standing, indicating that a factor such as social position needs to be considered carefully (Botha, 2007, Moliea, 2007).

d) **High adoption of mobile usage:**
Studies have shown that the adoption and use of mobile devices among businesses in Africa has been high over the last few years (Bornman, 2012, Esselaar et al., 2006, Kew and Herrington, 2009). Kew and Herrington (2009) indicate that mobile usage by businesses is higher in rural businesses than in urban-based businesses. Both are very high where 97.6% of rural businesses and 94.1% of urban businesses use their mobile device to conduct business. For VSEs in the informal sector, the use of a mobile device is necessary since the business does not have a real office location. Furthermore, the cost of implementing sophisticated ICT infrastructure such as using laptop computers and fixed phone lines is usually beyond the financial means of the VSEs owner.
e) Potential for digital business ecosystem technology to support VSE growth:
Recent research projects have consequently focused on investigating how to support VSEs such as shop owners by means of e-commerce applications backed by mobile and cloud-based technologies (Dorflinger et al., 2009). If VSEs such as small retail shops, plumbers, electricians, and tour guides can access business applications through their mobile devices, they can be brought into a digital business environment, creating new possibilities. A digital business ecosystem can provide a number of potential business opportunities that were not possible before, including: ordering products online from suppliers; forming online bulk buying cooperatives; automatic job scheduling; automatic invoicing, debtor management, and applying for micro-financing loans.

The potential growth of VSEs through ICT solutions using a digital business ecosystem is clear, however, the adoption of such existing ICT solutions has been low. In order to gain a better understanding of the operations of a typical VSE, the next section details a use case study that will be referred to throughout this research.

2.5 Use case study of VSEs in Africa

A recent research project conducted at SAP Research Pretoria, South Africa (Ngassam et al., 2011) attempts to support VSEs with a mobile ICT solution to provide mobile services to assist VSEs with the day-to-day running of their businesses. The research provides an accurate account of the needs of spaza shops, providing valuable insight by means of the use case study. In this section, the use case of VSE spaza shops is discussed. The use case represents typical challenges face by many VSEs in Africa.

2.5.1 Background

A spaza shop is an example of a VSE found in rural townships in Africa. These businesses are survivalist businesses that find it challenging to sustain their business. This is due to a low financial liquidity, making small purchases at a time, lack of credit or ability to negotiate discounts, and the transport costs associated with many small purchases (Kew and Herrington, 2009, Friedland et al., 2008). They sell groceries and general supplies to residents of the community, who cannot travel due to transport difficulties or because of financial reasons. The following features and challenges need to be considered:
a) Business operation is manual, slow and error-prone
Spaza shops have historically established collaborations with suppliers by physically going to a supplier and manually selecting and paying for the products. Typically, a spaza shop owner or employee takes stock in the morning. If new stock is required, the owner or employee travels into the town to purchase the required products from a supplier. Many factors influence which supplier is selected, such as on-going specials, prices per particular items, travelling distance to supplier, past experience with supplier, and supplier recommendations from others. Once the products are purchased, the spaza shop owner or employee travels back to the spaza shop and packs the shelves with the procured products. Spaza shops spend numerous hours each week travelling to and purchasing products from suppliers, which means this time is lost to selling goods if the shop only has one employee. This also has financial implications due to the cost of travelling. Over and above this, the spaza shop is responsible for ensuring stock is managed, finances are in order, and debtors are managed.

b) Spaza shops can increase efficiency with bulk buying
In bulk buying, spaza shop owners collectively purchase products from a supplier in order to be able to receive a greater discount where possible for a large order. One or more spaza shop owners or employees collects money from other spaza shop owners, who form part of the cooperative. A single spaza shop owner or employee travels and purchases all products and can negotiate better prices with suppliers due to bulk orders. The products are collected by the purchasing spaza shop, and distributed to the other spaza shops or a central location. Spaza shop owners are encouraged to form cooperatives and participate in bulk buying as it saves on costs and provides a competitive advantage against suppliers and other spaza shops (SpazaNews, 2010).

c) Challenges preventing bulk buying:
There are a number of issues that prevent spaza shops from partaking in joint bulk buying initiatives (SpazaNews, 2010):

- Spaza shop owners are concerned that their money would not be secure if a single person is entrusted to do the bulk buying.
- Some spaza shop owners are concerned that other spaza shop owners will gain insight into their financial status.
- Many spaza shop owners work in isolation and find it challenging to adapt to and operate in collective bulk buying environments.
• Some members of the bulk buying cooperative, who are competitors in the same region as other spaza shops, feel uncomfortable about collaborating when buying products in bulk.

d) Challenges preventing collaboration:
The underlying challenge that can be derived is that there is a basic level of distrust between VSEs. As failed transactions or mismanagement of money can lead to great losses for these businesses they need to carefully consider their position.

A main challenge to address is thus how to foster and support trust relationships between VSEs, and at the same time address the cultural behaviour of VSEs, to ensure they are more comfortable with the operation of the digital business ecosystem implementation. The next section presents the requirements of a proposed solution to address these challenges.

2.5.2 Requirements for a digital business ecosystem to support collaboration among VSEs

This research aims to provide a computational infrastructure that supports collaboration between VSEs, to enable a business community to evolve to meet emerging business opportunities. A custom-defined digital business ecosystem can contribute to achieving this goal.

Such a digital business ecosystem aims to support an environment for VSEs to operate, in a competitive yet collaborative manner. Figure 2.3 depicts an example of such an ecosystem where nodes represent the software agents of businesses, and the links between them represent the collaboration relationships that exist between businesses. The figure depicts many businesses that could potentially collaborate with one another to enhance the business ecosystem for these VSEs.
Figure 2.3 Digital business ecosystem for Africa consisting of SMMEs

In order to address some of the concerns highlighted in the case study, the following set of requirements for a digital business ecosystem to support collaboration among VSEs is defined:

a) Digital business ecosystem facilitates collaborations through mobile and cloud technology
b) Digital business ecosystem supports trust and reputation in a decentralised architecture
c) Digital business ecosystem complies to the cultural behaviour and beliefs of the participants

These requirements are now discussed.

a) Digital business ecosystem facilitates collaborations through mobile and cloud technology

Virtual collaborations between peers are created when VSEs are connected to each other to perform online procurement or online bulk buying initiatives through a mobile application.
Spaza shops can collaborate with each other over the Internet using their mobile devices and cloud technology to establish and maintain a successful business. The interface on the mobile application gives access to back-end resources on the cloud and supports the ability to find new business partners and participate in transactions. However, this requires that trust is supported.

b) Digital business ecosystem supports trust and reputation in a decentralised architecture

It is not feasible to partner with any available spaza shop or supplier if their reliability is not known beforehand. The spaza shop needs to determine who is trustworthy before deciding to collaborate. In this situation, recommendations for others can assist spaza shop owners to identify reliable and trustworthy partners. Such recommendations can be provided by SMMEs or a trust and reputation component in the digital business ecosystem system, or both. If a VSE needs to become a strong competitor in the environment, it needs to identify other strong partners in the network to collaborate with as they can provide better business opportunities.

A decentralised trust and reputation components needs to be implemented due to the decentralised nature of the environment. This means that the software agents of VSEs and other SMMEs in the digital business ecosystem need to maintain the state of connections and transaction history. This makes trust and reputation challenging to implement in the digital business ecosystem.

c) Digital business ecosystem complies to the cultural behaviour and beliefs of the participants

There are real differences between the environment and cultures of rural Africans and those of developed economies, such as in the Western world (Isherwood et al., 2012, Doney et al., 1998, Zaheer and Zaheer, 2006, Chong, 2003, Botha, 2007). Therefore, it cannot be assumed that existing trust and reputation models, primarily designed for developed economies are just as applicable to cultures in Africa. It is important that a digital business ecosystem built for Africa should consider African cultural behaviour. For example, recommendations from strangers may not easily be accepted by cultures in Africa. However, the success of an e-commerce platform such as Ebay (eBay, 2012) is testament to the role of recommendations from stranger, in developed economies.

Therefore, the influence that culture has on trust and reputation should be explored for the digital business ecosystem in Africa. Cultural parameters could provide additional input into a
trust and reputation system used by the digital business ecosystem, making it more relevant to the cultures in Africa.

For the remained of this research, the term “SMME” is used to refer to all businesses in a digital business ecosystem, including VSEs. Although the focus is on VSEs, SMMEs are also supported since the digital business ecosystem caters for SMMEs.

2.6 Conclusion

In this chapter, it is shown that SMMEs contribute to a large portion of the African economy. The facilitation of collaborations among SMMEs provides the opportunity for the survival and growth of SMMEs and the economy. A digital business ecosystem, adapted for the context of cultures in Africa is proposed, to support SMMEs to collaborate in the form of transactions.

The underlying environment of a digital business ecosystem was discussed in detail, providing the properties of a digital business ecosystem that need to be addressed. The digital business ecosystem adapts itself naturally to a P2P, decentralised architecture, satisfying many of its properties.

P2P architectures present a number of challenges for the digital business ecosystem for Africa. SMMEs are not always aware of other SMMEs in the network and may therefore be required to transact with strangers. Hence, trust needs to be address in such an environment and is an essential prerequisite for facilitating collaborations among SMMEs. A digital business ecosystem attempts to address these challenges by developing relevant software technologies that can accurately reflect the social and economic behaviour and relationships between SMMEs. Therefore, the state of SMMEs and ICT in Africa is discussed with a particular focus on VSEs. VSEs face many challenges in developing economies and the digital business ecosystem for Africa needs to consider these.

Through the use of mobile ICT solutions and cloud computing, the technology needs of VSEs can be satisfied. A use case is discussed, providing an understanding of the day-to-day operations of a VSE. Their approach to business makes it challenging to address the social behaviour of VSEs in Africa as it differs from many other regions in developed economies. The social behaviour is largely derived from the cultural norms and behaviour of VSE owners and employees, who conform to a specific culture. Trust in the digital business ecosystem for Africa, therefore needs to consider cultural behaviour and norms in its design.
Finally, the chapter is concluded by presenting three requirements for a digital business ecosystem for Africa to support collaboration among VSEs, namely: facilitate collaborations through mobile and cloud technology, support trust and reputation in a decentralised architecture, and comply with the cultural behaviour and beliefs of the participants. These requirements are addressed in the chapters that follow.

This chapter sets the tone for the literature review that follows. In chapter 3, trust and reputation for the digital business ecosystem is discussed in order to gain an understanding of important concepts to consider. As culture is identified to be an important aspect of an ICT solution in the African context, chapter 4 comprehensively discusses the influence of culture on trust. From this discussion, social relationships are found to play an important role and consequently chapter 5 introduces social network analysis for the digital business ecosystem for collectivist cultures.
Chapter 3

Trust and reputation for digital business ecosystems

3.1 Introduction

The previous chapter noted that the selection of collaboration partners, who may be strangers at the time, is a challenge that needs to be addressed. Since trust forms the basis of all human interaction, collaboration and society (McKnight and Chervany, 1996), businesses, represented as agents, need to decide on who to collaborate with based on the trust they have in each other.

The more a partner is trusted, the higher its reputation is likely to be in its community. Participants with high reputation are more likely to be selected, leading to further business and more profit due to successful transactions (Cornelli et al., 2002, Liu et al., 2012b). This indicates that in the digital business ecosystem, trust and reputation are important parameters to consider. By using a trust and reputation system, businesses can make better decisions about whom to collaborate with. By choosing more reliable partners, an environment can be cultivated where more successful collaborations occur.

A clear understanding is now required of how trust and reputation can be modelled in a dynamic, P2P environment where enterprises are represented as agents. Trust and reputation models calculate trust differently, depending on their goals and objectives. For example, one model might take into account the social position of a node (Sabater and Sierra, 2001) where others may attempt to encourage the nodes to provide feedback by rewarding them (Xiong and Liu, 2004).

There are core components of trust and reputation that are present, regardless of the trust and reputation model or system used. For example, trust is subjective and influenced by the context of the transaction (Abdul-Rahman and Hailes, 1998, Ziegler and Lausen, 2005, Xiong and Liu, 2004). Therefore, there are several aspects of trust and reputation that need to be present at all times. These aspects are discussed in this chapter, thereby providing an
overview of trust and reputation so as to focus its implementation within the digital business ecosystem.

In this chapter, trust and reputation are presented, and the difference between them is discussed. The approach to calculating trust and reputation is discussed, followed by a comparison of existing trust and reputation models and systems in order to identify important features. Based on the comparison, a relevant existing trust and reputation model is identified to provide the foundation of the proposed model for this research. The chapter is finally concluded.

### 3.2 Trust

Trust has received much attention in past and current literature, and a number of definitions from several disciplines such as psychology (Lewis and Weigert, 1985, Luhmann, 1979, Castelfranchi et al., 2003), economics (Zhang and Cohen, 2007, Bachmann, 2001), and sociology (Misztal, 1996, Rutter, 2001, Lewis and Weigert, 1985) are found. Trust definitions from a computer science perspective are built over the research on trust in other disciplines. Such definitions of trust are commonly used by, and implemented in, trust and reputation systems. A definition of trust for research is defined next, supported by current research.

**a) Trust in computer science**

Definitions of trust commonly used in computer science is that of McKnight and Chervany (1996) and Mayer et al. (1995).

McKnight and Chervany (1996) define trust as "the extent to which one entity is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible".

Mayer et al. (1995) define trust as “the willingness of an entity to be vulnerable to the actions of another entity, based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other entity”.

These definitions imply that entities that collaborate with others are vulnerable to the actions of other entities and therefore require trust to be present to allow them to rely on and predict the actions of the other entities. This situation is applicable in the digital business ecosystem and is discussed next.
b) Trust in the digital business ecosystem

Collaborations between entities in the digital business ecosystem are established when they participate in a transaction. Entities are in the form of software agents, representing a SMME, or the actual SMME itself. SMMEs thus require the management of trust to be supported through their corresponding software agent.

These collaborations imply a level of risk, since an agent or business can chose to act maliciously, thereby causing damage to the other entities involved in the transaction. Therefore, entities involved in transactions in the digital business ecosystem need to determine the extent to which they will depend on other entities, i.e. the trust they have in another entity.

For the purpose of this research, trust in the digital business ecosystem is defined as follows:

> Trust is the extent to which one entity, in the form of an agent or business or both, is willing to enter into a transaction with another entity in the digital business ecosystem, with the acceptance of being vulnerable to the actions of the other entity, whether negative or positive, and without control over the other entity’s actions.

Figure 3.1 depicts this situation where A the trustee is willing to enter into the transaction with B the trustor. $T_{AB}$ is the level of trust that A has in B, making A vulnerable to the actions of B.

![Figure 3.1 Trustee, trustor and trust level scenario](image)

This definition is based closely on the definition of McKnight and Chervany (1996) and Mayer et al. (1995) but is adapted for the digital business ecosystem. The definition of trust and its relation to social behaviour gives rise to a number of trust properties, which are common
among this and other definitions of trust. These properties are discussed in the next section. This is followed by a discussion on the constructs of trust. These discussions are relevant as they have an influence on the implementation of trust within a system.

### 3.2.1 Properties of trust

Regardless of the exact definition of trust and the discipline it is derived from, there are some key properties of trust which are identified, and which are used by trust models and mechanisms in computer systems (Hardin, 1993, Yamagishi, 1988, Abdul-Rahman and Hailes, 2000, Jøsang and Pope, 2005, Wang, 2010) The properties of trust are as follows:

i. **Trust is context dependent.** This means that the trust associated with an entity is relative to its context, and the trust might not be the same in another context. For example, SpazaShop A trusts Supplier A to supply products but not to provide repair services.

ii. **Trust is transitive.** This involves the notion that trust can be passed on between people to some degree (Matsuo and Yamamoto, 2009, Ziegler and Lausen, 2005). For example, if SpazaShop A trusts SpazaShop B, and SpazaShop B trusts SpazaShop C, then SpazaShop A can trust SpazaShop C to a certain extent, due to its trust in SpazaShop B.

iii. **Trust is subjective.** Trust is a personal opinion and cannot be assumed to be mutual (McKnight and Chervany, 1996). For example, SpazaShop A might trust Supplier A but it doesn't imply that SpazaShop B trusts Supplier A to the same extent.

iv. **Trust is dynamic and non-monotonic.** This means that trust does not always remain the same. Based on experiences at a later stage, the degree of trust in another may increase or decrease. If SpazaShop A trusts SpazaShop B, but then SpazaShop B behaves maliciously by not paying his portion of the bulk buying expense, then SpazaShop A can alter the amount of trust it places in SpazaShop B.

v. **Trust is based on prior experiences.** Experience and knowledge of another’s previous behaviour provides a basis for trust in future situations that are familiar in terms of context (Luhmann, 1979). For example, SpazaShop A trusted Supplier A to supply fresh fruit vegetables and Supplier A did a satisfactory job, then SpazaShop A can use this experience and decide to trust Supplier A again, to supply fresh fruit and vegetables.

vi. **Trust is multi-faceted** (Wang, 2010). An entity might model trust based on a number of characteristics and then make a trusting decision based on the aggregation of these characteristics. For instance, SpazaShop A might evaluate Supplier A on the freshness of fruit and vegetables it provides, how professional Supplier A is, and the price Supplier
A charges, and then aggregate the trust of each aspect to determine how much SpazaShop A trusts Supplier A.

vii. Trust only exists in an uncertain and risky environment (Wang, 2010). Where there is risk involved, the transaction may result in a bad consequence which could harm the entities involved in the transaction. For example, SpazaShop B could easily default on paying his portion of the bulk buying expense to SpazaShop A. This would force SpazaShop A to cover the additional costs of SpazaShop B. This is why SpazaShop A has to trust SpazaShop B when forming a bulk buying cooperative.

viii. Trust is used for decision making to help entities achieve desirable consequences (Wang, 2010). An example is SpazaShop A selecting Supplier A as its supplier of fresh fruit and vegetables. This so SpazaShop A can sell fresh fruit and vegetables to its customers.

These trust properties define the requirements for modelling trust and reputation in systems such as the digital business ecosystem. In the next section, the constructs of trust are discussed which gives insight into the formation of trust.

### 3.2.2 Constructs of trust

The constructs of trust were originally proposed by McKnight and Chervany (1996) and are discussed to provide a deeper understanding of how trust is formed.

#### a) Trust constructs

McKnight and Chervany (1996) identify six trust constructs that illustrate how trust is formed. Figure 3.2 shows four trust constructs namely ‘dispositional trust’ and ‘situational decision to trust’, ‘trusting beliefs’, ‘system trust’ that together support the construct ‘trusting intentions’, and eventually result in establishing ‘trusting behaviour’. 
i. Situational decision to trust denotes the readiness to trust other entities in general, in a given situation. This suggests that one has formed an intention to trust whenever a specific situation arises, regardless of the belief about the characteristics of the other entity in the situation. For example, SpazaShop A decides it can trust other spaza shops when it comes to forming bulking buying cooperatives but not for investing in other business opportunities. The situation being bulk buying.

ii. Dispositional trust is a general inclination to trust others. As one develops over the course of one’s life, expectations are generalised about how trustworthy others are. For example, SpazaShop A may generally trust newly established businesses more than other spaza shops would, leading to a higher dispositional trust.

iii. Trusting beliefs define the perception (belief) of one entity that the other entity will act appropriately in a given situation. These beliefs are mainly categorised as ability, integrity and benevolence.

- **Ability** pertains to the belief of one entity that the other entity acts according to their represented ability. For example, a supplier should supply quality goods if that is their represented ability.

- **Integrity** reflects the belief that a trusted entity adheres to its obligations. For example, spaza shops in a bulk buying cooperative are required to pay for their orders.

- **Benevolence** relates to the belief of one entity that the other entity cares about them, and will not take advantage of them. For example, SpazaShop A believes that SpazaShop B will not take advantage of them when collaborating.
iv. System trust refers to extent that one believes that there are proper and objective, structures in place to enable one to anticipate a successful future transaction. For e-commerce, structural assurance is the belief that the web has protective legal or technological structures that assure that business can be conducted in a safe and secure manner. If a consumer understands how SSL encryption works and experiences a sense of normality when a transaction happens securely, his/her system trust increases.

v. Trusting intention is the willingness of one entity to depend on another entity in a given situation. Trusting intention is determined according to an entity’s previous four constructs. If SpazaShop A generally trusts in a specific situation, has a high dispositional trust, has a high trust belief in SpazaShop B, and trusts the system then SpazaShop A will have a high willingness and trusting intention to trust SpazaShop B.

vi. Trusting behaviour is the extent to which one entity voluntarily depends on another entity in a specific situation with a feeling of relative security even though negative consequences are possible. One entity therefore takes action on their willingness to depend on another entity. In this case, SpazaShop A acts on its trusting intention by trusting SpazaShop B and therefore collaborates with them. Trusting behaviour is similar to trusting intentions with the key difference being that trusting behaviour is a behaviour-based construct where one entity depends on another and trusting intention is a cognitive-based construct where one entity is willing to depend on another.

b) Trust in e-commerce

According to Ratnasingam (2001) and Sia et al. (2009) trusting beliefs are a key construct of trust when considering e-commerce. Trusting beliefs form the foundation, along with the other constructs, leading into a trusting intention and thereafter a trusting behaviour. Literature further indicates that trust is established in three stages in e-commerce environments (Ratnasingam, 2001), namely: competence trust, predictability trust, and goodwill trust. These stages are similar to trusting beliefs and indicate how trusting beliefs influence once another. These stages are now mentioned.

i. Competence trust

Firstly, competence trust is established through the trust and security mechanisms embedded in e-commerce technologies to provide speed and real-time accurate information. In the digital business ecosystem this is established through security mechanisms implemented into the software of an agent, representing the SMME, and within the distributed ecosystem. A SMME
accessing a mobile application used by the digital business ecosystem will have to be sure that the application will perform reliably before having competence trust. Competence trust is therefore related to the ability trusting belief as well as the system trust construct.

ii. Predictability trust
Secondly, consistent positive behaviour from trading partners leads to credibility and reliability, which creates predictability trust. In the digital business ecosystem, predictability trust is established as SMMEs collaborate with each other and transact successfully. The SMMEs will then be able to predict the level of trust of SMMEs they have collaborated with previously. Predictability trust is therefore related to the integrity trusting belief as well as situational decision to trust construct.

iii. Goodwill trust
Lastly, goodwill trust focuses on organisational reputation and brand names, and is accomplished by enforcing best business practices. The formation of goodwill trust exists in the digital business ecosystem as enterprises implement best practices and enhance their company’s image and reputation through successful collaborations. Goodwill trust is therefore related to the benevolence trusting belief.

It’s clear that trust has many components which make it challenging to model and implement. Another measure often used, when referring to trust, is reputation. Reputation assists to determine the trustworthiness of an entity from another view. However, differences between trust and reputation are important to consider when understanding and implementing trust and reputation systems. Reputation is discussed in the next section.

3.3 Reputation

It is generally agreed upon in literature that reputation is an objective measure that represents the aggregated opinion of a group of entities towards another (Kamvar et al., 2003, Wang, 2010, Jøsang et al., 2007). The reputation of an entity is based on all past actions with the other entities that it has interacted with, and the associated ratings (Ion et al., 2008). This is in contrast to trust which is a subjective measure and reflects the opinion of an individual.

Reputation plays a major role in large open ended, P2P systems such as the digital business ecosystem, where entities involved in a transaction might not know each other (Wang, 2010, Jøsang et al., 2007). If a member of the digital business ecosystem, SpazaShop A has not previously interacted with another member, Supplier A, there is no previous experience on
which to evaluate the trust which can be placed in Supplier A. Therefore, reputation can be used to gain some insight into the perceived trustworthiness of Supplier A according to other members of the digital business ecosystem that have previously interacted with Supplier A.

Suppose SpazaShop A has previously interacted with Supplier A, the reputation of Supplier A can still be considered, along with the previous experience, when determining the trustworthiness of Supplier A. In this case, a weighting can be placed on the importance of previous experience and the importance of reputation in the trust calculation. Therefore, a member of the digital business ecosystem with a good reputation is trusted more by other members, than one with a bad reputation. This implies that trust can be built through reputation.

This is depicted in Figure 3.3 where SpazaShop A gathers the reputation of Supplier A from those that have collaborated with Supplier A (i.e. SpazaShop C and SpazaShop B). This is used as input to determine how much trust SpazaShop A can place in Supplier B.

![Figure 3.3 Determining reputation example](image)

Another positive implication of reputation in large open ended, P2P systems is that it encourages good behaviour within the system (Wang, 2010, Jøsang et al., 2007). Members that behave well are presented with more opportunities for collaborations. In contrast, members that behave badly and cause negative disruption in the network have a bad
reputation and are not considered by other members as trustworthy. Therefore, their collaboration opportunities are limited as other members are hesitant to collaborate with them. This could lead to the eventual exclusion from the digital business ecosystem network. The digital business ecosystem network would then have one less member who negatively affects the reputation of the entire digital business ecosystem.

In summary, reputation is an important measure when determining the trust of members in a large open ended P2P system such as the digital business ecosystem. For this research, the researcher now identifies two benefits of reputation for the digital business ecosystem:

i. From an individual perspective, members of the digital business ecosystem can use reputation to help identify other members, who are trustworthy, to interact with. As mentioned previously, this is particularly useful when members need to interact with strangers.

ii. From the perspective of the collective digital business ecosystem, reputation encourages good behaviour among the members. Reputation also enhances the digital business ecosystem by self-organising the network to ensure that bad or malicious members do not disrupt the network.

It is thus clear that trust and reputation are not the same, but that they complement each other.

Understanding trust, its associated properties and constructs, and reputation are the first step towards developing a trust and reputation system. In the next section, computations for trust and reputation for the digital business ecosystem are discussed.

### 3.4 Trust and reputation computation for the digital business ecosystem

When computing trust and reputation, a number of issues arise. Firstly, the type of metric to be used to measure the trust and reputation values needs to be determined. Secondly, the scope of this metrics should be determined. Thirdly, the type of trust and reputation computation architecture needs to be determined to make it compatible with the P2P architecture of the digital business ecosystem. Lastly, the approaches to calculating trust and reputation need to be determined. In this section, these issues are discussed and addressed.
3.4.1 Trust and reputation metrics

Initially, metrics were deployed to support Public Key Infrastructure (PKI) (Zimmermann, 1995) but more recent research has focused on trust metrics for other fields such as, P2P networks, mobile computing, rating systems for online communities and other fields where the use of a certification authority is not feasible (Ziegler and Lausen, 2005). Trust metrics are used to assign a computed estimate of how much one entity trusts another entity (Ziegler and Lausen, 2005). Regardless of how the trust metric is calculated, the value returned should enable an entity to make a trusting decision based on it.

There are a variety of approaches to trust metrics that are used in different trust and reputation systems. One of the first proposed trust metrics is defined by Abdul-Rahman and Hailes (1998). The trust metric is assigned as a category, with an associated value, namely: Distrust (-1), Ignorance (0), Minimal (1), Average (2), Good (3), and Complete (4).

Golbeck et al. (2003) extended on the Friend-Of-A-Friend (FOAF) model (Dumbill, 2002) by including a trust metric for a person using a scale of 1 - 9. The levels range from distrusts absolutely (1) to trusts absolutely (9). Later, this metric was extended to a scale of 1 – 10 (Golbeck and Hendler, 2006).

Other models make use of a trust metric which is a real number between 0 and 1 (Ziegler and Golbeck, 2007, Xiong and Liu, 2004, Zhou and Hwang, 2007). This trust metric usually assigns no trust to 0 and completely trustworthy to 1, to represent the level of trust in an entity. This is a popular trust metric among many reputable trust and reputation models.

For the purpose of this research, a real number in the range [0, 1] is used as the trust metric. This allows flexibility in the way trust is represented since the limits are the values 0 and 1 and any real number between them can assigned which allows for an accurate representation of levels of trust.

The trust metric defines a value to represent trust which is used throughout the system, however, the scope of such a metric still needs to be determined. This is discussed in the next section.
3.4.2 Scope of trust and reputation metrics

In order to evaluate a digital business ecosystems participant’s trustworthiness, an agent needs to rely on the judgments of other peers who have already interacted with them and shared their impression. These impressions are expressed as trust metrics. Trust metrics are divided into those with global and those with local scope (Ziegler and Lausen, 2005). This section discusses global and local trust metrics and their relation to the digital business ecosystem, making use of Figure 3.4 to highlight the difference.

![Figure 3.4 Digital business ecosystem for Africa with communities](image)

In Figure 3.4, w and x are communities that have formed within the network. Community w consists of a several SMMEs that have formed a collaboration group where they transact with each other on a regular basis. These communities are now referenced in this section so as to depict the scope of global and local trust metrics.
a) Global trust metrics

Global trust metrics take into account all the peers in the network and their relationships (Ziegler and Lausen, 2005). A global trust metric is computed based on the opinion of all the peers in the network. For example, computing the global trust metric of SpazaShop A from Figure 3.4 would require a collection of opinions from all the other peers in the network across all communities. This opinion is then assigned to SpazaShop A giving it a global trust metric.

A disadvantage of using a global trust metric is that the entire network must be known and all opinions stored in order to compute the global trust metric, making the computation expensive. Also, this type of trust metric is less personal, since it is based on the opinion of the complete network. However, this approach is simpler than a local trust metric because a single centralised entity is responsible for collecting and storing the opinions of all other peers. Peers would therefore know exactly where to retrieve the global trust metric for another peer in the network.

b) Local trust metrics

On the other hand, when computing trust and reputation in the local community or neighbourhood, only the local network needs to be explored. For example, community network w in Figure 3.4, surrounding SpazaShop A, is the local community or network. Here, only the opinions of the members of this community are needed for a reputation computation. Such local trust metrics are subjective as they are personalised and their computation scales well (Ziegler and Lausen, 2005). Should SpazaShop A, in Figure 3.4, wish to calculate the local trust metric for Supplier A, it would rely on its own experience as well as the experience of those peers it is connected to, who have previously collaborated with Supplier A, such as SpazaShop F.

Local trust metrics operate on partial trust network information defined by personalized webs of trust, where only neighbour links and their direct links are explored to a set of nodes reachable through these relationships (Ziegler and Lausen, 2005). Merging these local trust web networks give a more global trust network. To achieve this, peers have to concatenate their local network with the local network of neighbouring peers to which they are connected.

The disadvantage of using local trust metrics is that peers may find it challenging or impossible to obtain the trust metric of a node to which they are not directly connected. For example, should SpazaShop A wish to determine the trust metric of Supplier B it would require access to a peer connected to Supplier B, such as SpazaShop K, in Figure 3.4. This makes use of
the transitive property of trust, to determine the trust metric for Supplier B through recommendations for neighbouring peers and their neighbour’s neighbours and so on.

The nature of digital business ecosystems therefore dictate that local trust metrics should be preferred because of its decentralized P2P architecture (Isherwood and Coetzee, 2011, Massa and Avesani, 2005, Ziegler and Lausen, 2005). A digital business ecosystem agent forms a subjective opinion on participants it interacts with based on the computation it performs. In order to perform a trust and reputation computation, an architecture for computation needs to be identified that complements the digital business ecosystem. The types of architecture for trust and reputation are discussed in the next section.

3.4.3 Architectures for trust and reputation computation

Approaches to trust and reputation computation are generally classified as centralised or decentralised (Ziegler and Lausen, 2005). More recently, hybrid approaches (Wang et al., 2010) accommodate the difficulties of decentralised reputation systems. These computation approaches will be discussed next, in relation to the digital business ecosystem.

a) Centralised architectures

Centralised trust and reputation systems are found in existing e-commerce applications, for example, eBay (Despotovic, 2005). A central entity is responsible for collecting ratings from all entities involved in a transaction. The reputation of users is global and public and is computed by the system.

The advantage of this approach is that there is less communication required between users, since there is only one node, the central entity, which needs to be queried. The disadvantage is that there is a single point of failure and computation may be expensive depending on the number of peers in the network.

b) Decentralised architectures

In decentralised trust and reputation systems, agents represent users or enterprises. There is no central entity for agents to share their ratings with each other and no global or public reputation exists (Despotovic, 2005). For example, when a SpazaShop A, in Figure 3.4 wants to find out the reputation of a Supplier A, its agent has to ask other agents for their ratings about Supplier A, including those of SpazaShop A’s friends or the friends of friends. These ratings are then combined by the agent of SpazaShop A to determine the reputation of Supplier A.
The advantage of the decentralised architecture is that ratings are more personalised, making it possible for peers to make a more accurate trusting decision. The disadvantage is that a large volume of communication exists between agents, making it more complex to determine trust metrics for agents far away in the network.

c) Hybrid architectures
Recent work introduced a super-agent based mechanism (Wang et al., 2010), inspired from super-peer networks, for reputation management. This approach attempts to solve the inefficiency problem of a decentralised trust and reputation system. Now, an agent with poor capabilities will not be able to cause system blockages as in a true decentralised approach.

Super-agents are agents in the ecosystem that have greater capabilities than other agents. They operate as normal agents but have the added tasks of collecting and storing feedback about services, building reputation for services, and sharing reputation information with other agents. Super-agents can form communities of agents that have similar interests and judging criteria, creating cohesive groups that provide more accurate reputation information. The super-agent of a community therefore collects, stores, builds and shares a community based reputation with other agents.

The advantage of this approach is that it removes the extensive communication challenges that arise in decentralised approaches. It also reduces the significance of a single point of failure issue faced by centralised systems, since more peers maintain reputation information.

d) Motivation for the architecture of the digital business ecosystem
Centralised network architectures are not well-suited to properties of a digital business ecosystem such as open environment, decentralisation, scalability, robustness, and self-organisation. A central entity would have to maintain information for the entire network which limits scalability and robustness. The central entity is a single point of failure which affects the networks robustness. In a trust and reputation environment, the central entity in charge stores the reputation graph and related information. If the central entity is not available, trust and reputation information cannot be sourced.

Decentralised P2P network architectures are more suited to the properties of a digital business ecosystem. Some difficulties are that agents may not know which other agents have interacted with this agent for whom they are trying to build reputation. Also, agents are not always available at all times. If they are offline, their ratings about other agents are not
available at the time of request. Trust and reputation systems need to address these issues in order to be useful in centralised and decentralised environments.

Hybrid architectures address the disadvantages of both the centralised and decentralised architectures. By having a peer acting as the “manager” of a small group of other peers, it is easier to control this group and for other peers to request information from the “manager” peer. The computation is also less intensive than in the centralised approach since only a small graph needs to be stored by the “manager” peer. The challenge with the hybrid approach is that there may not be any peers that have the capabilities to be a “manager” peer. Also, in the digital business ecosystem, businesses might not want other businesses to maintain all the information about them and have it stored at their virtual premise. The hybrid approach may be more useful when considering social network information where highly reputable members can be identified to take the role of super-agents to assist other members in the community (Isherwood and Coetzee, 2011).

In the next section, the different approaches to computing the trust metric are discussed.

### 3.4.4 Approaches to trust computation

Trust and reputation systems generally consider personal experience as well as the experience of other peers in the network when determining the trust metric for another peer. In literature, there are various approaches to computing the trust metric. Trust and reputation systems use the approach most suited to their architecture, environment, and use case. A survey on trust and reputation systems for online service provision by Jøsang et al. (2007) summaries the different approaches to trust computation. The most common approaches are discussed in this section.

#### i. Simple summation

This approach simply sums all the positive ratings for a peer and minuses the sum of all the negative ratings for a peer to determine the trust metric of a peer (Jøsang et al., 2007). More advanced versions of this approach are used by web sites such as Amazon (Amazon, 2013). Here the trust metric is computed as the average of all the ratings for a peer. Further advances to this approach are also used, whereby weights are assigned to different factors such as the age of the rating, the distance between previous ratings and the current rating, and the trust rating for the peer providing the rating (Jøsang et al., 2007).
ii. Discrete trust model

Discrete trust models make use of discrete verbal statements to measure the trust metric for a peer because humans are better able to understand and rate performance according to verbal statements (Jøsang et al., 2007, Abdul-Rahman and Hailes, 1998, Cahill et al., 2003, Carbone et al., 2003). For example, Abdul-Rahman and Hailes (2000) uses discrete verbal statements such as: very trustworthy, trustworthy, untrustworthy, and very untrustworthy. However, the challenge with such an approach is that these measures do not lend themselves naturally to sound computational principals, and require the use of look-up tables which have computational costs (Jøsang et al., 2007).

iii. Bayesian systems

Another approach to trust and reputation computation is the Bayesian systems approach. Here, the system takes a binary rating as input and computes a reputation metric by updating of beta probability density functions (PDF). The reputation metric is represented in the form of the beta PDF parameter tuple \((\alpha, \beta)\) where \(\alpha\) is the amount of positive ratings, and \(\beta\) is the amount of negative ratings (Jøsang et al., 2007, Mui et al., 2002). Although this approach provides a sounds basis for computing reputation metrics, it might be complex for the average person to interpret.

iv. Fuzzy models

Some trust and reputation systems such as REGRET (Sabater and Sierra, 2001) represent trust and reputation as linguistically fuzzy concepts. Membership functions are used to describe an agent, such as trustworthy or not trustworthy. Fuzzy logic therefore provides rules for reasoning with fuzzy measures (Jøsang et al., 2007). However, as with Bayesian systems, fuzzy measures are not always easy to interpret and require extensive fine-tuning to ensure the correct measures are selected (Padak, 2005).

v. Flow models

Flow models are systems that compute trust and reputation by transitive iteration through arbitrarily long or looped chains (Jøsang et al., 2007). Some trust and reputation models provide a weight for trust and reputation which remains constant among the community and its members. Google’s PageRank algorithm (Page et al., 1999) makes use of a flow model. Here, a participant’s reputation increases as a function of incoming flow, and decreases as a function of outgoing flow. There are other trust and reputation systems such as the EigenTrust model (Kamvar et al., 2003) which calculates an aggregation of trust scores along transitive chains until all members in the community converge to stable values.
The most applicable trust computation for a digital business ecosystem at this stage of the research is possibly an advanced version of a simple summation, whereby weightings are assigned to different factors making up the trust metric. This allows for different factors to be considered and their weightings adjusted according to the requirements of the digital business ecosystem.

The next sections focuses on evaluating trust and reputation systems so as to select an appropriate one for the digital business ecosystem.

3.5 A comparison of relevant trust and reputation systems

Many trust and reputation systems exist to address different types of requirements when predicting the trustworthiness of peers in a network (Noorian and Ulieru, 2010, Jøsang et al., 2007, Mármol and Pérez, 2011). In this section, several trust and reputation systems are investigated and evaluated to determine their potential use for a digital business ecosystem environment for SMMEs. It is important to note here that the focus of this research is not to create a completely new trust and reputation model, but to extend a relevant trust model to support cultural behaviour.

Firstly, trust and reputation systems are discussed followed by evaluation criteria for selecting a trust and reputation system for the digital business ecosystem. This is followed by a discussion on the 4 potential trust and reputation system, namely: REGRET, TRAVOS, PeerTrust, and PowerTrust. Finally the trust and reputation systems are evaluated and a system is selected for the digital business ecosystem.

3.5.1 Trust and reputation systems

Trust and reputation systems are developed to predict the trustworthiness and proficiency of a peer’s behaviour in the future, based on how they have behaved in the past (Noorian and Ulieru, 2010, Ruohomaa et al., 2007). Figure 3.5, from Mármol and Pérez (2011), depicts the general components and process of trust and reputation systems indicating how they achieve the goal of predicting a peer’s behaviour. These five components and processes are agreed upon by many authors who have completed comparisons of trust and reputation systems (Mármol and Pérez, 2010, Marti and García-Molina, 2006).
1. Gathering information involves collecting information about the behaviour of entities in the system.
2. Scoring and ranking entails calculating the trust and reputation values for potential collaboration entities.
3. Once entities are ranked, a selection is made.
4. Then a transaction is conducted.
5. Based on the behaviour of entities in a transaction, they are either rewarded or punished.

The next section provides evaluation criteria for a trust and reputation system for the digital business ecosystem.

3.5.2 Evaluation criteria for trust and reputations systems for the digital business ecosystem

In literature, there are several comparisons of trust and reputation systems (Jøsang et al., 2007, Mármol and Pérez, 2011, Mármol and Pérez, 2010, Noorian and Ulieru, 2010). This section does not aim to redo the extensive comparison of trust and reputation models and systems but rather to investigate and evaluate trust and reputation systems that can be appropriate for a digital business ecosystem for Africa.
Based on the five properties of a digital business ecosystem identified in Chapter 2, and the three requirements for a digital business ecosystem to support collaboration among SMMEs, the following evaluation criteria are defined:

i. does it support an open environment
The trust and reputation system should be implementable over unstable networks such as the Internet. Since the trust and reputation systems used for the digital business ecosystem is to be implemented on top of a P2P overlay network, this requirement is satisfied by the overlay network. The trust and reputation system should however allow for a diverse range of peers, from different locations, to join and leave the network at any time.

ii. does it support a decentralised or hybrid architecture
The trust and reputation system should support a decentralised P2P architecture. This implies that no single peer should be made responsible for maintaining the reputation metrics of the entire network.

iii. does it support scalability
The trust and reputation system should be able to handle a large number of peers, transactions, services, and requests as the new peers join the network.

iv. does it support robustness
The trust and reputation system should not fail if there are errors in the system. Since P2P systems do not rely on a single peer and therefore no single point of failure within the network, this requirement is satisfied by the P2P overlay network. However, the trust and reputation system should guard against malicious peers within the network, ensuring that they do not disrupt the other peers in the network.

v. does it support self-organisation
The trust and reputation system should adapt to changes in the environment as nodes join and leave the network. Peers should be aware of neighbouring peers who are no longer accessible so that they do not attempt to retrieve information from them. Also, malicious nodes should be removed from the network or suspended from collaborating with other nodes.

vi. can it be implemented using a combination of mobile and cloud technology
The trust and reputation system should support the use of mobile devices as nodes and make use of cloud technology to support collaboration among nodes.
vii. does it support trust and reputation in a decentralised architecture
The trust and reputation system should specifically support trust and reputation in a decentralised architecture. Therefore, peers need to compute trust with a limited view of the network. Satisfying many of the previous requirements will result in the satisfaction of this requirement due to their decentralised relevance.

viii. does it have the ability to comply to cultural beliefs and behaviours of participants
The trust and reputation system should be flexible in its computation so that parameters relating to a peer's culture and behaviour can be included as input parameters into the trust calculation such as social information metrics.

The evaluation criteria discussed previously is used as guideline for selecting an appropriate trust and reputation system. That is to say, there might be no trust and reputation system that satisfies the criteria set out above, but the trust and reputation system that satisfies the most criteria may be selected. The next section will discussed the different trust and reputation systems to be evaluated.

3.5.3 A comparison of trust and reputation systems for the digital business ecosystem

The four trust and reputation systems to be discussed and evaluated are: REGRET (Sabater and Sierra, 2001), TRAVOS (Teacy et al., 2006), PeerTrust (Xiong and Liu, 2004), and PowerTrust (Zhou and Hwang, 2007). These systems have been selected for discussion and evaluation since they are among some of the most well-referenced models for P2P systems.

The author believes that the most appropriate and respectable trust and reputation system needs to be selected to be the foundation of the trust and reputation system proposed for the digital business ecosystem for rural Africa. The selected trust and reputation systems are now discussed.

a) REGRET
REGRET is a trust and reputation system for decentralised e-commerce environments where emphasis is placed on the agent's social structure (Sabater and Sierra, 2001). REGRET models social relationships on a graph (sociogram) where nodes are agents and edges denote the nature of the relationship such as competition, cooperation, and trade. This trust and reputation system is based on a 3 dimensional reputation model (Sabater and Sierra, 2001, Noorinan and Ulieru, 2010):
i. Individual dimension (subjective reputation) – The trust is calculated based on direct experience between two agents, and the result is prioritised according to the recency of interaction.

ii. Social dimension – This dimension indicates the trustworthiness of an agent in cases where direct experiences are inefficient, or the agent is new to the network. This dimension is further specialised into 3 types of reputation based on information source:
   a) Witness reputation – this represents the reputation from witnesses who are adjacent to the agent.
   b) Neighbourhood reputation – this represents the measure of reputation of individuals who are neighbours to the agent being considered.
   c) System reputation – this evaluates the trustworthiness of an agent based on the general role they play in the sociogram.

iii. Ontological dimension – The dimension provides the possibility of combining different aspects of reputation to make up a complex one.

The REGRET system has a reliability measure which reflects the confidence level of the calculated reputation value. This is calculated according to the number of available impressions and variability of the impression values. Also, due to the social relationship nature of REGRET, it contains an intimacy value which indicates the number of impression required to consider the relationship as a close relationship (Sabater and Sierra, 2001).

The main feature of the REGRET system is that it uses social relationships to determine the trustworthiness of nodes, but this feature makes it less supportive of the dynamic nature of an open environment (Noorian and Ulieru, 2010). As nodes join and leave the network, the population of the participants varies over time, making it challenging to keep track of the sociogram. Additionally, the node's behaviour can change over time, further adding to the dynamic nature of open systems. This also impacts the scalability and robustness of the network as the social relationships may rely on nodes that are no longer present in the sociogram. The system also assumes that each agent owns a predefined sociogram (Sabater and Sierra, 2001) but does not address the issue of locating witnesses in the social network (Noorian and Ulieru, 2010) making it challenging to collect the information required to perform the trust evaluation.

REGRET has the advantage of being able to support multiple-criterion rating, thereby enabling each participant to design an ontological structure of the contract which is adapted to its own requirements (Noorian and Ulieru, 2010, Sabater and Sierra, 2001, Jøsang et al., 2007). This feature leads to more precise predictions of the reputation value by addressing the criteria
similarity rate factor among nodes that have different criteria for determining and evaluating reputation. This has a positive influence on the robustness, as nodes have more relevant criteria and can therefore perform more accurate evaluations, potentially leading to more successful transactions.

Using social relationships provides advantages for new nodes who join the network and take part in the communities activities (Noorian and Ulieru, 2010, Sabater and Sierra, 2005). They can use this approach to improve their knowledge and enhance their social status. This characteristic addresses the issue of bootstrapping a trust value to a newly joining node in the network.

b) TRAVOS

The TRAVOS (Trust and Reputation model for Agent-based Virtual Organisations) system was designed and developed for large open systems (Teacy et al., 2006). This model exploits two information sources when determining the trustworthiness of agents:

i. Direct Interaction – this refers to the opinion of an agent based on their previous direct interaction with an agent.

ii. Witness Observation – this refers to the rating provided by others who have interacted with a particular agent.

This model relies heavily on direct interaction as a source. It only uses opinions of others if they are really necessary. It uses a confidence metric to determine if the agents direct experiences are sufficient enough to provide a reliable judgement for a particular agent (Noorian and Ulieru, 2010). If the confidence metric is not within the threshold, it sends out queries to collect information, about an agent, from other agents (witnesses) who claim to have had experience with this particular agent.

When judging the witnesses, this model uses an exogenous approach. This implies that witnesses are judged on the perceived accuracy of its past opinions. This is in contrast to an endogenous approach which refers to judging a witness according to the difference in opinion from that of the mainstream opinions about a node. This is achieved in two steps (Teacy et al., 2006):

- Firstly, the probability that a particular correspondent will provide an accurate report given its past opinions is determined.
- Secondly, based on the above value, the distance between a witness’s opinion and the prior belief that all likely values for an agent’s behaviour are equally probable, is reduced.

Through these two steps, the influence that a witness has on a truster’s assessment of a trustee is reduced if the witness’s opinion is consistently biased in a negative or positive way.

The TRAVOS model is incomplete in the sense that it considers virtual organisations as social structures, but does not extract any social data from the relationships that exist both between virtual organisations and virtual organisations and their members. According to (Teacy et al., 2006), such information would be useful for bootstrapping new nodes, joining the network, with trust values and also improve the accuracy of the trust assessments.

c) PeerTrust

The PeerTrust model is tailored for P2P e-commerce communities where the trustworthiness of peers is based on transaction-based feedback (Xiong and Liu, 2004). This model is designed for and implementable over a decentralised P2P network. To assess and quantify peer’s trust value, the PeerTrust model customises five common factors (Noorian and Ulieru, 2010, Xiong and Liu, 2004):

1. Transaction feedback – This is the feedback a peer obtains from another peer after a transaction has occurred.
2. Feedback scope – This is the total number of transaction the peer experienced with other peers.
3. Credibility – This is used to evaluate the honesty of feedback sources.
4. Transaction context factor – This uses the context of the transaction such as time, size and type to determine its weighting.
5. Community context factor – This is the reward function to encourage honest feedback from peers.

From an implementation perspective, this model provides each peer with a trust manager, small database, and a data locator (Xiong and Liu, 2004). The trust manager is responsible for the submission of feedback and the trust evaluation. The small database stores a portion of the global trust data that is required for trust evaluation. The data locator is responsible for the placement and location of trust data over the distributed P2P network. This setup ensures that the PeerTrust model is scalable, as each peer should be capable of only handling their own instance of the trust manager, small database, and data locator.
The PeerTrust model provides a mechanism to deal with various attacks such as collusions of malicious nodes and ballot stuffing where malicious nodes essentially form cooperatives to improve their own reputation (Noorian and Ulieru, 2010). Through the notion of the credibility factor, where a node’s credibility factor has an influence on their trust evaluation, the PeerTrust model develops a defence mechanism to guard against such attacks, thereby ensuring the robustness of the network.

The factors considered in the trust evaluation for the PeerTrust model addresses the self-organising issue relating the digital business ecosystem requirement to a certain extent. These factors ensure that malicious nodes do not gain controlling power within the network thereby limiting their growth and collaboration opportunities. However, there is no mechanism to remove malicious nodes from the network or to stop them from joining under a new alias. This gives malicious nodes a limited time interval for which they could take advantage before the system deals with them accordingly. This point leads to the issue which is generally challenging to address in trust and reputation systems i.e. the bootstrapping of newly joining peers with an appropriate trust value. This issue is not addressed in the PeerTrust model as nodes that join the network are given a default trust value specified by the system implementation (Xiong and Liu, 2004, Noorian and Ulieru, 2010).

d) PowerTrust

PowerTrust is a robust and scalable P2P reputation system that uses a trust overlay network to model trust relationships among peers. It also leverages on the power-law feedback characteristic (Zhou and Hwang, 2007) to facilitate trust and reputation in P2P networks. This system uses a distributed ranking mechanism to dynamically identify and select a few power nodes in the system. Power nodes are nodes that have become the most reputable in the network. They have the highest feedback in the system and can easily be replaced if they become less active or demonstrate unacceptable behaviour.

The PowerTrust system is composed of five functional modules (Zhou and Hwang, 2007):

i. Initial Reputation Aggregation – This module performs the initial round of global reputation aggregation where each node sends all local trust scores the score managers.

ii. Look-ahead Random Walk – This module is used to update the reputation score, periodically.

iii. Distributed Ranking Module – This module is used to identify the power nodes dynamically by working together with the Look-ahead Random Walk module.
iv. Regular Random Walk – This module provides support to the Initial Reputation Aggregation module.

v. Reputation Updating – This module is responsible for updating the reputation scores as peers leave and join the network.

The PowerTrust system uses the look-ahead random walk strategy and the power nodes to aggregate user’s feedback and compute the global reputation scores for each peer (Mármol and Pérez, 2011, Zhou and Hwang, 2007). Also, all peers send local trust scores among themselves when transactions take place. Using this technique as well as using the power nodes to update the global reputation scores, the PowerTrust system achieves high robustness and scalability and is capable of supporting large-scale P2P applications (Mármol and Pérez, 2011).

The set of power nodes in the PowerTrust model are continuously updated which enables the system to be resilient against dynamic behaviour of peers in a P2P network. Each node also has a score manager that accumulates its global reputation. According to Mármol and Pérez (2011), who did a comprehensive evaluation of trust and reputation models, PowerTrust is the first reputation system that is able to reliably deal with the dynamic behaviour of P2P systems. It enables self-organisation within the network since it adapts to nodes leaving and joining the network continuously thereby enhancing the robustness of the network.

e) Summary of trust systems evaluated

Having discussed these four systems, it can be seen that in general, all are capable of providing a trust and reputation environment for the digital business ecosystem due to their support for P2P networks. However, some are more relevant than others. Table 3.1 provides a summary of the extent to which each trust and reputation system supports the predefined criteria. The following measurements are used for comparison: low, medium, high. These measurements are compared relative to the other models discussed so that they are compared among themselves, since that is the purpose of the evaluation.
Table 3.1 Trust and reputation system evaluation summary

<table>
<thead>
<tr>
<th></th>
<th>REGRET</th>
<th>TRAVOS</th>
<th>PeerTrust</th>
<th>PowerTrust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open-environment</td>
<td>Low</td>
<td>High</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Decentralised/hybrid architecture</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Scalability</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Robustness</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Self-organisation</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Mobile and cloud</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Decentralised trust and reputation</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Cultural support</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

All of the discussed systems achieve a high result for supporting business opportunities and growth. The main purpose of all these systems is to provide an environment where peers can successfully collaborate with each other. For these systems to support business opportunities and growth they need to be implemented in the correct environment, for which they are suited. Therefore, it is beyond the scope of the discussed systems to provide business opportunities and growth, but rather to provide an environment where successful collaborations can occur and then be used in the appropriate business environment.

The REGRET system has poor performance, relative to the other models, in distributed P2P environments. This is due to the implementation of the social graph which represents the P2P network. The social graph is tightly coupled with the nodes in the network making it less susceptible to the dynamic nature of a P2P environment. Also, nodes are depended on other nodes social graphs so that when nodes leave and join the network, the social graph might not be completely up to date thereby influencing the robustness of the network. Therefore, REGRET has the ability to support cultural extensions to its algorithm but lacks in terms of performance.
The TRAVOS system performs well in large open environment. However, it lacks in flexibility since it relies heavily on its two parameters for evaluating trust, making it challenging to include new parameters. Also, it does not take advantage of the social structures which it considers within the network. Therefore, TRAVOS does not support the cultural behaviour requirement.

The PeerTrust system performs very well and but does not take social network information into account. However, due to its support for decentralised architecture and self-organisation, it provides a good platform on which to implement social graph information from a local network perspective. Also, the input parameters defined in the PeerTrust model are flexible in the sense that these can be replaced with other values and parameters can be added with different weightings assigned to them. Therefore, PeerTrust has a greater support for including cultural behaviour and satisfying the needs of the digital business ecosystem.

Lastly, the PowerTrust system performs very well in decentralised P2P environments, however, it does not efficiently use social network information. Additionally, its input parameters are also tightly coupled to the system without much flexibility. This limits its extension in terms of being useful for the consideration of additional cultural input parameters.

3.5.4 A trust and reputation system for the digital business ecosystem for Africa

The PeerTrust system and the PowerTrust system are the two most relevant systems based on the evaluation. For the purpose of the study, the PeerTrust system is selected because of the following reasons:

i. It has high support for the properties required by a P2P system such as the digital business ecosystem. This includes support for open-environments, decentralised architecture, scalability, robustness, and self-organisation.

ii. It has a high support for mobile and cloud infrastructure since each node (mobile device) maintains its own system which could be hosted on the device or on a cloud platform.

iii. It is specifically designed to support trust and reputation in a decentralised architecture.

iv. The trust and reputation computation supports five factors such as transaction feedback, credibility, community and transaction context, which are relevant to the operation of peers in a digital business ecosystem environment.

v. It provides flexibility in its trust calculation so that parameters based on cultural properties can be included, therefore providing support for cultural behaviour.

The next section provides a more in-depth explanation of the PeerTrust system.
3.6 PeerTrust system for the digital business ecosystem

This section provides more details on the system architecture of PeerTrust, and discusses how PeerTrust can be extended to address trust and reputation for the digital business ecosystem for Africa.

3.6.1 PeerTrust system

The PeerTrust model (Xiong and Liu, 2004) is proven to be the most relevant model on which to build a trust and reputation system for the digital business ecosystem. The system architecture of the PeerTrust model is truly adapted to decentralised P2P environments and provides good support for robustness, scalability, and self-organisation. Figure 3.6 depicts the system architecture of the PeerTrust model as presented by Xiong and Liu (2004). In the PeerTrust system architecture, peers are represented as agents. There are five peers, each with their own computational ability.

![Figure 3.6 PeerTrust system architecture](image)
The components of each agent are shown in the block on the right namely a Trust Manager, Data Locator, and Trust Data. These components are now discussed.

**a) Trust Manager**

The Trust Manager has two main functions (Xiong and Liu, 2004):

i. Submit feedback from a transaction to other peers in the network, through the Data Locator. This is handled by the Feedback Submission module.

ii. Evaluate the trustworthiness of another peer according to the PeerTrust trust computation. This is handled by the Trust Evaluation module.

To evaluation the trustworthiness of another peer, the PeerTrust system performs the following two steps (Xiong and Liu, 2004):

i. Trust data about the target peer is collected by the Data Locator.

ii. This data is used by the Trust Evaluation module to perform a trust computation. This result is then used to evaluate if a user is trustworthy or not.

The process clearly illustrates that the PeerTrust system is decentralised, since each node can determine the trustworthiness of another node without relying on central entity. The trust data is obtained from other peers each time a peer is evaluated. This enforces the dynamic and reliable nature of the system since up-to-date evaluations are performed.

**b) Data Locator**

The Data Locator is responsible for inserting, updating, and accessing trust data, either locally at the agent, or remotely at other agents. There are a number of data placement schemes which can be used to achieve this (Xiong and Liu, 2004), such as CAN (Ratnasamy et al., 2001), Pastry (Rowstron and Druschel, 2001), Chord (Stoica et al., 2001), and P-Grid (Aberer, 2001). The PeerTrust system makes use of the P-Grid approach which uses a distributed hash table (DHT) to map keys into points in a logical coordinate space (Aberer, 2001).

The trust data about a peer is stored at designated peers which can be located by hashing a unique ID of that peer to a data key. Figure 3.7, which is directly taken from Xiong and Liu (2004), depicts the Data Locator of the PeerTrust system. Each peer is responsible for multiple keys and for maintaining a routing table so that other keys can be located in the network. For example, in Figure 3.7, the routing table for peer \( P_1 \) has a routing key 001 and can route to peer \( P_6 \) and \( P_3 \). A peer that receives a request to update a key for which they are not
responsible for, will simply forward this request to another peer based on the routing table. This example is depicted in Figure 3.7, where $P_2$ is queried for key 110.

![Figure 3.7 PeerTrust DataLocator with routing tables](image)

c) Trust Data

The Trust Data database is responsible for storing the feedback information about the peer for which it is associated. Each piece of feedback contains the following information (Xiong and Liu, 2004):

i. ID of the peer, as the data key.
ii. Timestamp or counter of the transaction.
iii. Feedback for the transaction.
iv. ID of the peer who provided the feedback.
v. Any other applicable transaction contexts.

This data is used in the trust computation to evaluate the trust worthiness of a target peer. The storage cost involved at each peer is proportional to the amount of history that gets stored as well as the degree of replication.

The Trust Manager, Data Locator, and Trust Data stored at each peer make up the system architecture of the PeerTrust model. This approach ensures the network remains dynamic and decentralised making it very relevant to P2P networks. The next section discusses the PeerTrust algorithm and how the PeerTrust model uses trust and reputation.
3.6.2 PeerTrust algorithm

To calculate the trust level of another peer in a P2P environment the trust level computation is performed by the Trust Evaluation component. The formula for computing the trust level of a peer is defined in Equation 1:

\[
T_l(u) = \alpha \sum_{i=1}^{I(u)} S(u,i) \cdot Cr(p(u,i)) \cdot TF(u,i) + \beta \cdot CF(u)
\]  
(Equation 1)

The parameters of Equation 1 are as follows (Xiong and Liu, 2004):

- \(T_l(u)\) – The trust level of a peer \(u\).
- \(I(u)\) – The total number of transactions performed by peer \(u\) with all other peers.
- \(p(u,i)\) – The other participating peer in peer \(u\)’s \(i\)’th transactions
- \(S(u,i)\) – The normalised transaction feedback peer \(u\) receives from \(p(u,i)\) in its \(i\)’th transaction.
- \(Cr(p(u,i))\) – The credibility of the transaction feedback submitted by peer \(p(u,i)\).
- \(TF(u,i)\) – The adaptive transaction context factor for peer \(u\)’s \(i\)’th transaction.
- \(CF(u)\) – The adaptive community context factor for peer \(u\)
- \(\alpha\) and \(\beta\) denote the normalised weight factors for the collective evaluation, and community context factor, respectively.

This formula is used to calculate the trust level \((T_l)\) of peer \(u\) and is calculated by peer \(u\)’s agent. Equation 1 is the core trust level computation and provides peers with an indication of how much trust they can assign to another peer.

Suppose a peer, \(w\) in the P2P network, would like to transact, there are a number of steps that would occur in the PeerTrust model to facilitate the transaction. These steps are as follows:

1. **Specify the service required**

   Peer \(w\) first decides which service it would require, for example sharing a document.

2. **Identify peers in the network that offer the specified service**

   Peer \(w\) then asks its connections who will ask their connections, and so on, until a peer or peers can be recommended. A peer that is connected to a peer offering the desired service provides feedback. The recommending peer is known as \(p(u,i)\) and the peer being recommended is known as \(u\). The feedback provided by \(p(u,i)\) is represented as \(S(u,i)\). All this information is collected by the Data Locator of peer \(w\).
3. Select a peer to transact with
At this stage, peer w’s Trust Manager can compute the trust level of peer u according to equation 1 and the information retrieved. The peer with the highest trust level, out of the all the recommended peers, is selected for the transaction.

4. Establish a transaction and transact
Peer w and the selected peer u proceed to transact with each other and the performance of each peer is stored.

5. Provide feedback based on the transaction
Peer w and peer u provide a feedback rating based on the characteristics and performance of the other peer during a transaction.

6. Update the network
In terms of the P2P network, a connection is now created from peer w to u, if no connection exists. The Data Locator stores the results of the transaction using the Trust Data storage. Therefore, next time peer w requires the same service; it will have the possibility of making a decision based on previous experience, for the selected peer.

This steps form the foundation of transacting in a P2P environment using the PeerTrust model. The next section discusses how this architecture can be used and extended for the trust and reputation system for the digital business ecosystem.

3.6.3 Trust and reputation for the digital business ecosystem
Each SMME in the digital business ecosystem is represented by an agent consisting of a Trust Manager, Trust Data, and a Data Locator, making it more scalable for the digital business ecosystem. A mobile device could represent the agent, and the Trust Manager, Trust Data, and Data Locator can be stored on the mobile device if such capacity is available, or on the cloud.

Extending the PeerTrust model by adding a social network component to the Trust Manager can support the use of social network information for trust computations. The TrustEvaluation module of the Trust Manager can be updated with cultural property parameters to extend the trust calculation.

Therefore, trust and reputation system for the digital business ecosystem has the following features:
Trust and reputation for digital business ecosystems

- Provides a P2P overlay network for the digital business ecosystem.
- Facilitates collaborations among SMMEs and other members of the digital business ecosystem.
- Provides trust and reputation data for SMMEs based on PeerTrust computations.
- Extend PeerTrust computation with cultural properties and social network information.

The PeerTrust model thus provides a concrete trust and reputation model foundation on which to extend and use for trust and reputation in the digital business ecosystem.

3.7 Conclusion

In this chapter, the different definitions of trust were presented along with the trust properties and trust constructs which make up trusting behaviour. These constructs were discussed in the context of e-commerce, so as to show its relevance to the digital business ecosystem.

Reputation was discussed next, indicating its difference and relation to trust. It was shown that reputation can benefit the digital business ecosystem from two perspectives, namely: and individual perspective, and a collective perspective.

The approach to trust and reputation was also discussed so that the appropriate approach can be considered for the digital business ecosystem environment. This included the identification of trust metrics, the scope of such metrics, architecture of trust and reputation systems, and computational approaches to trust and reputation systems.

Trust and reputation systems were then introduced and the general components of such systems were described. Next, evaluation criteria was defined, relating to the digital business ecosystem, culture, and social position. This was used to evaluate four trust and reputation systems, namely: REGRET, TRAVOS, PeerTrust, and PowerTrust. These models were evaluated and discussed resulting in the selection of the PeerTrust system being selected.

An in-depth discussion of the PeerTrust system architecture provided an indication of how this system can be used and extended for trust and reputation in the digital business ecosystem for Africa. It was concluded that PeerTrust system would be the foundation for the trust and reputation system for the digital business ecosystem for Africa.
Finally, trust properties were derived from the definition of trust and social aspects of trust, and are the basis on which trust can be modelled. Trust and reputation systems implement these properties to facilitate a trust and reputation environment.

For the digital business ecosystem in Africa, culture has an impact on trust and therefore has an effect on trust properties, constructs leading to trusting behaviour, and the implementation of trust and reputation systems. For this reason, the cultural influence on trust and reputation is explored in the next chapter.
Chapter 4

The influence of culture on trust and reputation

4.1 Introduction

In developed economies that exhibit high levels of industrialisation and living standards, as well as widespread infrastructure, collaborating and trading online has become something of a norm. Online e-commerce environments such as eBay (eBay, 2012) are highly successful as they implement well-accepted and understood trust mechanisms to provide secure online trading. These mechanisms include institutional guarantees, laws and policies, information security mechanisms, and social controls (eBay, 2012) to assist individuals and small businesses who trade online. Users of such systems are generally very familiar with online trading and collaborating with others online, and therefore have trust in such online systems.

To date, owners of very small enterprises (VSEs) in Africa, such as spaza shops, lack the necessary understanding and awareness of how they can be protected against possible risks when conducting online trading and collaboration. Sophisticated mechanisms have little meaning to them, as they are not accustomed to technology. They prefer to rely on personal relationships established through regular face-to-face interactions to create trust between themselves and their collaboration partners. This creates a challenge for the adoption of technology for very small enterprises in the digital business ecosystem in Africa. Facilitating trust in e-business solutions is therefore extremely important to ensure its success.

There are real differences between the environment and cultures of Africa, and the residents of developed economies in the Western world (Doney et al., 1998, Zaheer and Zaheer, 2006, Chong, 2003, Botha, 2007, Isherwood et al., 2012). The trust mechanisms used by online transaction tools and e-commerce environments, such as eBay, may not be entirely relevant to e-commerce consumers of emerging economies (Sia et al., 2009), particularly in rural areas where VSEs generally operate (Isherwood et al., 2012). Each culture has different norms and values which influence beliefs and, in turn, the decision of who to trust (Doney et al., 1998, Lane, 1997, Sia et al., 2009).

In Africa, the collectivist culture is most common. In many areas VSEs conduct business and make trusting decisions according to their cultural norms (Botha, 2007, Cramer, 2010).
digital business ecosystem for Africa deals specifically with SMMEs, particularly VSEs, in Africa and should therefore consider the collectivist cultural approach to trust, when implementing a trust and reputation system.

In this chapter, the influence of culture on trust and reputation is discussed. The following section provides a definition for culture and introduces individualist and collectivist cultures. The influence that culture has on trust is discussed using a use case scenario for both individualist and collectivist cultures. Collectivist cultures are discussed further, providing a deeper insight on how their behaviour affects the development of trust. Four trust and reputation properties for collectivist cultures are proposed, to be used by the trust and reputation component of the digital business ecosystem for Africa. Finally, the chapter is concluded.

### 4.2 Culture

Culture and its dimensions, as proposed by Hofstede, are now presented and explained. These dimensions are used to assist in differentiating between cultures. Individualist and collectivist cultures are then introduced.

**a) Definition for culture**

For the purpose of this research, the definition of culture by Hofstede (1980) is used:

```
Culture - “the collective programming of the mind that distinguishes the members of one group or category of people from another”.
```

Hofstede (1980) identified five dimensions of culture that were developed following a survey of 72 countries, these are:

i. power distance
ii. collectivism vs. individualism
iii. femininity vs. masculinity
iv. uncertainty avoidance
v. long-term vs. short-term orientation.

These dimensions are discussed next.
The influence of culture on trust and reputation

b) Dimensions of culture
Hofstede’s dimensions of culture have formed the basis of much work relating to culture and are considered useful when differentiating between cultures. The five dimensions are explained as follows (Hofstede, 1980, Hofstede et al., 1991):

i. Power distance
Power distance refers to the degree of inequality that exists in society, and the manner in which it is accepted by people with and without power. In cultures with a high power distance index, subordinates expect to be told what to do. Centralisation is seen as popular, and less powerful people are seen as dependent on the more powerful. In contrast, cultures with a low power distance, share the power and people are considered more equal.

In African cultures, there is a high power distance (McFarlin et al., 1999, Cramer, 2010).

ii. Femininity vs. masculinity
A high masculinity index means that performance is valued; there is more sympathy for the strong; and equality is important. In contrast, a culture with a high femininity index indicates that people are more generous towards each other; there is sympathy for the weak; and intuition is used to strive for consensus.

Femininity is more prevalent in African cultures (McFarlin et al., 1999, Cramer, 2010).

iii. Uncertainty avoidance
Uncertainty avoidance relates to the degree of anxiety people experience when in uncertain or unknown situations. People from cultures with a high uncertainty avoidance index have a need for rules and predictability and they consider anything that is different as dangerous. There is an inherent fear of uncertain situations and unfamiliar risks, and a high premium is placed on belief in experts and specialisation. Conversely, in cultures with low uncertainty avoidance, people are more open to taking risks and interacting in environments where there is more freedom and less predictability.

African cultures have a very high uncertainty avoidance index (McFarlin et al., 1999, Cramer, 2010).

iv. Long-term vs. short-term orientation
The long-term vs. short-term orientation dimension relates to the fostering of virtues. In long-term orientated cultures, there is more emphasis on fostering future virtues oriented towards
rewards. Examples of this include ordering relationships by status, investing in real estate, saving and being thrifty. In contrast, short-term orientated cultures are more concerned with fostering values related to the past and present. Emphasis is placed on respect for tradition, preservation of one’s face, quick results, personal steadfast and stability.

Short-term orientation is found in many African cultures (McFarlin et al., 1999, Cramer, 2010).

v. Collectivism vs. individualism
The collectivism vs. individualism dimension classifies a culture according to how strong the ties are between individuals in society (Hofstede, 1980). In an individualistic culture the ties among people in society are very loose and people focus on themselves and their immediate family. However, in collectivist cultures people focus on family and on forming strong cohesive groups.

Westernised American culture adopts a world view that states I am because I, the individual hero, dream and do (Mbigi, 2003), whereas the world view in the African culture is I am because we exist. These two world views capture the essence of the individualism vs. collectivism dimension defined by Hofstede (1980), and has become the main and most significant difference between cultures (Triandis, 2001, Cramer, 2010, Chong, 2003). For this reason, this research focuses on the collectivism dimension in order to understand trust in these societies.

4.3 Individualist vs. Collectivist cultures
As several other researchers have done (Triandis, 2001, Sia et al., 2009, Huff and Kelley, 2003, Cramer, 2010, Isherwood et al., 2012), this research uses the collectivism vs. individualism dimension as the main and most significant dimension for the comparison between cultures. In this section, individualist and collectivist cultures are discussed in more detail, using consumer trust in e-commerce as an example to provide an understanding of the difference between these two types of cultures.

a) Individualist cultures
Individualist cultures are found mainly in North America and much of Western Europe. Here individuals are responsible for their own welfare and that of their direct family (Cramer, 2010), and a high value is placed on individual freedom. Westerners tend to be logical and action-oriented. These characteristics determine their behaviour. For example, they do not hesitate
to criticise an e-commerce website for a failed transaction (Isherwood et al., 2012). In their evaluation of an e-commerce website, they are influenced by logic, facts and directness.

To people in individualist cultures, consumer trust is established by considering all facts comprehensively. Trusting decisions are based on the facts that are presented, such as verified certificates and assurance labels, rather than intuition. In their evaluation of an e-commerce transaction, they tend to be straightforward, concise and efficient (Isherwood et al., 2012). They prefer to use words that accurately describe a situation, and intend them to be taken literally.

b) Collectivist cultures
Collectivist cultures are found mainly in much of the Middle East, Asia, Africa and South America (McFarlin et al., 1999, Cramer, 2010). Collectivist cultures integrate individuals from their birth into tightly knit, cohesive groups (Cramer, 2010). This means that people in these cultures emphasise interpersonal relationships where loyalty is obtained by protecting the group members for life. Individuals see themselves as subordinate to a social collective such as a state, a nation, a race, or a social class.

They prefer group harmony and consensus to individual achievement. For example, saying no to the wishes of the group would destroy the harmony in the group. It is also out of the question to disagree with someone’s opinion in public. Any criticism is rather voiced in a private forum and direct confrontations are avoided as far as possible (Hofstede, 1980). For these individuals, their opinions are predetermined by the group they belong to. Any action out of the scope of expected group behaviour leads to shame and loss of face for self and group (Botha, 2007, Cramer, 2010). This means that any criticism or evaluation of an e-commerce website must be in line with the opinion and goals of the group, and should be made using descriptive expressions or phrases instead of harsh statements or metrics.

In the next sections, the different approaches to trust is discussed by making use of a use case to demonstrate how each culture responds to online environments where trust is required.

4.4 Cultural influence on trust

The purpose of the section is to indicate that existing, popular e-commerce environments such as eBay, cater mostly for individualist cultures and not as much for collectivist cultures. This section also aims to further enhance the fact that culture influences the trust constructs
discussed in the previous chapter, namely: situational decision to trust, dispositional trust, trusting beliefs, system trust, trusting intentions, and trusting behaviour.

4.4.1 Use case for trust in individualist cultures

eBay describes itself as the world’s largest online marketplace that supports more than 97 million active users globally in 2011 (eBay, 2012, Schlägel and Wolff, 2007). Founded in 1995, eBay connects a diverse community of individual buyers and sellers, as well as small businesses. By 2010, the total value of goods sold on eBay was $62 billion, more than $2 000 every second. eBay itself contributes the high rate of successful transactions to its reputation system (eBay, 2012).

When transacting on eBay, buyers and sellers sign up for an account and are provided with a comprehensive set of rules and policies that must be followed. They are advised to take note of a seller’s feedback rating (eBay, 2012). If the rating is high, the seller is presumed to be honest. Buyers are further advised to only deal with sellers via the eBay site. The seller’s method of payment should be via a trusted third party such as PayPal (PayPal, 2012). A buyer should never be expected to provide his/her credit card details or to perform a bank wire. Buyers are often required to make advanced payments, this introduces more risk as the seller may well deliver a substandard product/service once payment has been received (Schlägel and Wolff, 2007). It is also advised that buyers should test the trustworthiness of the seller by first purchasing a small item.

eBay has a feedback system to provide buyers and sellers with the opportunity and a method of evaluating each other. For each transaction, only the buyer and seller can rate each other by leaving feedback. Each feedback left consists of a positive (+1), negative (-1), or neutral (0) rating, and a short comment. A feedback score of at least 10 earns a buyer or seller a yellow star. There are twelve stars, where a silver shooting star indicates 1 000 000 ratings or more. It is vital that community members provide honest ratings and comments about a particular eBay member, as eBay stars represent the trustworthiness, reputation and community standing of buyers and sellers. The trust and reputation mechanisms used by eBay are defined at numerous layers, which are described next.

a) eBay trust and reputation mechanisms

When one considers the manner in which the eBay site is designed and used, it becomes imminent that the trust mechanisms and general procedures are geared to support the requirements of the individualist buyer or seller (Isherwood et al., 2012). This section
discusses the influence of individualist culture on the constructs of trust as introduced in Chapter 2.

i. Dispositional trust
Trust starts with an individualist buyer accessing the eBay website. As the dispositional trust of such a buyer is generally higher than that of a collectivist buyer, a basic level of trust exists that enables the buyer to investigate the possibilities that eBay presents. As this buyer is more of a risk taker, acting as an individualist, this may happen without recommendations from friends about the trustworthiness of eBay (Chong, 2003, Huff and Kelley, 2003). The success of eBay supports the notion that people from individualistic cultures tend to trust strangers with more ease.

ii. Situational decisions to trust
Since dispositional trust is high in individualist cultures, the use of online collaboration platforms like eBay is more natural to individualist cultures. There is a high level of acceptance of such online environments, and therefore systems such as the digital business ecosystem are easily adopted.

The next steps followed by a typical eBay user are to create an account. During this time, an eBay user reads and accepts the rules and policies as outlined by eBay. These safeguards increase the trust of the buyer, as he/she prefers a rules-based environment (Chong, 2003). Therefore, individualist cultures are more willing to trust in this particular situation, thereby increasing the situational decision to trust.

iii. System trust
System trust in eBay is formed when the buyer observes the institutional guarantees, laws and policies, as well as information security mechanisms that are provided. For example, the buyer understands the meaning of sophisticated mechanisms such as certificates and third party assurances, which increases his/her trust in the eBay system. In general, the implementation and reputation of eBay facilitates the trust of individualist cultures since it appeals to their norms of behaviour.

iv. Trusting beliefs
Through continued use of the eBay platform, a buyer proceeds to transact with sellers and vice versa. Once a number of successful transactions occur, the users form their own trusting beliefs. If goods are received as promised, the ability belief characteristics increase. In the same way, integrity and benevolence increase and lead to a higher trust in eBay. To enable
buyers to avoid untrustworthy sellers, a feedback system is implemented that provides a calculated numeric score indicating the reputation of each seller. This is ideal for individualist buyers who prefer to make trust decisions based on analytical means.

The trust and reputation mechanisms provided by eBay satisfy the trust constructs as perceived by individualist cultures. This results in its increased usage by individualist consumers and number successful transactions and collaborations.

b) eBay for individualist cultures
Individualist cultures are more willing to share information with the public compared to collectivist consumers (Hofstede, 1980). Their communication style is more expressive and explicit and they are likely to voice their dissatisfaction if necessary. Due to the masculine nature of individualist cultures, individualist buyers behave judgementally and are less concerned about the feelings of others (Hofstede, 1980). This reflects on their consumer satisfaction scores. eBay’s feedback system provides buyers and sellers with the opportunity to freely and honestly express their opinion of others. This makes eBay reliable and appropriate to the individualist buyer or seller, leading to its success in Western cultures.

Through satisfying the dispositional trust, situational decision to trust, system trust, and trusting belief constructs the eBay user is now willing to trust the system as well as those identified as collaboration partners, i.e. sellers and buyers. This refers to the trusting intention and based on this, the individualist user goes ahead and transacts, thereby forming their trusting behaviour.

An e-commerce system such as eBay clearly caters for the individualist consumer (Chong, 2003). The collectivist consumer requires a different approach to e-commerce, which should be based on his/her characteristics relating to collectivist norms of behaviour and values, as will be discussed next.

4.4.2 Use case for trust in collectivist cultures
In order to implement a digital business ecosystem for collectivist Africa successfully and render it usable, the collectivist cultural approach to consumer trust needs to be understood (Isherwood et al., 2012). Ideally, a similar e-commerce system should support VSEs and other SMMEs in the digital business ecosystem for African in the same way that eBay facilitates e-commerce in the developed world for individualist cultures. This e-commerce system should
support collaboration in the digital business ecosystem and address the requirements of cultures in Africa.

The example of spaza shops as VSEs is now considered. An e-commerce system needs to be created to allow spaza shops to place orders directly with suppliers. As indicated, similar systems already exist, particularly those implemented by Ngassam et al. (2011) in South Africa. Additionally, VSEs should be supported to cooperate with one another by forming cooperatives (Chebelyon-Dalizu, 2010) so as to enable discounts on bulk buying and goods delivery costs.

For any system supporting this scenario, cooperative members must trust one another, cooperatives must be trusted by suppliers, and suppliers must trust cooperatives (Tadelis, 2003). The collectivist consumer’s approach to conducting business in this environment is described next in an attempt to demonstrate the collectivist consumer’s behaviour to trust.

**a) Trust mechanisms of the spaza shop online system**

The trust constructs are now discussed from the viewpoint of the spaza shop VSE in order to demonstrate the approach of collectivist cultures towards trust.

i. Dispositional trust

Trust starts with the collectivist buyer (VSE) encountering the e-commerce mobile website or application on his/her mobile device. This system allows the buyer to form a cooperative with other spaza shops and place orders with suppliers that are supported by cloud-based technology. As the dispositional trust of the collectivist buyer is generally lower than that of the individualist buyer (Hofstede, 1980), he/she may choose simply not to investigate the possibilities posed by the e-commerce system any further.

ii. Situational decision to trust

Collectivist buyers are risk-averse as they have a high uncertainty avoidance index. Any unfamiliar situation may be seen as dangerous (Hofstede, 1980) and initial trust needs to be formed using other means. If an e-commerce interaction is seen as a comfortable situation, without much risk involved, then the situational decision to trust of the VSE increases.

Collectivist buyers are more willing to commit to their existing group relationship, rather than consider forming a relationship with others outside the group. This minimises the perceived risk and collectivist buyers therefore form new relationships only if strong institutional safeguards are present. As a high premium is placed on belief in experts, a recommendation
The influence of culture on trust and reputation

from a well-respected person may be required to ensure a basic level of trust in the system (Lee and Kacen, 2008).

iii. System trust
System trust in the spaza shop e-commerce system can be formed when the spaza shop owner observes the institutional guarantees, rules and policies, as well as information security mechanisms that are provided. As the spaza shop owner may be unaware of the meaning of features such as certificates and third party assurances, it may not affect his/her trust in the system considerably.

iv. Trusting beliefs
Even if the collectivist buyer proceeds to transact successfully with the supplier, their trusting beliefs may increase only marginally when goods are received as promised, as he/she does not place a high value on the ability belief characteristic (Chong, 2003, Mayer et al., 1995). On the other hand, if asked by a leader in the community to use the system, his/her benevolence (Cramer, 2010, Chong, 2003) towards the system may increase, leading to a higher level of trusting beliefs (Mayer et al., 1995).

This use case gives an indication of the approach followed towards trust building by collectivist cultures. It indicates that there is a difference between the approach of individualist and collectivist individuals. The next section provides a summary how culture influences the trust constructs.

4.4.3 Culture and it’s relation to trust

The use cases give a good indication of the difference between the individualist approach to trust in an e-commerce environment and the collectivists approach to trust in e-commerce environment. The table below, Table 4.2, highlights the differences as discussed.
Table 4.1 Difference between individualist and collectivist culture in terms of trust

<table>
<thead>
<tr>
<th></th>
<th>Individualist cultures</th>
<th>Collectivist cultures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Acts as individual</td>
<td>Acts with a group</td>
</tr>
<tr>
<td>Dispositional trust</td>
<td>• Generally higher.</td>
<td>• Generally lower.</td>
</tr>
<tr>
<td></td>
<td>• Risk takers.</td>
<td>• Risk-adverse.</td>
</tr>
<tr>
<td>Situational decision to trust</td>
<td>• Trust in strangers is higher.</td>
<td>• A high uncertainty avoidance index.</td>
</tr>
<tr>
<td></td>
<td>• Prefer rule-based environment.</td>
<td>• Rely on expert recommendations of group members.</td>
</tr>
<tr>
<td>Trusting beliefs</td>
<td>• Emphasis on ability trusting belief due to masculine nature.</td>
<td>• Ability trusting belief is not as important as integrity and benevolence due to femininity nature and loyalty.</td>
</tr>
<tr>
<td></td>
<td>• Express opinions explicitly.</td>
<td>• Less explicit in expressing opinions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Maintain group harmony</td>
</tr>
<tr>
<td>System trust</td>
<td>• Rule-based environment where institutional guarantees, laws and policies are defined.</td>
<td>• Rule-based environment is not as important, instead expert recommendations are important.</td>
</tr>
<tr>
<td></td>
<td>• Analytical need is fulfilled.</td>
<td>• Strong groups are needed to support recommendations.</td>
</tr>
</tbody>
</table>

Cultural differences influence the trust building mechanism of members of a cultural group (Isherwood et al., 2012). In Chapter 3, the constructs of trust were presented based on the work of McKnight and Chervany (1996). These constructs showed that trusting behaviour is a result of trusting intentions which are determined by, the situation decision to trust, dispositional trust, trusting belief and system trust. This is depicted in Figure 3.1 from Chapter 3. However, since culture has an influence on trust and reputation, Figure 3.1 is altered to depict that the constructs of trust are influenced by culture, resulting in Figure 4.1 below.

This research now adapts the constructs of trust presented by McKnight and Chervany (1996) to reflect the influence of culture, shown in Figure 4.1.
The influence of culture on trust and reputation

Since trust is influenced by culture, and there is a difference between individualist cultures and collectivist cultures, the next section explores the collectivist cultural approach further. The purpose of this is to gain a good understanding of the collectivist cultural norms of behaviour that influence trust. These can then assist with the implementation of an appropriate trust and reputation properties in the digital business ecosystem in an African context.

4.5 Collectivist cultures and their trusting behaviour

For the collectivist spaza shop owner, the formation of trust is consequently not the same as for the individualist consumer (Isherwood et al., 2012). If a similar feedback system as eBay’s is implemented to increase trust, the results may not be able to reflect the true trustworthiness of collectivist cooperative members, cooperatives, and suppliers. This section extends upon some of the norms of collectivist cultures which were previously mentioned. Four features relating to group behaviour and community are now identified by the researcher, namely:

- Trust grows as group harmony increases.
- Recommendations from in-group members are trusted more.
- Trust grows with an increase in social position.
- Trust in outsiders is formed by recommendations from in-group members.

This sets the tone for the identification of trust properties for collectivist cultures.
4.5.1 Trust grows as group harmony increases.

In collectivist cultures, individuals are integrated into the Ubuntu way of life at an early stage (Mbigi and Maree, 1995, Botha, 2007). Here individuals are encouraged to subordinate their goals to the goals and needs of their family and community (Hofstede, 1980), also known as vertical collectivism (Chen et al., 1997). Generally, collectivists are more likely to share information within the group and are less expressive and explicit when expressing an opinion about another (Chong, 2003) in order to maintain group harmony. Group members rely on other members to act in a way as to benefit the group. To enforce such behaviour, collectivist cultures can be harsh in their punishment towards in-group members that jeopardise the group’s position. According to (Moliea, 2007), non-compliance to the group’s expected behaviour can easily lead to expulsion from the group.

The collectivist approach to group harmony influences behaviour in business and collaborations (Cramer, 2010). For example, consider the use case discussed previously. Suppliers know they can rely on the loyalty of all members of a cooperative they all belong to, even if they do not always provide a good service. They are not too concerned about a spaza shops badmouthing them publicly if their service is bad, as they know that the spaza shop would not want to disturb the harmony of the group. This is very different to the individualist consumer, who easily gives negative ratings and comments on poor performance. A collectivist consumer is more lenient towards a bad experience (Chong, 2003) and rather discusses this experience within the group than make a public statement, in order to maintain group harmony. If the spaza shop should publically criticize the supplier, he may be punished by the group for disturbing the group harmony. This approach leads to strong trust communities, where the members of the community are more concerned about the reputation of the community as a whole, than about their individual reputations.

The role of groups and community in collectivist cultures is clearly visible, and is the biggest differentiator between collectivist and individualist cultures (Triandis, 2001, Cramer, 2010, Chong, 2003). This leads to a number of other behavioural norms which are the main focus of collectivist cultures. For example, group members have a stronger preference for the advice or recommendations of in-group members (Moliea, 2007, Botha, 2007). The next section discusses the preference towards in-group members and how it influences trust.
4.5.2 Recommendations from in-group members are trusted more.

In collectivist cultures, groups form, based on shared goals, demographics and personal interests. Such groups are selected according to similarities such as gender, age, occupation, ethnicity, kinship, residential origin or a combination of these similarities (Tsai, 2000, Moliea, 2007). Similarity indicates shared interests and goals, making it easier to relate to another individual or group. Additionally, the importance of groups in collectivist cultures further emphasis the preference towards in-group members. The initial trust between individuals who are similar is more than between those who are not. Ziegler and Golbeck (2007) conducted a study on the dependencies between trust and similarity and found that dependencies exist when the group’s trust network is tightly bound to a shared cause such as profit or business growth. Shared similarities in a group provide an initial understanding amongst members that can provide an initial level of trust among group members. Therefore, in-group members tend to share similarities which enforce a level of trust among them. This encourages more trust in in-group members, rather than those outside of the group, known as out-group members.

As mentioned, there is the shared cause of maintaining group harmony. This cause encourages in-group members to behave as to not disturb the group’s harmony. Group members rely on other in-group members to behave in accordance to shared goals, making in-group members more reliable than those outside of the group (Moliea, 2007, Botha, 2007). Collectivist cultures therefore encourage individuals to trust more within groups, and rely less on others outside the group (Yamagishi, 1988, Triandis, 2001) to instil strong loyalty towards the group (Huff and Kelley, 2003). Considering the scenario of SMMEs in the digital business ecosystem, in-group members are thus more likely to be selected for transactions that those outside the group, based on the preference towards in-group-members.

Another norm of collectivist cultures, which follows from the preference towards in-group members, is social position/standing. Particularly, the group dynamics of groups formed in collectivist cultures can largely influence who is considered as trustworthy or not. The next section discusses the role of social position in collectivist cultures.

4.5.3 Trust grows with an increase in social position.

In African cultures, social hierarchies influence trust (Botha, 2007). The collectivist consumer in rural Africa trusts another more if he/she has a higher social standing. In contrast, in individualist cultures, social position is not a defining factor in increasing consumer trust. Individualist consumers are risk takers who establish initial trust relatively easily with
strangers. In contrast, collectivist consumers are risk adverse and avoid situations where there is a high uncertainty. As emphasis is placed on the social position and standing of a member in the community, those in a more influential position tend to be trusted by the community. Recommendations from such members are considered more reliable since they are trusted and have the group’s reputation in mind, due to their collectivist mind-set (Moliea, 2007).

In collectivist cultures, members rely on other group members such as group leaders, who have a higher social standing to make informed decisions. The social position of a group leader can increase or decrease the level of trust that group members have in him/her. Leaders who are well connected and in good standing with others are generally viewed as more trustworthy by members of the group (Mbigi and Maree, 1995). Well-connected group members can also provide access to a wider range of resources (Oh et al., 2006, Mehra et al., 2006) such as identifying trustworthy collaboration partners outside of the group that may lead to potential business opportunities.

Establishing business opportunities with outsiders requires that they can be trusted to not jeopardise the harmony of the group. Establishing trust in outsiders is discussed in the next section.

4.5.4 Trust in outsiders is formed by recommendations from in-group members

Research by Moliea (2007) and Botha (2007) identify that when groups are formed, new members are generally included only if they are personal friends of existing members. Since the existing member is held responsible, to a certain degree, for the new member’s behaviour, it is vitally important that any new member should be trustworthy. The social position of new members relative to the group further indicates the initial trust level that is assigned to the new member when joining the group.

With this being said, collectivist consumers take a longer time to trust outsiders, but once this trust is developed, it can be stronger and more enduring (Huff and Kelley, 2003). When spaza shops partake in group buying, a relationship is required between the spaza shops and the suppliers. A new supplier introduced into such an ecosystem would find it challenging to establish initial trust with the spaza shops. However, if the supplier manages to establish a trusting relationship with the group of spaza shops, the supplier would benefit. The group would have a high level of loyalty in the supplier, resulting in regular business.
The next section identifies trust and reputation properties from this discussion on collectivist cultures behaviour.

## 4.6 Trust and reputation properties for the digital business ecosystem

The previous sections identified that trust is influenced by the behaviour of collectivist cultures. In this section, four properties are proposed that is a refinement of the previous discussion, namely:

- **a)** Members of a group that maintain group harmony are trusted more
- **b)** Members of a group trust in-group members more than out-group members
- **c)** Influential nodes such as group leaders are trusted more
- **d)** Out-group members can be trusted if they are recommended by in-group members

These properties are addressed in the remainder of the research in order to support trust and reputation for collectivist cultures in the digital business ecosystem. These trust and reputation properties for collectivist cultures are now discussed in more detail.

### 4.6.1 Trust and reputation properties for collectivist cultures

The proposed trust and reputation properties for collectivist cultures are now described in more detail and their use in the digital business ecosystem is specified.

#### a) Members of a group that maintain group harmony are trusted more

For the purpose of this study, group harmony refers to the collective trust perception of a group by others outside of the group (Kim et al., 1990). Group harmony is influenced by the behaviour of the members of the group where group harmony decreases if a group member behaves destructively. As they are loyal to the group, other group members have less trust in such group members.

If members of a group follow the general rules of the group, they are trusted more by other group members as they are seen to be reliable. To be able to implement this property, the following is noted:

- **i.** Groups form where members collaborate with each other.
- **ii.** Members should act in the best interest of the group.
- **iii.** Members that jeopardise the group should be punished.
iv. Group members generally trust each other more than strangers.
v. Dense groups should be considered more trustworthy since collective decisions can be made and information can be verified by many.

Implementing this property can result in the formation of strong cohesive groups which create and foster a trusting environment as collectivist societies naturally behave.

b) Members of a group trust in-group members more than out-group members

Research has shown that members of the same group, sharing similarities are more cohesive and trustworthy (Ziegler and Golbeck, 2007, Ziegler and Lausen, 2004, Moliea, 2007, Walter et al., 2008, Golbeck, 2009). Therefore, these members can trust their in-group members. However, this results in reduced trust towards out-group members.

To implement this trust property, the following is noted:

i. Trust is higher between members that are similar and have shared interests.
ii. Members who are not similar are initially distrusted.
iii. Groups are formed among members that are similar.

This trust property supports trusted interactions among in-group members to enhance the strength of the group.

c) Influential nodes such as group leaders are trusted more

For the purpose of this research, social position refers to the relative position of a person or node within a society, culture, or network. Research has been done to determine the impact of social position on trust and reputation (Page et al., 1999, Varlamis et al., 2010, Isherwood and Coetzee, 2011) and has shown those in influential social positions are trusted by many.

To implement this property, the following is noted:

i. Influential nodes that control the flow of information should be identified and can be more trusted by the community.
ii. Highly connected members of a group should be identified and can be considered as group leaders.

This ensures that members with higher social standing and influence in the network are trusted, to reflect the collectivist behaviour better.
d) Out-group members can be trusted if they are recommended by in-group members

In-group members are considered more trustworthy than out-group members in collectivist cultures. However, without new members joining the group, the group is not be able to grow and has limited possibilities for collaboration (Huff and Kelley, 2003). Therefore, out-group members need the opportunity to become group-members.

In collectivist cultures, there are rules that enable out-group members to become in-group members. The following can be noted:

i. Collaborations with non-group members can be initiated if they are recommended by existing group members.

ii. The recommending in-group member takes responsibility for the behaviour of the recommended out-group member.

The trust property enables SMMEs to transact with unknown SMMEs with a certain confidence in their trust, due to the recommendations from in-group members. This supports the growth of the digital business ecosystem as more business opportunities are possible.

These four trust properties proposed in this section are implemented in following chapters, to facilitate trust and reputation for collectivist cultures in the digital business ecosystem. For this purpose, the definition of the digital business ecosystem is revised in the next section.

4.6.2 Summary of trust properties for collectivist digital business ecosystems

Table 4.2 provides a summary of the previous discussion. The trust properties of collectivist cultures are presented together with the features relating to the trust property.
### Table 4.2 Trust properties for collectivist cultures

<table>
<thead>
<tr>
<th>Trust property</th>
<th>Features of note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Members of a group that maintain group harmony are trusted more</td>
<td>i. Groups form where members collaborate with each other.</td>
</tr>
<tr>
<td></td>
<td>ii. Members should act in the best interest of the group.</td>
</tr>
<tr>
<td></td>
<td>iii. Members that jeopardise the group should be punished.</td>
</tr>
<tr>
<td></td>
<td>iv. Group members generally trust each other more than strangers.</td>
</tr>
<tr>
<td></td>
<td>v. Dense groups should be considered more trustworthy since collective decisions can be made and information can be verified by many.</td>
</tr>
<tr>
<td>Members of a group trust in-group members more than out-group members</td>
<td>i. Trust is higher between members that are similar and have shared interests.</td>
</tr>
<tr>
<td></td>
<td>ii. Members who are not similar are initially distrusted.</td>
</tr>
<tr>
<td></td>
<td>iii. Groups are formed among members that are similar.</td>
</tr>
<tr>
<td>Influential nodes such as group leaders are trusted more</td>
<td>i. Influential nodes that control the flow of information should be identified and can be more trusted by the community.</td>
</tr>
<tr>
<td></td>
<td>ii. Highly connected members of a group should be identified and can be considered as group leaders.</td>
</tr>
<tr>
<td>Out-group members can be trusted if they are recommended by in-group members</td>
<td>i. Collaborations with non-group members can be initiated if they are recommended by existing group members.</td>
</tr>
<tr>
<td></td>
<td>ii. The recommending in-group member takes responsibility for the behaviour of the recommended out-group member.</td>
</tr>
</tbody>
</table>
The next section provides a definition for the collectivist digital business ecosystem and takes into account the behaviour of collectivist cultures.

### 4.7 Collectivist digital business ecosystem

For this research, the definition of a digital business ecosystem, to be applied in a collectivist African context, is now refined as follows:

A **collectivist digital business ecosystem** is an environment where entities such as SMMEs interoperate and collaborate with each other through digital means via transactions, while at the same time considering the influence of the collectivist culture and beliefs. Transactions occur among software agents of SMMEs when a SMME provides a service to another SMME and/or vice versa. This service is in the form of knowledge exchange, goods exchange, or expertise exchange.

This research specifically refers to communities in Africa, but the resulting model should also be relevant to collectivist communities in other parts of the world such as South America and Asia. In order to be able to support trust in a collectivist digital business ecosystem, the next chapters refine the trust properties introduced in this chapter.

### 4.8 Conclusion

A trust and reputation system that provides guidance and recommendations to VSEs and other SMMEs in the collectivist digital business ecosystem should consider collectivist cultural behaviour. This could lead to more accurate recommendations to enhance the growth of the collectivist enterprise.

In this chapter, an introduction to culture was provided and Hofstede’s five dimensions of culture were discussed. The individualist versus the collectivist dimension was identified as the most important dimension for the classification of cultures, and an introduction to these two different cultures were given.

Next, each of these cultures was discussed in terms of their approach to trust in e-commerce systems and it was clear that there is a difference between the individualist and collectivist
approaches. The influence that culture has on trust was highlighted by the extension of a well-known diagram that depicts the constructs of trust.

The behaviour of collectivist cultures was further examined indicating that groups, group members, and social position play an important role in this culture. Based on this behaviour, four properties for trust and reputation for collectivist cultures were proposed. A definition for the collectivist digital business ecosystem was given.

These trust properties are considered as the main result of this chapter. These properties can support trust and reputation for collectivist cultures in the collectivist digital business ecosystem. The next chapter takes a more in-depth look at how these trust properties can be satisfied and implemented.
Chapter 5

Social network analysis for collectivist digital business ecosystem trust and reputation

5.1 Introduction

The previous chapter identified four trust properties that can be applied to a trust and reputation system for a collectivist digital business ecosystem. In this chapter, an attempt is made to investigate these four trust properties by considering social network analysis, so that they can be made implementable. By identifying and interpreting a SMME’s social position within the collectivist digital business ecosystem, information can be gleaned about the possible trust that exists in a member of a collectivist community. Social network analysis can potentially contribute towards enhancing the calculation of trust for collectivist digital business ecosystems.

Studies by Kim and Srivastava (2007) and Sinha and Swearingen (2001) show that consumers are more likely to trust recommendations provided by friends, acquaintances, and business partners, rather than strangers. The identification of influential nodes can further be a valuable source of recommendations to many other nodes in the network. The discovery of the social position of a node within a social network can enhance trust and reputation calculations, which can prove to be highly relevant to collectivist cultures in Africa.

Social network analysis encapsulates a set of techniques and methods used to analyse social graphs and interpret relationships within a network (Daly and Haahr, 2009, Serrat, 2009). It has been used in many domains and its benefits have been proven (Rosenquist et al., 2010, Carroll et al., 2010, Berkman et al., 2000, Daly and Haahr, 2009). In this chapter, social network analysis is explored to determine its benefit and use in the context of trust and reputation for the collectivist digital business ecosystem. To achieve this, the collectivist digital business ecosystem is represented as a social graph where social network analysis centrality measures are explored.
This chapter provides an introduction to social network analysis. The representation of the collectivist digital business ecosystem as a social graph is discussed. Social network analysis centrality measures are explored to identify relevant measures for trust and reputation in a collectivist digital business ecosystem. The resulting centralities are further investigated and their relevance to this study is further motivated. Lastly the chapter is concluded.

5.2 Benefits of social network analysis for the collectivist digital business ecosystem

Social network analysis is now defined and its use in different domains discussed. This is followed by a discussion on typical problems that social network analysis aims to solve in the context of the digital business ecosystem.

a) Social network analysis

According to different authors, social network analysis has many definitions. Otte and Rousseau (2002) define social network analysis as a broad strategy for investigating social structures. Similarly, Varlamis et al. (2010) and Serrat (2009) define social network analysis as the study of the relationships that exist between entities. Carroll et al. (2010) consider social network analysis as “an approach and set of techniques which studies the exchange of resources (for example, information) among actors”.

These definitions all assume that relationships are important (Serrat, 2009). Ortiz-Arroyo (2010), defines social network analysis as a model rich in conceptualization and investigation, which provides a powerful set of concepts and methods for designing, modelling and analysing complex situations. It has therefore been used in different domains, such as psychology (Rosenquist et al., 2010, Scott, 2000, Wasserman and Galaskiewicz, 1994), business (Carroll et al., 2010, Tichy et al., 1979), health (Berkman et al., 2000, Christakis and Fowler, 2007), and electronic communications (Daly and Haahr, 2009, Brown et al., 2007).

With the increase of social networking websites such as Facebook (Facebook, 2013), Twitter (Twitter, 2013), and Google+ (Google+, 2013), blogs, and customer reviews, social network analysis has become a major area of research (Varlamis et al., 2010). The representation and analysis of vast amounts of links and relationships provide useful information regarding the role that nodes, such as people, businesses, and routers, play in a network. Social network analysis provides the techniques and methods to identify such nodes and determine which relationships are important within networks.
b) The benefits of social network analysis

Social network analysis techniques have been proposed to solve the following problems found in social networks (Kim and Srivastava, 2007, Varlamis et al., 2010, Wasserman and Galaskiewicz, 1994):

i. Extracting communities in a large social network

In collectivist digital business ecosystems, large communities with SMMEs that often interact can be extracted using social network analysis. The benefit of extracting such communities is that they are generally strong cohesive groups that develop over continuous successful collaborations (Isherwood et al., 2012, Cramer, 2010, Opsahl and Panzarasa, 2009). Other businesses in the collectivist digital business ecosystem would attempt to join such groups if they can be identified, as this can provide more business opportunities.

ii. Identifying trusted, expert, and prominent actors that are key nodes in a social network

Businesses that control information flow and have strong influence need to be identified in a network. The identification of such central nodes is useful, since they often play an important role by issuing information, ideas, and establishing connections with other communities, due to their influence and position within the network (Chau and Xu, 2007). Essentially, such businesses are considered more trustworthy since they can lose their influence and position in the social graph if they behave maliciously (Isherwood and Coetzee, 2011, Droege and Dong, 2007).

iii. Predicting trust between actors in the social network

The location of a specific member of a community within a collectivist digital business ecosystem social network can be used to infer some properties about their reputation (Isherwood and Coetzee, 2011, Teacy et al., 2006). Organisations that are effective and highly regarded by most members of the collectivist digital business ecosystem tend to be highly connected nodes in the social network graph.

The benefits of social network analysis directly relate to the trust and reputation properties for collectivist cultures. Using social network analysis, it can be possible to identify groups, group leaders, other influential nodes, and predict trust-related properties based on a nodes social position. This makes it relevant to collectivist cultures and the collectivist digital business ecosystem.
For the collectivist digital business ecosystem to benefit from social network analysis the ecosystem needs to be represented as a social graph, so that social network analysis techniques and methods can be applied. The next section addresses this requirement.

5.3 Social graph of the collectivist digital business ecosystem

Social network graphs are used to represent the nodes and relationships between nodes. Next, the social graph and social overlay network for the collectivist digital business ecosystem is defined.

a) Social graph

A social graph is a directed weighted graph G defined as:

\[ G = (V, E) \]

V is the finite set of vertices and E is the finite set of edges where each edge is an unordered pair of distinct vertices (Zolfaghar and Aghaie, 2011, Bilgin and Yener, 2010).

Since the digital business ecosystem is represented as a P2P network, where nodes represent the SMMEs and the links represent the connections between agents, it is natural to consider this ecosystem as a social graph. The SMMEs in the collectivist digital business ecosystem are thus represented as vertices (V) and the relationship between them is represented as weighted edges (E).

b) Social overlay network

To define a social graph for the collectivist digital business ecosystem, a social overlay is defined as discussed in Chapter 2. This is depicted in Figure 5.1.
The Social Overlay Network overlays the collectivist digital business ecosystem P2P Overlay Network. This implies that each agent representing a SMME in the collectivist digital business ecosystem is considered as a node in the social graph.

c) Social graph of the collectivist digital business ecosystem

Figure 5.2 shows the social graph of the collectivist digital business ecosystem, similar to Figure 2.3 where SMMEs are considered as nodes in a social graph.
On the top left, the social graph shows a VSE such as SpazaShop A, and another SMME such as Supplier A as the nodes (actors) and the connections (links) between them. The connections are directed and weighted according to the properties of the social graph. In the case of the collectivist digital business ecosystem, the weights refer to the level of trust that exists between two nodes.

As nodes may not have a complete view of the network due to the decentralised nature of the collectivist digital business ecosystem, challenges arise when considering either local or global social graph views. This is considered in the next section.

5.4 Social graph views for social network analysis

Agents in the collectivist digital business ecosystem make use of a social graph to perform social network analysis. There are two types of views of a social graph that are used for social network analysis (Daly and Haahr, 2009) namely socio-centric and ego-centric. Each view constrains the scope of trust and reputation information that can be obtained, and
personalisation of such information. These two social graph views are discussed next, considering their impact on determining trust and reputation.

5.4.1 Socio-centric view

In the socio-centric view, analysis is performed on a complete and bounded social graph from a global view (Daly and Haahr, 2009) as shown in Figure 5.2. Social network analysis techniques take into account all the nodes as well as the links between them (Ziegler and Lausen, 2005). This implies that each node only considers the global reputation of any other node calculated by a centralised reputation manager who has a view of the entire network.

The analysis of the entire network from a single point is process intensive, as the complete social graph of the network may continuously change. The centralised and global approach limits the personalised property of trust, as a node’s trust is considered from an aggregated third party view, and not personally (Golbeck, 2006). This leads to a very general trust and reputation opinion, as well as a centralised architecture.

Therefore, this approach is not be useful for collectivist digital business ecosystem trust and reputation systems, which needs to have a decentralized architecture (Isherwood and Coetzee, 2011, Daly and Haahr, 2009, Sabater and Sierra, 2001).

5.4.2 Ego-centric view

In the ego-centric view, analysis is performed on the ego-network of a node, which consists of the node (actor), its friends (alters) and all the connections between them (Daly and Haahr, 2009, Newman, 2003). The ego neighbourhood is the collection of the ego and all nodes with which ego has a connection at some path length. In social network analysis, this includes only the ego and actors that are directly adjacent and all of the ties among all of the actors to whom the ego has a direct connection (Ziegler and Lausen, 2005). If one considers SpazaShop S as an ego in Figure 5.2, then Figure 5.3 is the ego neighbourhood to be considered.
Using this view to perform trust and reputation computations is less process intensive compared to the socio-centric view. Each node, such as SpazaShop S, only maintains trust and reputation for its own locally stored ego-network, and does not require complete knowledge of the network. It is natural to use an ego-centric view in P2P networks due to the decentralised nature of these networks (Daly and Haahr, 2009, Isherwood and Coetzee, 2011).

The ego-centric view to represent a social graph is therefore more relevant to the collectivist digital business ecosystem than the socio-centric view. Nodes are not aware of all other nodes in the network since there is no central controller or node which has an overall view of the network. Each node stores a local social graph of the connections or direct links. This supports more efficient computation with regards to storage and processing.

The next section performs an analysis on the different social network analysis centrality measures that can be used by a trust and reputation system for the collectivist digital business ecosystem.
5.5 Social network analysis for trust and reputation

To be able to understand how to apply social network analysis to collectivist digital business ecosystems, the measures that can be used needs to be identified. Centrality is a popular and commonly used social network analysis measure. Centrality provides an indication of a node’s position relative to the other nodes in a social graph (Wasserman and Galaskiewicz, 1994, Ortiz-Arroyo, 2010, Freeman, 1979, Wasserman and Faust, 1994, Daly and Haahr, 2009). For example, the degree centrality measure gives an indication of how connected a node in the social graph is. Since all centrality measures give an indication of the relative importance of a node within a social network, they can be useful in a trust and reputation system for the collectivist digital business ecosystem (Isherwood and Coetzee, 2011, Daly and Haahr, 2009).

In social graphs, trust is computed by considering the strength of the relationship between two nodes. The strength of the relationship can be based up many factors such as, the number of times nodes have interacted, past experience, and the context of pervious interactions. Also, factors such as, the number of the ego node’s connections that have interacted with another node, and how their past experience was with that node, can give an indication of relationship strength.

These factors are now investigated as they apply to types of trust namely (Golbeck, 2006, Daly and Haahr, 2009, Bentahar et al., 2009):

a) Direct trust
b) Indirect trust

In this section direct and indirect trust are discussed. Requirements are defined to determine which centrality measures can best assist with trust and reputation for collectivist cultures.

a) Direct trust

Direct trust exists between two nodes that have a trust relationship established, also referred to as individual trust (Hang et al., 2009, Noorian and Ulieru, 2010). Consider the case of just two nodes as depicted in Figure 5.4. SpazaShop A and Supplier A, taken from Figure 5.2, is labeled A and B respectively.
There are three elements that form trust, regardless of which definition is used, namely, the
trustor, trustee, and the state of trust (Dong et al., 2010, Bentahar et al., 2009). If Supplier A
(B), on the right, is the trustor and SpazaShop A (A), on the left, the trustee, $T_{BA}$ is the state of
trust. In other words, Supplier A trusts SpazaShop A, and $T_{BA}$ is the value of the trust that
Supplier A has in SpazaShop A.

It has already been noted that trust is subjective and therefore Supplier A does not necessarily
trust SpazaShop A to the same extent that SpazaShop A trusts Supplier A and vice versa.
This highlights the asymmetric and subjective properties of trust (Golbeck, 2006). The direct
trust value can evolve over time as the two SMMEs collaborate more often, thereby potentially
forming a stronger trust relationship, indicating the dynamic property of trust.

In a social graph, nodes have ties pointing to it and coming from it, which gives an indication
of the number of relationships a node has. This has a bearing on trust as the strength of
relationships is affected by either weak relationships or strong relationships. Therefore, the
number of relationships and strength of these relationships influence trust in the social graph.

b) Indirect trust
Transitive trust implies that if A trusts B and B trusts C then it is inferred that A can trust C to
some degree. The trust established from transitive trust is known as indirect trust as it is
determined by recommendations (Ziegler and Lausen, 2005, Jøsang et al., 2006).

Consider the case where the social network graph, from Figure 5.4 grows and more nodes
are linked together as depicted in Figure 5.5. Another SpazaShop B, shown as C, establishes
a relationship with Supplier A. There is direct trust between these two nodes, $T_{BC}$. However,
no relationship exists between SpazaShop A and SpazaShop B. If SpazaShop A would like to
collaborate with SpazaShop B it may ask Supplier A for a recommendation of SpazaShop B.
The transitivity property of trust can be used to assist SpazaShop A in its decision whether it
should trust SpazaShop B. Because of the number of links, trust can therefore be propagated through the network (Golbeck, 2006, Hang et al., 2009, Liu et al., 2010).

The reputation of Supplier A influences SpazaShop A's decisions on how much to trust SpazaShop B. If there were many nodes linked to both SpazaShop A and SpazaShop B, SpazaShop A could aggregate all the recommendations received about SpazaShop B. Indirect trust is therefore calculated from the recommendations among nodes related by connections in the graph.

Factors such as how long the path is between nodes, the number and reputation of the nodes along this path, how many nodes are present in the community, which nodes can extend the path for further connections, and what is the reputation of such nodes may all influence the indirect trust that exists between nodes.

c) Requirements for centrality measurement for the collectivist digital business ecosystem

In order to address the influence of culture on trust and relevance to the collectivist digital business ecosystem, centrality measures identified need to consider a number of requirements. The satisfaction of these requirements can ensure that a centrality measure is considered relevant for use in a trust and reputation system for the collectivist digital business ecosystem. The requirements are identified by the researcher to comply with the nature of the collectivist digital business ecosystem:

a) How does the centrality measure relate to direct trust or indirect trust?

b) Can the centrality measure be computed from an ego-centric view of the network?
c) What effect on trust does the centrality measure have?

The next section performs an analysis on centrality measures according to the requirements.

5.6 Analysis of centrality measures for the collectivist digital business ecosystem

The purpose of this section is to identify which centrality measures can assist with trust and reputation for the collectivist digital business ecosystem by supporting the requirements defined previously. Following a literature survey, the centralities to be discussed in this section are as follows:

- **Degree** (Freeman, 1979, Buskens, 1998)
- **Tie Strength** (Granovetter, 1973, Daly and Haahr, 2009)
- **Shortest Path** (Bilgin and Yener, 2010, Hang et al., 2009)
- **Density** (Granovetter, 1973, Buskens, 1998)
- **Clustering Coefficient** (Watts and Strogatz, 1998, Schilling and Phelps, 2007)
- **Closeness** (Freeman, 1979, Daly and Haahr, 2009)
- **Betweenness** (Freeman et al., 1991, Borgatti and Li, 2009)

Each of these centralities is now discussed with regards to previously defined requirements. This section also includes a summary of the analysis.

5.6.1 Degree Centrality

The degree centrality of a node is defined as the total number of connections the node has (Bilgin and Yener, 2010, Hupa et al., 2010). In a directed graph there are two types of degrees centralities, namely outdegree and indegree.

- Outdegree is the number of connections a node has to other nodes, i.e. the number of nodes that can be reached from a node in one hop (Buskens, 1998).
- Indegree is the number of connections a node receives from other nodes, i.e. the number of nodes that can reach a particular node in one hop.
Degree centrality of \( u_i \) is calculated as follows (Freeman, 1979):

\[
C_D(u) = \sum_{k=1}^{N} a(u_i, u_k)
\]

Where \( a(u_i, u_k) = 1 \) if a direct link exists between \( u_i \) and \( u_k \) otherwise it is 0, and \( i \neq k \).

In Figure 5.2, SpazaShop A has an indegree and outdegree of 2. Supplier S from Figure 5.2 has the highest degree centrality with an indegree of 9 and an outdegree of 7.

a) **Applies to direct trust** - the degree considers only the direct relationship that exists between two nodes in terms of the connections coming into and going out of a node.

b) **Ego-centric view** - since the degree centrality only requires knowledge of a node’s direct connections, it is measurable from an ego-centric view.

c) **The effect on trust** - degree centrality can be seen as a parameter that defines the extent to which a node conveys information about another node to the trustor (Bentahar et al., 2009). Therefore a node that is reliable has a higher outdegree than a node who is less reliable (Bentahar et al., 2009), meaning that they are able to convey information to more nodes. They have influence over other nodes and therefore play a role in disseminating and obtain trust and reputation related information, and are, themselves influential. However, should nodes with a high outdegree act maliciously, other nodes would soon disconnect from these nodes and therefore the outdegree of these node decreases, making them less influential within the network. Similarly, nodes with a higher indegree are able to receive more information from many other nodes and therefore make better decisions.

The degree centrality satisfies the requirements and is therefore appropriate for increasing or decreasing trust and reputation when considering the social graph in the collectivist digital business ecosystem.

### 5.6.2 Tie Strength

In social network analysis, tie strengths are classified as either strong ties or weak ties reflecting the strength of a relationship (Granovetter, 1973, Daly and Haahr, 2009). A weight is used to measure the strength of a tie and is represented as the weight of the edges in a
social graph (Granovetter, 1973). This weight can be in the form of a trust rating but is not limited to this.

In Figure 5.2, the tie strength of the relationship between SpazaShop A and Supplier A, represented as the weight of the edge connecting these two nodes, could be high, with a value of 0.8. This would be considered as a strong relationship provided the trust metric is real number on the scale [0, 1], where 1 is complete trust and 0 is no trust. In contrast, the tie strength of the relationship between SpazaShop B and Supplier A might be 0.3, which is therefore considered a weak tie.

a) **Applies to direct trust** - tie strength applies to direct trust since it considers a single relationship that exists between two nodes i.e. their direct connection.

b) **Ego-centric view** - tie strength centrality can be measured from an ego-centric view as it only considers direct connections.

c) **The effect on trust** - a strong tie can represent a strong trust relationship between two nodes and a weak tie can represent a weaker trust relationship between two nodes. Weak ties will have a weight relatively smaller than the weights of the connections a node regularly maintains, and the opposite is true for strong ties (Hupa et al., 2010). Therefore, a node with many strong ties is more trusted than a node with many weak ties.

Tie strength may be considered relevant to use in the collectivist digital business ecosystem. However, the challenge with this centrality measure is that it requires the weight of the edges to have trust values associated with them, making it more complex to establish the initial social graph.

### 5.6.3 Shortest Path

Indirect trust is computed using a number of paths that link two nodes. The challenge is to identify the shortest path between nodes. The shortest path $(\sigma_{st})$ between two nodes $s$ and $t$ in a social graph is defined as the geodesic distance between these nodes according to the unit length of the edges (Bilgin and Yener, 2010). The unit of length is the weight of an edge. This weight is not necessarily a distance measure but can also be, for example, the trust level...
of the relationship (Hang et al., 2009), or any other weight that is assigned to the edges in the social graph.

For example, in Figure 5.2, the shortest path from SpazaShop S to Supplier L would be through Supplier M, Supplier N, and SpazaShop O. The path length is 4 if the weight of each edge is 1. Alternative routes also exist but these routes are longer.

a) **Applies to indirect trust** - shortest path applies to indirect trust as it considers a path along which recommendations are provided and transitive trust is formed.

b) **Ego-centric view** - this measure is only computable from a socio-centric view and therefore cannot be applied to an ego-centric view of the social network graph.

c) **The effect on trust** - considering the transitive trust property and trust propagation, the shorter the path between two nodes, the more trustworthy the indirect trust value is (Golbeck, 2006, Hang et al., 2009). This is due to the fact that a node trust its direct contacts more compared to nodes that are further away. Therefore, the trust value of these nodes is less, leading to less trustworthy recommendations. This centrality relates directly to the transitive property of trust and can therefore assign lower weightings to recommendations from nodes that are further down the path. This is useful when considering recommendations from other nodes.

Since the shortest path centrality is not measurable from an ego-centric view, it is not suited to the collectivist digital business ecosystem.

### 5.6.4 Density

Density is the number of connections a node has, divided by the number of possible connections (Buskens, 1998). The density of a directed graph \(G(V, E)\) where \(V\) is the set of vertices and \(E\) the set of edges is calculated as:

\[
\text{Density} (G) = \frac{|E|}{(|V| \times (|V| - 1))}
\]

Therefore, taking the number of connections (164) and dividing it by the possible number of connections (49 * 48), the density of the social graph \(G\) in Figure 5.2 is:
Density centrality may be appropriate for computing trust and reputation in the collectivist digital business ecosystem.

### 5.6.5 Clustering Coefficient

A node’s clustering coefficient is defined as the proportion of alters that are themselves directly connected (Hupa et al., 2010, Schilling and Phelps, 2007). This metric therefore quantifies how close the node’s graph is to becoming a cluster or, in social networking terms, a clique (Bilgin and Yener, 2010). The clustering coefficient $C_i$ for a vertex $v_i$ is given below (Watts and Strogatz, 1998):

$$C_i = \frac{\text{number of triangles through } v_i}{\text{number of all possible triangles from } v_i}$$
Social network analysis for collectivist digital business ecosystem trust and reputation

\[ C_i = \frac{\left| \{e_{jk} : v_j, v_k \in N_i, e_{jk} \in E \} \right|}{k_i(k_i - 1)} \]

\( N_i \) is the neighbourhood to which \( v_i \) belongs, \( k_i \) is the number of neighbours of \( v_i \), \( e_{ij} \) is the edge connecting vertex \( v_i \) and \( v_j \) in a directed graph. In Figure 5.2, clusters are formed around Supplier A, I, P, and S. These nodes and nodes in the associated clusters have high clustering coefficients. For example, Supplier A has a \( C_{\text{SupplierA}} = \frac{5}{9*8} = 0.07 \) whereas Supplier B has a \( C_{\text{SupplierB}} = \frac{2}{9*8} = 0.03 \). A high clustering coefficient increases the transmission efficiency and information quality in the network by giving nodes the ability to assess all the information received.

a) **Applies to indirect trust** - clustering coefficient applies to indirect trust as it provides a property relating to a nodes community rather than a direct relationship between two nodes.

b) **Ego-centric view** - the clustering coefficient is measured from a socio-centric view where the complete social graph is known, making it easier to identify clusters. However, by considering the local density of a node’s ego-network, the local clustering coefficient can be determined (Wasserman and Faust, 1994, Scott, 2000). To create an overall local coefficient for the complete social network, the individual fractions are averaged across all the nodes in the network. Although this approach can be used to determine the clustering coefficient from an ego-centric view, it requires that all the nodes in the network are known, which is not the case in decentralized environment (Opsahl and Panzarasa, 2009). Therefore in the case of the digital business ecosystem, the clustering coefficient does not support the ego-centric view.

c) **The effect on trust** - as organisations collaborate with other organisations, they form stronger trust relationships and clusters tend to form (Schilling and Phelps, 2007). If nodes are clustered in trust groups the quality of recommendation information is increased (DuBois et al., 2009). This is possible as there are a number of direct relationships with each community participant. Therefore a number of direct trust values can be compared to get an accurate trust measures (Isherwood and Coetzee, 2011, DuBois et al., 2009, Schilling and Phelps, 2007), similar to the density centrality.
The clustering coefficient is not an appropriate centrality measure for trust and reputation systems for the digital business ecosystem, in terms of identifying clusters. Also, it does not satisfy the ego-centric view requirement.

5.6.6 Closeness centrality

Freeman (1979) identified the closeness centrality as the total distance to or from all other nodes, where distance refers to the number of links along the shortest path (Ortiz-Arroyo, 2010). Since closeness measures the distance to all other nodes, the shorter this distance is, the more central the node is (Varlamis et al., 2010). In other words, the closeness centrality identifies how connected a node is. A node that is highly connected has access to more information and is more reachable due to its central position within the network (Droege and Dong, 2007). The formula for determining closeness for a node \( p_i \) is as follows (Freeman, 1979, Daly and Haahr, 2009):

\[
C_C(p_i) = \frac{N - 1}{\sum_{k=1}^{N} d(p_i, p_k)}
\]

\( d(p_i, p_k) \) is the geodesic distance from \( p_i \) to \( p_k \), \( N \) is the number of nodes in the network and \( i \neq k \). In Figure 5.2, the node with the highest closeness centrality is SpazaShop U since this is the most central node in the social graph.

a) **Applies to indirect trust** - closeness applies to indirect trust since it represents the closeness of a node to all other nodes. This makes it relate to the complete social graph rather than a direct relationship between two nodes.

b) **Ego-centric view** - the closeness centrality is uninformative when viewed from an ego-centric view, since it requires the complete social graph to determine the closeness of a node, relative to all other nodes in the network.

c) **The effect on trust** - closeness is related to the shortest path in the sense that if a node is closer to you, the indirect trust values might be more accurate and reliable (Varlamis et al., 2010). If nodes are central but have a low trust, they should be avoided. Information should rather flow through nodes with greater trust and possibly less centrality (Isherwood and Coetzee, 2011, Droege and Dong, 2007). This could lead to information taking longer and less efficient routes in the network (Droege and Dong, 2007). Therefore, as a node's trust lowers, the closeness centrality of the node
also decreases. This is due to the fact that the node is bypassed so that a more trusted node can be used to transmit the information.

Closeness centrality for trust and reputation in the digital business ecosystem is not recommended due to the fact that it is not measurable in an ego-centric view.

5.6.7 Betweenness Centrality

Betweenness centrality is the measurement of the extent to which a node falls along a number of shortest paths connecting other pairs of nodes (Borgatti and Li, 2009, Hupa et al., 2010, Daly and Haahr, 2009, Varlamis et al., 2010, Freeman et al., 1991). A node has a high betweenness value based on the extent to which it exists on the shortest paths between all other pairs of nodes. This means that the node has control over these paths (Borgatti and Li, 2009). High betweenness nodes thus have the ability to enable interactions and control information flow between unconnected nodes (Daly and Haahr, 2009). The betweenness of a node \( p_i \) is calculated as follows (Freeman, 1979, Daly and Haahr, 2009):

\[
C_B(p_i) = \sum_{j=1}^{N} \sum_{k=1}^{j-1} \frac{g_{jk}(p_i)}{g_{jk}}
\]

\( g_{jk} \) is the total number of geodesic paths linking \( p_j \) and \( p_k \) and \( g_{jk}(p_i) \) is the number of those paths that include the node \( p_i \). Nodes with high betweenness values essentially act as “brokers” or “bridges”. This is due to the fact that there are no other short paths that can bypass this node with a high betweenness (Borgatti and Li, 2009). Consider Figure 5.2, nodes Supplier F and SpazaShop U have high betweenness values since they occur along many of the shortest paths connecting nodes.

Nodes with high betweenness values are very important within the network as the loss of these nodes can disrupt the structure of the network (Varlamis et al., 2010). Should a node with a high betweenness value in the digital business ecosystem no longer be in existence, this would impact a significant number of organisations negatively (Isherwood and Coetzee, 2011). For example, if node Supplier F or SpazaShop U fail, there would be no path by which nodes in the different clusters could connect with each other. This indicates how important these nodes are in establishing and maintaining a robust network structure.
a) **Affects indirect trust** - betweenness affects indirect trust as it gives information about a node's position in a social graph, rather than a direct relationship between two nodes.

b) **Ego-centric view** - Daly and Haahr (2009) prove that, to a large extent, the betweenness centrality can be calculated in both socio-centric and ego-centric networks providing a reliably similar value in both network views. This means that regardless of how the network and the trust relationships are viewed, i.e. globally or locally, the betweenness centrality value of a node can always be determined.

c) **The effect on trust** - a node with a high betweenness is central and has control over much of the information that passes through the network. This type of node achieves its central position as it is trusted by other nodes to control information flow (Stai et al., 2011). Similarly to the closeness centrality, a node loses this central position in the network should other nodes lose trust in this node, thereby decreasing its betweenness centrality. Therefore, a node with a high betweenness should be identified and treated as important nodes (Isherwood and Coetzee, 2011, Daly and Haahr, 2009, Stai et al., 2011) since they are considered as trustworthy and are important to the structure of the network. The betweenness centrality can be used to identify trustworthy nodes that provide connections among otherwise disconnected nodes and communities in the network.

The betweenness centrality may be appropriate for computing trust and reputation in the collectivist digital business ecosystem.

### 5.6.8 Summary of centrality measure analysis

Several centralities have been discussed thus far; however only a few are relevant to a trust and reputation system for the collectivist digital business ecosystem. Table 5.1 shows the summary of this analysis. The type of trust which the centrality supports is indicated in terms of direct and indirect trust. Also, the support for an ego-centric view is indicated as well as the effect a centrality measures has on trust.
Table 5.1 Analysis of centrality measures for the collectivist digital business ecosystem

<table>
<thead>
<tr>
<th>Centrality measure</th>
<th>Type of trust</th>
<th>Ego-centric view</th>
<th>Effect on trust</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Direct trust</td>
<td>Indirect trust</td>
<td></td>
</tr>
<tr>
<td>a) Degree</td>
<td>X</td>
<td>X</td>
<td>• Influence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Decisions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Connections</td>
</tr>
<tr>
<td>b) Tie strength</td>
<td>X</td>
<td>X</td>
<td>• Trust level</td>
</tr>
<tr>
<td>c) Shortest path</td>
<td>X</td>
<td></td>
<td>• Trust of recommendations</td>
</tr>
<tr>
<td>d) Density</td>
<td>X</td>
<td>X</td>
<td>• Strong trust groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Cohesiveness</td>
</tr>
<tr>
<td>e) Clustering coefficient</td>
<td>X</td>
<td></td>
<td>• Strong trust groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Recommendations</td>
</tr>
<tr>
<td>f) Closeness</td>
<td>X</td>
<td></td>
<td>• Influence</td>
</tr>
<tr>
<td>g) Betweenness</td>
<td>X</td>
<td>X</td>
<td>• Influence, control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Connections</td>
</tr>
</tbody>
</table>

It is clear to see that the degree, tie strength, density, and betweenness centrality satisfy all the requirements. However, as discussed, the tie strength represents the strength of the relationship. For the purpose of this study it can simply be the trust value that a node on one end of the edge has in the node on the other end of the edge in the directed social graph.

Therefore, for the purpose of this study, the next section discusses existing trust and reputation systems that specifically use degree, density, and betweenness centrality. The purpose of this is to evaluate current literature to determine how these centralities are used for trust and reputation.
5.7 Review of state-of-the-art research for trust and reputation systems supported by centrality measures

Trust and reputation systems that employ degree, density, and betweenness centrality measures are now discussed to gain an understanding of their use in current literature. The trust and reputation systems to be discussed are: PageRank (Page et al., 1999), TrustRank (Gyöngyi et al., 2004), a study by authors Gilsing et al. (2008), and BarterCast (Delaviz et al., 2010). Finally an evaluation of the results is given.

a) PageRank

PageRank (Page et al., 1999) is a well-known network graph-based reputation system. The PageRank algorithm uses hyper-links as a sign that one web page recommends another web page. PageRank can also be used to indicate the number of times a random surfer visits a web page, thereby reflecting the popularity and reputation of a web page. PageRank uses degree centrality to indicate the popularity of a web page, based on the number of connections coming in and going out.

The drawback of PageRank as a reputation measure is that all outgoing links from a node are considered equally, and not whether the interaction was a good or bad experience (Avrachenkov et al., 2007). In order to address this problem the TrustRank (Gyöngyi et al., 2004) algorithm was defined.

b) TrustRank

The TrustRank (Gyöngyi et al., 2004) algorithm computes trust scores for web pages based on a small data set that is provided by users who indicate if a web page was spam or not (i.e. good or bad).

The TrustRank algorithm uses degree centrality. Here, links are viewed as recommendations from other web pages. A web page that has links to other web pages is considered as recommendations to other pages, known as its outdegree. Conversely, all links to a specific web page from other web pages is considered as recommendations to the specific web page, known as its indegree.

These algorithms use the degree centrality to determine the popularity of a node (web page) regardless of whether they are popular for positive or negative behaviour. This is useful in trust and reputation systems that require the popularity of a node. A challenge is that additional
computation is needed to determine if the node is popular because it behaves well or because it behaves maliciously and has malicious supporting nodes.

c) Gilsing et al. (2008)
Gilsing et al. (2008) conducted a study on the usefulness of certain centrality measures to determine the innovation potential of a firm’s alliance network. They agree that a dense network facilitates the build-up of trust. This is because information received from neighbouring firms is richer and more reliable, and can be confirmed through the triangulations resulting from redundant connections. To determine the density of the network, they made use of the density centrality.

Together with the density centrality, Gilsing et al. (2008) consider the betweenness centrality of a node. They conclude that firms with a high betweenness and a high density centrality measure are able to yield potential for high exploration performance. This is due to the fact that they are in a position to receive different kinds of knowledge and information because of their high betweenness centrality and are able to verify information due to their high density centrality. This study does not explicitly indicate the effect such a position in the network has on the reputation of nodes.

d) BarterCast
Delaviz et al. (2010) uniquely make use of the betweenness centrality of nodes in the BarterCast reputation mechanism. BarterCast is used by a Bittorent-based file sharing client Tribler (2013) to compute reputation, not from the view of a node, but from the view of the node with the highest betweenness centrality. By computing reputation from the node with the highest betweenness centrality, they found that reputation values were more accurate but computation was less efficient.

The cost of computing betweenness centrality in large growing dynamic networks and periodically is prohibitive (Gkorou et al., 2011). However, after further experiments, Gkorou et al. (2011) conclude that using approximations methods, such as Scale-BC (Geisberger et al., 2008, Gkorou et al., 2011) and k-BC (Borgatti and Everett, 2006, Gkorou et al., 2011), for identifying nodes with a high betweenness in large scale-free networks, proved to be computationally less expensive and produced “excellent” reputation coverage and accuracy.

e) Evaluation
Current research discussed shows that the degree, density, and betweenness centrality are effectively used in popular, well-known trust and reputation systems, where the network is
represented as a social graph. However, there are some constraints when using these centrality measures:

- When using the degree centrality, additional computation and/or information are required to determine if the node is good or bad, in terms of reputation. The node may have many connections but this could be for malicious purposes.
- The density centrality is useful, but collusive malicious nodes can also form dense networks when working together.
- The most important constraint for the betweenness centrality is the computational costs required to calculate node’s betweenness. However, as computing power improves, these computations become less of an issue and as proven by Gkorou et al. (2011). Also, alternative methods have been defined to reducing the computation costs of determining such measures.

For the purpose of this study, these constraints need to be kept in mind.

### 5.8 Motivation of centrality measures for trust and reputation for the collectivist digital business ecosystem

Centrality measures used to determine information about a node in a network can provide valuable information that may be used to compute trust and reputation. In the previous chapter, trust properties were defined based on an analysis of collectivist cultures behaviour and its influence on trust. The properties were:

a) Members of a group that maintain group harmony are trusted more  
b) Members of a group trust in-group members more than out-group members  
c) Influential nodes such as group leaders are trusted more  
d) Out-group members can be trusted if they are recommended by in-group members

The focus is now to identify how centrality measures can be used to implement these trust properties to support the collectivist digital business ecosystem. For this discussion, the terms group, community and cluster are used interchangeably. They refer to a collection of nodes that are tightly connected to each other. All the properties imply that a group is identified and therefore, in this section, the identification of groups is discussed. It is also important to identify influential nodes and group leaders.

After centrality measures have been discussed to identify groups, group leaders and influential nodes, each of the trust properties for collectivist communities are discussed.
5.8.1 Centrality measures identifying groups, influential nodes, and group leaders

a) Identification of groups
For the purposes of this research, a group is considered as the ego-network of a node. Large groups form among nodes that are well-connected and may be strong cohesive groups if they are dense. Therefore, density centrality can be used to identify the strength of the group a node belongs to. A node with a high density centrality is thus considered as a member of a dense group. Consequently, many groups may be present in the collectivist digital business ecosystem, where dense groups are considered as strong groups where high levels of trust are present.

b) Identification of influential nodes
Influential nodes have the potential to control information and connect nodes that are otherwise disconnected (Everett and Borgatti, 2005). Influential nodes may be respected by others and may have a higher level of trust within their community (Varlamis et al., 2010). Also, influential nodes have the ability to establish collaborations and provide recommendations for members of the digital business ecosystem.

Influential nodes can be identified with two centrality measures namely: degree, and betweenness centrality, discussed next.

- **Degree centrality** identifies popular and well-connected nodes in the network by calculating the in-degree and out-degree of a node in the social graph. This determines the popularity of the node relative to its local community. A node with the higher in-degree may be trusted more, based on the number of connections and the strength of relationships. However, two issues arise. Firstly, malicious nodes in a network can also have many connections that are other malicious nodes, forming a collusive group that cooperate to disrupt the network (Xiong and Liu, 2004). Secondly, due to the fact that an ego-centric view is considered, the degree centrality measure of a node needs to be compared relative to the entire network. For example, should a node have an indegree and outdegree of 10, this may seem high in a network of 50 nodes but not 10 000 nodes.

- **Betweenness centrality** by definition identifies nodes in the network that are in central positions that control information flow and are therefore influential. Betweenness centrality is calculated for each node in the social graph. A node with a betweenness value greater than a predefined threshold is then be considered to have a high
betweenness (Daly and Haahr, 2009, Everett and Borgatti, 2005). The trust calculation can be done based on the level of betweenness as high betweenness nodes play a more influential role in the network. Therefore, the power that a node with high betweenness exerts over the environment should be carefully considered. A node with high betweenness centrality passes information such as recommendations to others, thereby creating a risk. Such a node can compromise information and behave opportunistically (Droege and Dong, 2007). To gain more power in a digital business ecosystem, a node may fail to pass important information to nodes that are dependent on this information (Varlamis et al., 2010) and thereby risk its position of power. If the other nodes should find this out, the node may lose its position in the network over time and its betweenness centrality will decline.

c) Identification of group leaders
Influential nodes have an influence throughout the entire social graph compared to group leaders who are influential within their ego social graph. A group leader is a member of a group that is trusted by all within the group. Group leaders play an important role as they provide recommendations to all members of the group, who are not risk takers by nature, thereby assisting them to make decisions. A group leader may also maintain information about the members of the group so that others outside the group can ask the group leader about the reputation of specific group members. This approach is used by Wang (2010) where a super-agent or super-peer is considered as a group leader. This approach shifts the architecture of trust and reputation from a decentralised architecture to a hybrid architecture. Regardless of which architecture is used, the degree centrality and the density centrality can be used to determine if a node is a group leader.

- **Degree centrality** is used to identify group leaders similarly to how influential nodes are identified. Once a group is identified, a comparison between group members is done where the group member with the highest degree centrality is considered as the group leader (Liu et al., 2012a).

- **Density centrality** is used to ensure that group leaders are more accurately chosen. The density centrality ensures that influential nodes of dense groups are considered as group leaders as these are highly trusted groups in a network. Dense groups have members that constantly collaborate in a successful manner (Govindan and Mohapatra, 2012, Wang, 2010) and work together to enhance their businesses and those of their groups and therefore the ecosystem. Since a dense group consists of many nodes connecting to each
other, there is an opportunity for nodes to receive information and be able to verify that information (Gilsing et al., 2008), making it more reliable. Therefore, more successful collaborations are established, within a dense group.

Next, each of the four trust properties are discussed with reference to centrality measures.

### 5.8.2 Members of a group that maintain group harmony are trusted more

The density centrality is used to identify strong cohesive groups where high levels of trust exist among group members (Coleman, 1988, Granovetter, 1992, Schilling and Phelps, 2007). The identification of such groups and associated group leaders assist to maintain the group harmony. Dense groups have members with high trust levels and are therefore perceived as trustworthy by outsiders. To maintain this perception and the group harmony, group leaders are available to provide recommendations to group members. The quality of recommendations from group leaders can guide group members to transact with nodes that will not disrupt the group’s harmony. Group leaders therefore attempt maintain group harmony and are also highly trusted by the other group members.

Members of groups that have group harmony need to behave in a manner that ensures they remain in the group. Should a member of such a group behave poorly and jeopardise the group harmony he/she will eventually be removed from the group. The group leader and other group member will not recommended such a malicious member based on previous transactions. The malicious member’s density and degree centrality will decrease as he/she loses connections as other members lose their trust in the member. Conversely, members that do not behave maliciously and maintain group harmony can be trusted as they enhance or maintain their density and degree centrality.

### 5.8.3 Members of a group trust in-group members more than out-group members

This trust property extends from the previous properties where groups and group leaders are identified using density and betweenness centrality, resulting in the identification of group members. A transaction with a member outside of the group requires recommendations from an in-group member (Moliea, 2007). This makes use of the collectivist cultural approach whereby members behave in a way so as to not jeopardise the group’s reputation. A group member therefore only recommends another if it has high trust in that node, and can be sure that they will not act maliciously.
The ability to accept recommendations from in-group members is extended to influential nodes that have a high social standing, as collectivists place trust in such persons based on their position. Here, betweenness centrality is used to identify influential nodes. This creates an opportunity for collaborations to occur outside the group but with good recommendations as though coming from in-group members.

5.8.4 Influential nodes such as group leaders are trusted more

Group leaders maintain group harmony and have many connections and influence over their group. Their high density and degree centrality ensure they are highly trusted by group members. However, group leaders also have to be responsible and maintaining their high trust level. Should a group leader begin to behave poorly, their density and degree centrality decreases similarly to other group members that behave poorly. Therefore, group leaders can be trusted more and would lose their position as group leader if they behave poorly.

Influential nodes, not necessarily group leaders, are identified using the betweenness and degree centrality. These nodes are required to establish new opportunities in a decentralised network. Such nodes are used by many other nodes to either connect to distant nodes or verify information and are thus trusted by many. Therefore, similarly to group leaders the position and importance of such nodes in the network, implies a certain level of trust. The degree and betweenness centrality of such nodes would also decrease if they behave poorly and therefore, decrease their influence in the network and their trust level.

The centrality measures identified can therefore identify influential nodes and according to this property, influence the trust computation and perception of such nodes.

5.8.5 Out-group members can be trusted if they are recommended by in-group members

This property enforces the collectivist cultural norm of having group harmony as priority. Responsibility is taken by a node when it makes a recommendation. The trust level of a node can potentially decrease should it recommend a node that does not behave in a manner that reflects its reputation. This ensures that dense groups that have strong trust relationships are able to maintain their positive group harmony. This trust property does not use a specific centrality measure but requires that dense groups are identified and in-group members take responsibility for the recommendations they provide.
Since it is a risk for in-group members to make recommendations, they can make use of nodes with a high betweenness, to identify potential collaboration nodes that can be considered trustworthy. Also, to ensure that in-group members take the risk and make recommendations, a reward mechanism can be implemented. For example, when a node makes a recommendation whereby the recommended node behaves satisfactory, the node that provided the recommendation can have its reputation enhanced by the system. Therefore, to implement this requirement, the density and betweenness centrality are used in an indirect manner through the satisfaction of the previous properties.

5.8.6 Summary of centrality measures for trust and reputation for the collectivist digital business ecosystem

Table 5.2 and 5.3 give the summary of the previous discussion indicating which centralities will be used to identify collectivist digital business ecosystem components and satisfy the trust properties for collectivist cultures, respectively.

Table 5.2 Centrality measures to identify collectivist digital business ecosystem components

<table>
<thead>
<tr>
<th>Identification of collectivist digital ecosystem components</th>
<th>Centrality Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>• Ego-network</td>
</tr>
<tr>
<td>Influential nodes</td>
<td>• Degree</td>
</tr>
<tr>
<td></td>
<td>• Betweenness</td>
</tr>
<tr>
<td>Group leaders</td>
<td>• Degree</td>
</tr>
<tr>
<td></td>
<td>• Density</td>
</tr>
</tbody>
</table>
Table 5.3 Centrality measures to satisfy collectivist cultural behaviour

<table>
<thead>
<tr>
<th>Trust property</th>
<th>Centrality Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Members of a group that maintain group harmony are trusted more</td>
<td>• Degree to determine group leaders that are trusted more</td>
</tr>
<tr>
<td></td>
<td>• Density to determine the trusted group</td>
</tr>
<tr>
<td>Members of a group trust in-group members more than out-group members</td>
<td>• Density to determine trusted groups</td>
</tr>
<tr>
<td></td>
<td>• Betweenness to obtain recommendations for trusted members outside the group</td>
</tr>
<tr>
<td>Influential nodes such as group leaders are trusted more</td>
<td>• Degree to determine the influence of influential nodes</td>
</tr>
<tr>
<td></td>
<td>• Density to identify trusted groups</td>
</tr>
<tr>
<td></td>
<td>• Betweenness to identify influential nodes outside the group</td>
</tr>
<tr>
<td>Out-group members can be trusted if they are recommended by in-group members</td>
<td>• Density to determine trusted groups (indirectly)</td>
</tr>
<tr>
<td></td>
<td>• Betweenness to identify influential nodes outside the group (indirectly)</td>
</tr>
</tbody>
</table>

5.9 Conclusion

In this chapter, the concept of social network analysis is introduced and motivated as a useful analysis tool for determining trust and reputation in the collectivist digital business ecosystem. To make full use of social network analysis the collectivist digital business ecosystem is represented as a social graph by using a social overlay network.

The resulting social graph of the digital business ecosystem is depicted in Figure 5.2, where VSEs and SMMEs are the nodes and their collaboration relationships are the edges. The different views of a social graph are then introduced, showing that a social graph for the digital business ecosystem can only make use of the ego-centric perspective due to its decentralised nature.

The types of trust are explained and social network analysis centrality measures are introduced. Centrality measures are identified as useful measures for obtaining additional trust
and reputation information from a social graph. This results in requirements being defined for a centrality measure to be appropriate for the collectivist digital business ecosystem.

An analysis is conducted on the different effects that centrality measures has on trust and reputation and the relevance to the collectivist digital business ecosystem. This analysis concludes that the degree, tie strength, density, and betweenness centrality are the relevant centrality measures. Tie strength is depicted by the weight of the edge and is used by default in the trust and reputation computation as the amount of trust one node has in another.

Existing systems and literature that use degree, density, and betweenness centrality are discussed, indicating that these centralities can be used for trust and reputation information.

Lastly, it is motivated that the degree, density, and betweenness centrality can be used to satisfy the collectivist cultural trust properties, making them useful for the collectivist digital business ecosystem.

The next chapter introduces the model for a trust and reputation system for the collectivist digital business ecosystem, satisfying the collectivist culture trust properties using social network analysis. The model is supported by the research conducted to this point, ensuring that an appropriate model is defined.
PART II
Chapter 6

Introducing Trust$_{cv}$ – a trust and reputation model for the collectivist digital business ecosystems

6.1 Introduction

The research to this point has provided a background and critical overview of current studies that support the development of a trust and reputation model for the collectivist digital business ecosystem. To create an understanding of a collectivist digital business ecosystem and how to facilitate successful collaborations, the properties of a digital business ecosystem were discussed and the current state of ICT technology in Africa was explored. It was concluded that a decentralised P2P architecture is required, where peers are represented by mobile devices and cloud infrastructure provides additional processing and storage capabilities. More importantly, culture was identified as a potential consideration to address to ensure business growth. Trust and reputation was explored for decentralised P2P networks, and this resulted in the selection of the PeerTrust model as the foundation of a trust and reputation model for the collectivist digital business ecosystem. To gain an understanding of the different cultures and their approach towards trust, the differences between individualist and collectivist cultures were explored. Four trust properties were identified to support collectivist norms and beliefs in Africa, making them relevant for the collectivist digital business ecosystem. The implementation of these trust properties ensure that collectivist communities are comfortable when using this environment. Trust properties were further explored, and it was determined that a social overlay network and social network analysis centralities such as degree, density, and betweenness can be used to satisfy these properties.

In part two of this research, the researcher set out to design a trust model to addresses collectivist cultures, called the Trust$_{cv}$ model where “$_{cv}$” is derived from collectivist. The major contribution of the Trust$_{cv}$ model is to demonstrate that it supports collectivist norms and beliefs in the collectivist digital business ecosystem, for business transactions and business partner selection.
The section that follows presents the architecture of the Trust\textsubscript{cv} model. Next, the components of the Trust\textsubscript{cv} model are discussed. Finally a use case for the Trust\textsubscript{cv} model is provided.

### 6.2 Trust\textsubscript{cv} architecture

The purpose of the research is to enhance trust and reputation in the collectivist digital business ecosystem by supporting collectivist culture norms and beliefs. To achieve this, transactions and transaction partner selection needs to be done according to a culturally specific manner. This can increase trust in the system and each other, as people in collectivist communities would be more comfortable with the manner in which the system behaves. The Trust\textsubscript{cv} model aims to achieve this by defining a model that can be implemented in the collectivist digital business ecosystem, on SMMEs mobile devices, desktop and laptop computers, and cloud infrastructures. The architecture of the Trust\textsubscript{cv} model is illustrated in Figure 6.1.

Since the PeerTrust model forms the architectural foundation of the Trust\textsubscript{cv} model, the architecture depicted in Figure 6.1 is adapted from the PeerTrust system architecture. However, new components are introduced, such as the Cloud Infrastructure component and the Social Graph module, which are specific to the Trust\textsubscript{cv} model. Also, mobile devices and personal computers represent the peers in the Trust\textsubscript{cv} architecture.

Figure 6.1 indicates that a Trust\textsubscript{cv} model implementation, known as an agent, can be hosted either on the device used to represent the SMME in the digital business ecosystem or on the Cloud. A SMME can install or run the appropriate agent depending on the computing infrastructure available to the SMME. For example, if the SMME does not have compatible mobile device, the SMME can make use of an agent for a personal computer or a Cloud implementation of the agent.
Introducing Trustcv – a trust and reputation model for the collectivist digital business ecosystems

All agents have the same features of the Trustcv model, however, the different versions of the agent are adapted to make use of the computing infrastructure on which they are hosted. The agent has the following main functionalities:

i. Receive feedback and other input from the SMME representative – the user who interacts with the system on behalf of the human SMME

ii. Interact with other SMME agents

iii. Perform trust computations for the Trustcv model

In order to understand the operation of the Trustcv model, consider the following: suppose SpazaShop A would like to collaborate with another spaza shop in the collectivist digital business ecosystem, to participate in a bulk buying cooperative. SpazaShop A’s owner uses the agent on his/her mobile device, personal computer, or cloud implementation, by specifying requirements such as the service required, location, and date. The agent determines a list of spaza shops in its local set of connections or remote connections that are suitable for the type
of transaction. A list is presented to the owner of spaza shop A, who may not know the reliability of the spaza shops to be able to make an informed decision.

Here, the Trust\textsubscript{cv} component performs an analysis to provide SpazaShop A’s owner with information about potential partners to transact with, and presents this information to the SpazaShop A so that an informed decision can be made. As it is visible that group leaders of the community have recommended some of the spaza shops, the spaza shop owner feels comfortable to make a choice. In turn, the selected cooperative partner is presented with a request and similar information, to make an informed decision to cooperate. Finally a transaction is performed that leads to cost savings and business growth for all parties.

The Trust\textsubscript{cv} model implementation performs analysis to provide trust and reputation information to SMMEs such as spaza shop A. To achieve this, it makes use of four main components, namely: Trust Manager, Data Locator, Trust Data, and Transaction Tool. These components are discussed in more detail in the next section.

### 6.3 Trust\textsubscript{cv} components

A description of the Trust\textsubscript{cv} architecture components is provided in this section so as to gain an overview of the Trust\textsubscript{cv} model. As previously discussed, the Trust\textsubscript{cv} model is derived from the PeerTrust model, extensively discussed in chapter 3. Some information is repeated in this chapter to provide a clear understanding of the Trust\textsubscript{cv} model.

#### 6.3.1 Trust Manager

The Trust Manager, shown in Figure 6.1, consists of three main components:

- i. Submit feedback from a transaction with other SMMEs in the network, through the Data Locator using the Feedback Submission module.
- ii. Evaluate the trustworthiness of another peer according to the Trust\textsubscript{cv} trust computation using the Trust Evaluation module.
- iii. Perform social network analysis on the SMMEs ego-network using the Social Graph module and make the analysis results available to the Trust Evaluation module.

In summary, the Trust Manager is responsible for determining the trust level of other SMMEs in the network and maintains the social graph of all connected nodes.
6.3.2 Data Locator

The Data Locator is responsible for locating data from other SMMEs in the P2P network by making use of routing tables. Additionally, the data locator is responsible for locating local data stored in the Trust Data component and providing data manipulation instructions to the Trust Data component. The Data Locator ensures that any information that is accessible and required by the Trust Manager can be located.

6.3.3 Trust Data

The Trust Data component represents a data store that stores the data maintained by the Trustcv implementation. This data is typically in the form of feedback information received after transactions have occurred. Additionally, the Trust Data component caches information relating to the ego-network social graph such as relationships and social network analysis results.

6.3.4 Transaction Tool

The Transaction Tool provides a tool for a collectivist digital business ecosystem member, so that they can transact using Trustcv. The tool provides the ability for a SMME to specify a service, known as ServiceType, it desires. For example, a spaza shop may desire bulk buying (BulkBuying) as a service. All other spaza shops willing to collaborate for this purpose also expose the ServiceType, BulkBuying.

Additionally, the tool provides the ability to initiate and complete a transaction, and submit feedback once the transaction is finished. SMMEs can select other SMMEs to transact with based on trust and reputation information provided. Feedback is submitted in the form a satisfaction rating which the SMME provides based on how the other SMMEs performed in the transaction.

The Trust Manager, Data Locator, and Trust Data components are the main components of the Trustcv model and their functionality is made available via the Transaction Tool. The next section provides a use-case design to demonstrate the behaviour of the Trustcv model.
6.4 Trust\textsubscript{cv} use-case design

Trust\textsubscript{cv} is a P2P architecture, exposing both client and server behaviour. Servers produce and offer services and clients consume them. Figure 6.2 is a UML (Unified Modelling Language) use-case diagram of Trust\textsubscript{cv} to explain its basic behaviour. UML is an industry-standard language for modelling of software engineered systems, including specification, visualisation, construction and documentation (Hamilton, 1999, Bennett et al., 2001).

![CollectoTrust Diagram](image)

**Figure 6.2 Trust\textsubscript{cv} UML use-case**

The discussion that follows provides a description of all the components in the Figure 6.2 and how they relate to each other.
a) Actors

The actors include:

i. User (Collectivist digital business ecosystem member)
Collectivist digital business ecosystem members, in the form of a SMME owner or SMME representative, manage collaborations and transactions with other SMMEs. This is a human user that interacts with the Transaction Tool from their mobile device, or other computing system. This actor generalises the action of a Client or a Server actor.

ii. Client
A Client makes use of Service Consumption to consume collaboration service(s) offered by a server.

iii. Server
A Server makes use of Service Advertisement to advertise the collaboration service(s) it offers.

iv. System (Agent)
This is an autonomous entity that manages the Trust Manager, Data Locator, and Trust Data components and provides a Transaction Tool for interaction with the User.

b) Service Advertisement
Service Advertisement exposes services offered by a SMME in the collectivist digital business ecosystem. Services can be offered digitally and autonomously via a service interface or these may be simple indicators of physical services that a SMME offers.

c) Service Consumption
Service Consumption entails the discovery and consumption of services. Services are consumed digitally and autonomously or they indicate whether a service has been physically consumed by a SMME.

d) Transaction Tool
The Transaction Tool provides an interface for Users to interact with the Trustcv model. Users input information into the system, consume system output, and instruct the system from the Transaction Tool.
Introducing Trustcv – a trust and reputation model for the collectivist digital business ecosystems

**e) Trust Manager**
The Trust Manager integrates and combines data received from the Feedback Submission, Trust Evaluation, Social Graph, and Data Locator components to provide information to the Transaction Tool. Additionally, it also provides input into these components the form of data and instructions.

**f) Feedback Submission**
The Feedback Submission component maintains the feedback received from the User through the Transaction Tool and Trust Manager, so that the correct feedback information can used when computing trust in the Trust\textsubscript{cv} model.

**g) Trust Evaluation**
The Trust Evaluation model receives instructions and data from the Trust Manager which it uses to compute trust in the Trust\textsubscript{cv} model and return trust related information to the Trust Manager.

**h) Social Graph**
The Social Graph model performs social network analysis on a graph based on the data and instructions it receives from the Trust Manager. Once it performs social network analysis, the results are returned to the Trust Manager that uses them as input to make decisions or compute trust.

**i) Data Locator**
The Data Locator assists the Trust Manager by locating data in the system and/or network that is required by the Trust Manager to compute trust in the Trust\textsubscript{cv} model.

**j) Trust Data**
The Trust Data provides persistence for the Trust\textsubscript{cv} model by storing any data that is required for later use by the agent and its other components.

All these components work together to make the Trust\textsubscript{cv} model available for the collectivist digital business ecosystem.

**6.5 Conclusion**

This chapter identified the architecture, components, and behaviour of the Trust\textsubscript{cv} model. The system architecture illustrated the main components which included the Trust Manager, Data
Introducing Trustcv – a trust and reputation model for the collectivist digital business ecosystems

Locator, Trust Data, and Transaction Tool. A description of these components where provided together with an overview of the system flow, indicating the interaction between these components.

A UML use-case diagram was presented to show the object-oriented design of the Trustcv model and how its components interact as objects. A description of the actors was also provided depicting interaction with the Trustcv model.

The following chapter discusses and formally models the Trustcv model. This is followed in the next chapter by a simulation and evaluation of the Trustcv model.
Chapter 7

Trust\textsubscript{cv} model

7.1 Introduction

In this chapter, the Trust\textsubscript{cv} model is modelled and discussed in more detail with the aim of satisfying the requirements set out by the research discussed to this point.

The Trust\textsubscript{cv} model is applied when SMMEs consider basic factors such as the service required, the scope for selecting SMMEs that offer the service, and the selection of a transaction partner. When selecting a transaction partner, the SMME needs to decide if the potential transaction partner can be trusted to deliver the required service. To determine such trust, the Trust\textsubscript{cv} model takes into account previous experiences and recommendations from others. Questions such as: what is considered trustworthy; which SMMEs do I know have transacted with this SMME; and can other information be sourced to better predict their behaviour; need to be answered by the Trust\textsubscript{cv} model.

The contribution of the Trust\textsubscript{cv} model is to support collectivist communities, to ensure that they are comfortable with their decisions, as they understand that they are supported to behave in a manner that does not compromise group harmony. In order to achieve this, recommendations need to be sourced from SMMEs that are trusted by the group and who enjoy good social standing in the community. In addition, malicious behaviour from SMMEs need to be handled in a manner that complies to the mindset of collectivist communities.

The Trust\textsubscript{cv} model aims to address the identified trust properties and more, to create an environment that can facilitate trustworthy transaction among different entities. As discussed previously, the foundation of the Trust\textsubscript{cv} is PeerTrust (Xiong and Liu, 2004) which satisfies many of the properties discussed this far (Chaokai and Meng, 2010, Noorian and Ulieru, 2010, Mármol and Pérez, 2011). However, Trust\textsubscript{cv} aims to additionally satisfy the collectivist cultural properties identified previously.

In the remainder of this chapter, the collectivist cultural trust properties are revisited. This is followed by the modelling and discussion of the basic trust model, which is for the most part based on the PeerTrust model. Next, the social graph constituents of Trust\textsubscript{cv} are presented.
The operations and associated algorithms specific to Trust\textsubscript{cv} are modelled and its support for collectivist cultural trust properties is discussed. Finally, the chapter is concluded.

### 7.2 Trust\textsubscript{cv} model properties

In order to define a trust model that meets the norms and beliefs of collectivist communities in digital business ecosystems, four trust properties were identified in chapter 4. These trust properties aim to enhance business growth by ensuring the development of strong cohesive groups with a high level of harmony, to meet the needs of the community. These properties are now revisited to focus the development of the Trust\textsubscript{cv} model.

| a) | Members of a group that maintain group harmony are trusted more |
| b) | Members of a group trust in-group members more than out-group members |
| c) | Influential members such as group leaders are trusted more |
| d) | Out-group members can be trusted if they are recommended by in-group members |

In the following sections, the basic PeerTrust model is discussed as the foundation for Trust\textsubscript{cv}. The Trust\textsubscript{cv} model is then described, with unique constituents and operations that address centrality measures and algorithms that support collectivist cultures.

### 7.3 Basic trust model constituents and operations

The constituents and operations of the PeerTrust model are now presented in the context of the Trust\textsubscript{cv} model. This section is discussed according to the following structure:
1. Trust environment
   a) SMME profile
   b) Set of SMMEs
   c) Set of Agents

2. Trust constituents and operations
   a) Trust level
   b) Transaction feedback
   c) Transaction feedback scope
   d) Credibility of transaction feedback source
   e) Transaction context
   f) Community context factor
   g) Trust threshold

3. Trust computation

7.3.1 Trust environment

The trust environment encapsulates the basic components of the collectivist digital business ecosystem. In this section, the SMME profile, SMMEs, and Agents are discussed and modelled.

a) SMME profile

An important aspect to address is the unique identification and profiling of participating entities. To become a member of the collectivist digital business ecosystem, SMMEs create a profile when joining. The creation of the SMME profile is performed by the Transaction Tool component of the Trustcv agent. An SMME profile contains information such as the unique identifier, company name, representative, services offered, email address, and other SMME related information. The SMME profile can be extended to include more complex data types such as location, pictures, and advertisements.

An SMME profile is defined as a set of attributes as:

\[ SP \in \{attr_1, attr_2, \ldots, attr_n\}. \]

In the Trustcv model, the SMME profile is a custom data structure understood by implementations of the Trustcv model. The history of transaction partners and previous experience is also linked to the SMME profile but is not included in the profile which is accessed by other SMMEs in the collectivist digital business ecosystem.
b) Set of SMMEs
An SMME is defined by an SMME profile and is uniquely identified by an email address and/or a unique id. The SMME is responsible for the final selection of transaction partners and for the provision of satisfaction ratings based on the transaction partner(s).

An SMME refers to a business that is a member of the collectivist digital business ecosystem. The set of SMMEs is defined as:

\[
\text{SMME} \in \{\text{smme}_1, \text{smme}_2, \ldots, \text{smme}_n\}.
\]

c) Set of Agents
An agent is deployed on the SMME’s computing device, such as a mobile device, personal computer, or cloud infrastructure. An agent is a representation of the SMME in the system and is responsible for the maintenance of the SMME profile, to provide recommendations, and determine the trust level of other SMMEs. Each agent is uniquely identified by a unique id.

The set of agents that correspond to the set of SMMEs is defined as:

\[
A \in \{a_1, a_2, \ldots, a_n\}.
\]

The SMME profile, set of SMMEs, and the set of agents, together contribute towards the establishment of the collectivist digital business ecosystem environment. The constituents and operations which enable the calculation of trust and reputation in this environment are discussed in the next section.

7.3.2 Trust model constituents and operations

a) Trust level
For the purpose of this research, the trust level represents the extent to which a SMME trusts another SMME. The trust level is a real number in the range \([0,1]\) where 0 indicates no trust in another SMME and 1 indicates complete trust in another SMME.

A trust level is defined as follows:

\[
T_l \in [0,1]
\]
The trust level is the central component of a trust model as it quantifies how much a node can be trusted. A SMME in the collectivist digital business ecosystem is initially assigned a default trust level which changes over time as the SMME transacts with other SMMEs. SMMEs use the trust level extensively in the collectivist digital business ecosystem as it influences the selection of transaction partners. The trust level of SMMEs is built up from the behaviour of SMMEs during transactions and the associated feedback which is discussed next.

**b) Transaction feedback**

Transaction feedback from an SMME refers to the satisfaction rating an SMME gives another SMME after they have transacted. This rating is manually provided by the SMME, based on their evaluation of the service that was provided. Transaction feedback is a real number value in the range $[0,1]$ where 0 indicates that an SMME is completely unsatisfied, and 1 indicates that the SMME is completely satisfied with the service offered.

Transaction feedback received, once a transaction $i$ is complete, for the service provided by a SMME $u$ is defined as follows:

$$S(u, i) \in [0,1]$$

Upon determining the transaction feedback of an SMME, recommendations from other SMMEs that have previously interacted with SMME $u$ is considered as the transaction feedback. The transaction feedback directly influences the trust value as SMMEs use the transaction feedback to compute the trust value of other SMMEs. However, transaction feedback should be with a particular scope so it can be relevant for trust computations. This is discussed next.

**c) Transaction feedback scope**

The transaction feedback scope refers to the number of transactions a SMME has participated in, within a given time frame $[t_s, t_e]$, where $t_s$ is the start time and $t_e$ is the end time. This gives an indication of how active a SMME is, in the collectivist digital business ecosystem.

Transaction feedback scope for a SMME $u$ in the time frame between $t_s$ and $t_e$, is defined as follows:

$$I(u) \in [t_s, t_e]$$
I(u) is used to limit the transactions which are considered as input to recent transactions, when the trust level of an SMME is computed. This ensures that computed trust levels are relevant to the recent behaviour of a SMME (Xiong and Liu, 2004).

d) Credibility of transaction feedback source
The credibility of the transaction feedback source provides an indication of the weighting the trust computation should assign to the transaction feedback provided by a SMME. If the credibility of the SMME is low, their feedback has less significance in the trust calculation. Credibility is determined at the time when the feedback was submitted. In the PeerTrust model, a trust value metric (TVM), is used to compute the credibility of a peer (Xiong and Liu, 2004). Therefore, the credibility of a SMME $u$ is based on level of trust $v$ has in SMME $u$ when $u$ provided its transaction feedback. This is defined as follows:

$$
Cr(u) = \frac{T(p(u,i))}{\sum_{i=1}^{I(u)} T(p(u,i))}
$$

where $T(p(u,i))$ is the trust level of $u$ at the time of transaction $i$.

e) Transaction context
The context of the transaction influences the weighting of a trust value for that transaction. For example, a transaction that occurs with a high risk, e.g. R1 000 000 investment, has a higher transaction context, and vice versa. The transaction context of transaction $i$ with SMME $u$ is modelled as:

$$
TF(u, i) \in [0,1]
$$

The context of the transaction is a relative value since different SMMEs have different perspectives on what is considered a high or low transaction context value. Therefore, the value is decided by participating SMMEs for a particular transaction, or is a predetermined value based on the structure and profile of the SMMEs participating in the collectivist digital business ecosystem.

f) Community context factor
The community context factor is used as an incentive to encourage SMMEs in the ecosystem to provide feedback for transactions (Xiong and Liu, 2004). In the PeerTrust model, a peer can increase its reputation by providing transaction feedback. However, in the Trustcv model,
the community context factor is a dynamic value associated to a SMME based on their behaviour. SMMEs that provide accurate recommendations achieve a higher community context factor than those that provide inaccurate recommendations. The community context factor for an SMME $u$ is modelled as:

$$Cr(u) \in [0,1]$$

The computation of a SMMEs community context factor is defined in Equation 6 and 7 which is defined later in the chapter.

g) Trust threshold

When a SMME collaborates with others in the collectivist digital business ecosystem, the SMMEs can grow their business and access more business opportunities. Therefore, when an SMME wants to collaborate with another SMME, they require some reference about the level of trustworthiness of the other party. This reference is known as the trust threshold $u$ and is defined as follows:

$$T_{\text{threshold}}(u) \in [0,1]$$

A trust threshold allows a SMME to set an acceptable level of trust for unknown or known SMMEs that may be suggested by the system for a transaction. Therefore, in the Trustcv implementation, only SMMEs above this threshold are selected as transaction partners.

The trust threshold value for an SMME may change over time depending on their circumstances, previous experience, transaction context, and business service required for a transaction. For example, a SpazaShop S may not necessarily require another SMME to have a very high trust level for a transaction with a transaction context factor of R100. The risk is low, and therefore, SpazaShop S's trust threshold may be defined as 0.3 as depicted below:

$$T_{\text{threshold}}(\text{SpazaShop S}) = 0.3$$

Additionally, the environment may define a basic trust threshold for all SMMEs. If the level of malicious activity is high, the trust threshold may be set higher to avoid malicious transactions. Therefore a SMME can alter their trust threshold based on these factors, through the Transaction Tool, or this can be set to a standard trust threshold for the all SMMEs that participate in the collectivist digital business ecosystem.
The components discussed in this section lead to the trust computation for PeerTrust and Trustcv, which is presented in Chapter 3. The next section revisits this trust computation as it computes the trust level of SMMEs in the collectivist digital business ecosystem.

### 7.3.3 Trust computation

The trust level computation is performed by the Trust Evaluation component in the Trustcv and PeerTrust system architecture. Equation 1, the formula for computing the trust level of a SMME is:

\[
T_l(u) = \alpha \times \sum_{i=1}^{I(u)} S(u, i) \times Cr(p(u, i)) \times TF(u, i) + \beta \times CF(u) \tag{Equation 1}
\]

The parameters of Equation 1 were previously discussed, and the list below describes the parameters from the perspective of the collectivist digital business ecosystem:

- \( T_l(u) \) – The trust level of a SMME \( u \).
- \( I(u) \) – The total number of transactions performed by SMME \( u \) with all other SMMEs.
- \( p(u, i) \) – The other participating SMME in SMME \( u \)'s \( i \)’th transactions
- \( S(u, i) \) – The normalised transaction feedback SMME \( u \) receives from \( p(u, i) \) in its \( i \)’th transaction.
- \( Cr(p(u, i)) \) – The credibility of the transaction feedback submitted by \( p(u, i) \).
- \( TF(u, i) \) – The adaptive transaction context factor for SMME \( u \)'s \( i \)'th transaction.
- \( CF(u) \) – The adaptive community context factor for SMME \( u \)
- \( \alpha \) and \( \beta \) denote the normalised weight factors for the collective evaluation, and community context factor, respectively.

This formula is used to calculate the trust level \( (T_l) \) of SMME \( u \). This trust level gives a very good estimation of the quality of the service provided, given the five parameters that are used in the calculation, and is therefore suitable to use by SMMEs. A SMME’s agent performs this calculation to determine the trust level of another SMME. This occurs when a SMME requests a recommendation, or when the SMME wants to transact and computes the trust level of its own connections. The SMME with the highest trust level is consequently selected as partner. This manner of partner selection thus supports the way in which individualistic cultures make decisions. This section has defined the trust environment for the digital business ecosystem, the main constituents and operations and finally the trust computation. The trust constituents and operations in this section provide the foundation of the Trustcv model which is based on the PeerTrust model. According to the research conducted in the study, the specific trust
properties, presented in Section 7.2, needs to be satisfied for trust and reputation in the collectivist digital business ecosystem. The implementation of trust properties do not modify the basic trust computation, but rather addresses the manner in which partners are selected.

In order to implement identified trust properties, the specific contribution of the Trust$_{cv}$ model is now described. Section 7.4 introduces the Trust$_{cv}$ model social graph constituents. Thereafter section 7.5 describes the Trust$_{cv}$ model operations and algorithms to supports collectivist norms and beliefs in the collectivist digital business ecosystem.

### 7.4 Trust$_{cv}$ model social graph constituents

The Trust$_{cv}$ model social graph constituents add the components necessary to extend the basic trust model. This section discusses the extensions to the basic trust model according to the structure given below. First, social graph concepts are introduced and then centrality measures used in the model are defined.

1. SMME’s ego-network social graph
   a) Ego-network social graph
   b) Ego-network social graph representation
2. Centrality measure calculations
   a) Degree centrality for ego-networks
   b) Density centrality for ego-networks
   c) Betweenness centrality for ego-networks

#### 7.4.1 SMME’s ego-network social graph

The decentralised architecture of the collectivist digital business ecosystem dictates the use of ego-networks, where a node considers the node (actor), its friends (alters) and all the connections between them. In the collectivist digital business ecosystem, this is known as the SMME’s ego-network and is represented by a social graph. For the purpose of the following discussions, the term “node” is used to refer to the SMME agent in the ego-network social graph.

For the purpose of this discussion, a simple scenario is now considered: Consider the ego-network social graph of SpazaShop S, depicted in Figure 7.1, which is based on Figure 5.2. It indicates that SpazaShop S has a direct connection to SpazaShop T, SpazaShop R and Supplier P. The value on the edge between each node is the trust level (T$_l$) that a node has
assigned to another node. For example, SpazaShop S has assigned a trust level of 0.65 to SpazaShop R. This trust level is computed by Equation 1, discussed previously.

Figure 7.1 SpazaShop S Ego-network

a) Ego-network social graph

An ego-network social graph follows on the same definition of a social graph which is \( G = (V, E) \). The ego-network social graph is smaller than the social graph of the entire network due to its local scope.

i. Vertices

In an ego-network social graph \((G)\), the vertices \((V)\) are defined by a non-empty set of vertex \(v\) elements. A vertex \(v\) represents the SMME and the software agent \(A\) that acts on behalf of the SMME:

\[
v = \text{SMME} \cup A
\]

ii. Edges

In the ego-network social graph, relationships between vertices are defined by edges. The value of each edge is based on at least one transaction that occurs between two SMMEs. In the ego-network social graph for Trust\(_{cv}\), edges are directed and weighted. The weight of an edge represents the trust level that the vertex at the start of the edge has in the vertex at the end of the edge.

A weighted edge from vertex \(u\) to vertex \(v\) is represented by \(W(u,v)\). The weighted edges range between \(\{W(i,1) \cdots W(i,n)\}\) where the set of transaction connections \(\nu = \{1, \ldots, n\}\)
excluding \( i \). Since the graph is directed, the weighting of the edges is asymmetric meaning that \( W(i, j) \neq W(j, i) \) where \( i, j \in v \). It may occur that \( W(i, j) = j, i) \) where \( i, j \in v \) but it is not enforced. For example, in Figure 7.1, SMMEs assign different trust levels to each other.

b) Ego-network social graph representation

To represent the ego-network social graph, an adjacency list data structure is used. Here, SMMEs in the ego-network are represented as indexes in an array. The SMMEs connected to that node are themselves a list. For example, consider the ego-network of SpazaShop S in Figure 7.1. The resulting ego-network social graph representation for SpazaShop S is depicted in Figure 7.2.

![Figure 7.2 Adjacency list representation of SpazaShop S ego-network social graph](image)

The names or ids of SMMEs, such as SpazaShop S, are used for representational purposes but ideally a unique key should represent a SMME. Also, since the social graph used by the collectivist digital business ecosystem is weighted, each node contains an associated weight, that corresponds to the weight of the edge between the node in the array, and the node in the list associated with that node. In the previous example, the trust level SpazaShop S assigns to SpazaShop R is 0.65 as depicted in Figure 7.2.

One alternative data structure for social graph representation is an adjacency matrix (Golumbic, 2004, Cormen et al., 2001). This structure is a 2D \( M \times M \) array, where \( M \) is the number of nodes in the social graph. Each intersecting index in the array contains the weight.
of the edge between the node in the column and the node in the row of the matrix, and zero if the node in the column and row is the same node. The representation of the social graph as an adjacency list has the following advantages over an adjacency matrix representation (Golumbic, 2004):

- In an adjacency list, space complexity is proportional to the number of connections a node has. In an ego-network, this is relatively small. Whereas an adjacency matrix uses $M \times M$ space, which is less space efficient if the nodes in the network are not all connected to each other.
- Operations such as getting the neighbours of a node run in constant time in an adjacency list. In an adjacency matrix, such an operation would require more iterations to determine who is a neighbour of a particular node.

Although an adjacency list has some advantages over an adjacency matrix, there are other implementations, such as incident lists and incident matrices (Cormen et al., 2001). Therefore, the ego-network social graph representation is not restricted to the adjacency list implementation but could use any implementation that is able to efficiently represent a social graph.

### 7.4.2 Centrality measure calculations

The Trustcv model uses degree, density, and betweenness centralities that are calculated by the Social Graph component of the Trustcv model. In this section, the calculation of centrality measures in an ego-network social graph is modelled so that their values can be used by the Trustcv model. The centrality measure equations presented in this section have already been discussed in chapter 5 and are adapted and discussed in accordance with the Trustcv model.

#### a) Degree centrality for ego-networks

The degree centrality for ego-networks determines the number of connections a node has relative to the other nodes in the ego-network. A node calculates its degree centrality so that other neighbouring nodes can request it. In a directed graph, degree consists of indegree and outdegree. The equation used to calculate either indegree or outdegree of a node $u$, is defined is previously presented in chapter 5 and is as follows:

$$\text{Indegree/Outdegree}(u) = \sum_{k=1}^{N} a(u_i, u_k)$$  \hspace{1cm} (Equation2)
The degree centrality, in the form of indegree and outdegree, is thus simple to calculate. For the purpose of this study, degree centrality is considered as the average of the combination of indegree and outdegree, defined in Equation 2:

$$\text{degree}(u) = \frac{\text{indegree}(u)+\text{outdegree}(u)}{2}$$  \hspace{1cm} \text{(Equation 3)}

Data, such as the number of incoming connections can be identified by the number of links a node has in the adjacency list. The number of outgoing connections can be identified as the number of times a node appears in another node’s links, in the adjacency list of the ego-network. Other nodes can then request this node’s degree centrality during a trust computation for that node.

\[ b) \text{ Density centrality for ego-networks} \]

The density centrality for ego-networks determines how densely populated an ego-network is. A node can determine the density of its own network and this information can be made available to other neighbouring nodes, which request it. The equation used to calculate density of a node u’s social graph \( A \), is depicted in Equation 4.

$$\text{Density} (A) = \frac{|E|}{(|V|*(|V|-1))}$$  \hspace{1cm} \text{(Equation 4)}

The density of a node’s ego-network is essentially the ratio of the number of edges in the ego-network to the total number of possible edges in the ego-network. To determine this, the adjacency list is iterated over to determine the number of actual connections and is then divided by the number of possible connections.

\[ c) \text{ Betweenness centrality for ego-networks} \]

The betweenness centrality determines if a node is a “bridge” or “broker” in the network. This will be used to determine the betweenness centrality of a node u. The algorithm is presented in Equation 5, below.

$$\text{Betweenness}(u) = \sum_{j=1}^{N} \sum_{k=1}^{j-1} \frac{g_{jk}(u)}{g_{jk}}$$  \hspace{1cm} \text{(Equation 5)}

To calculate the ego betweenness centrality, the ego-network of a node u is converted into an adjacency matrix, where 1 indicates a connection between two nodes, to perform matrix operations on the nodes in the network. Equation 5 indicates that the matrix network is first
squared; this is then multiplied by the substitution of the network matrix from a 1 matrix. The resulting matrix is then converted into a vector which contains the non-zero entries in the matrix. The sum of the reciprocals of all these values is then returned as the betweenness value for a node u.

The three centrality measures have now been modelled in the form of equations. Table 7.1 provides a summary of the centrality measures, containing the name, reference, and calculations.

Table 7.1 Centrality measures calculation summary

<table>
<thead>
<tr>
<th>Centrality Measure</th>
<th>Calculation</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Indegree</strong> of node u</td>
<td>indegree(u)</td>
<td>Equation 2</td>
</tr>
<tr>
<td><strong>Outdegree</strong> of node u</td>
<td>outdegree(u)</td>
<td>Equation 2</td>
</tr>
<tr>
<td><strong>Degree</strong> of node u</td>
<td>degree(u)</td>
<td>Equation 3</td>
</tr>
<tr>
<td><strong>Density</strong> of node u's social graph</td>
<td>density(G(u))</td>
<td>Equation 4</td>
</tr>
<tr>
<td><strong>Betweenness</strong> of node u</td>
<td>betweenness(u)</td>
<td>Equation 5</td>
</tr>
</tbody>
</table>

The next section uses these centrality measures to define operations and algorithms used by the Trust\textsubscript{cv} model to satisfy the collectivist cultural trust properties.

**7.5 Trust\textsubscript{cv} model operations and algorithms**

This section describes the Trust\textsubscript{cv} model operations and associated algorithms and its use in the collectivist digital business ecosystem. The discussion in this section conforms to following structure:

1. Use case for Trust\textsubscript{cv}
2. Recommendations for Trust\textsubscript{cv}
   a) A SMME from my group
b) Recommendations from my group leader

c) Recommendations from my group

d) Recommendations from other influential SMMEs

3. Reward and punishment for Trustcv

   a) Punish group members

   b) Reward group members

   c) Impact on trust

4. The final Trustcv algorithm

5. Trustcv support for collectivist cultural trust properties

7.5.1 Use case for Trustcv

This section presents a use case that is used throughout the remaining sections to practically describe the implementation of the Trustcv model. The use case considers a VSE in a collectivist digital business ecosystem known as SpazaShop A. SpazaShop A’s ego-network is depicted in Figure 7.3.

![SpazaShop A's ego network](image)

**Figure 7.3 SpazaShop A’s ego network**

Suppose SpazaShop A wants to transact with another SMME in the collectivist digital business ecosystem. SpazaShop A needs another spaza shop to participate in a bulk buying cooperative, represented as serviceType, so that a discount can be received at a supplier. The
steps SpazaShop A follows to achieve this transaction are similar, on a high level, to those followed by peers using the PeerTrust model. These steps are:

1. Specify the service required – SpazaShop A specifies bulk buying as the serviceType required.
2. Identify SMMEs that offer the service required – SpazaShop A seeks recommendations from other SMMEs in order to identify a transaction partner.
3. Select an SMME to transact with – Based on the recommendations received, SpazaShop A selects an SMME to transact with.
4. Establish a transaction and transact – SpazaShop A proceeds to transact with the selected SMME.
5. Provide feedback based on the transaction – The selected SMME and SpazaShop A provide feedback based on the performance of the other transaction partner.
6. Update the network – The feedback provided is stored and the network is updated with the new information.

These steps lead to successful transactions for the collectivist digital business ecosystem. These steps have been discussed previously in chapter 3, with regards to the PeerTrust model. However the main contribution of Trustcv alters step 2 and step 6. Trustcv provides recommendations to SMMEs by taking into account the collectivist cultural trust properties which is not accomplished by PeerTrust. Additionally, Trustcv rewards and punishes nodes, which updates the network to satisfy a collectivist cultural trust property which is also not accomplished by PeerTrust.

The next section discusses how recommendations are sought after in the Trustcv model. Then the reward and punish approach of Trustcv is discussed. The Trustcv algorithm is proposed and finally a summary is provided that indicates how Trustcv supports the collectivist cultural trust properties.

### 7.5.2 Recommendations for Trustcv

For collectivist SMMEs in the collectivist digital business ecosystem, recommendations are provided by Trustcv according to the behaviour of collectivist cultures. To achieve this, the collectivist cultural trust properties are addressed. Consider SpazaShop A from the previous discussion. SpazaShop A has selected the serviceType it requires, i.e. bulk buying and the following sources are queried for a potential transaction partner or recommendations:
a) A SMME from my group
b) Recommendations from my group leader
c) Recommendations from my in-group members
d) Recommendations from other influential SMMEs

These sources are now discussed individually and for the purposes of algorithms, thresholds, and computations in this section, SpazaShop A is also referred to as \( u \).

a) A SMME from my group

SpazaShop A analyses the neighbours in its own ego-network social graph to see if there are SMMEs that offer the specified serviceType. If there are, the trust level of each potential SMME is computed using Equation 1. The result of this calculation is stored in a variable known as:

\[
\text{recommendationValue} \in [0,1]
\]

When a recommendation is not made, as in this case, the recommendation value is set to the trust levels of the SMMEs identified. These SMMEs are added to the list of potential transaction partners, represented as:

\[
\text{potentialPartnersList}
\]

In this case, SpazaShop B, D, and E all offer serviceType and are therefore added to the list of potentialPartnersList.

Selecting a SMME from its group is not uncommon and is used by the PeerTrust model. Peers in the PeerTrust model, favour peers they have a direct connection to. In the Trustcv model, SMMEs from SpazaShop A's group are also considered but there are also other options available, particularly if no other group member offers the service required. These options are discussed next.

b) Recommendations from my group leader

SpazaShop A can request recommendations from its group leader. The purpose of having group leaders, from the perspective of collectivist cultures, is to provide a good starting point to find recommendations. This is because a group leader is connected and trusted by in-group members due to their social standing. To achieve this, SpazaShop A first needs to identify the leader of its group.
Group leaders are considered as nodes in SpazaShop A’s ego-network that are highly connected. Highly connected nodes can be determined by the degree centrality and the density centrality of a node. SpazaShop A will compute the degree centrality and density centrality of each of its group members, using Equation 3 and 4 respectively. Comparing these results, SpazaShop A can use a threshold to determine its group leader. This threshold can be a custom threshold defined by a node’s settings or a predefined threshold assigned to all nodes. The group leader threshold for a node $u$ is represented as follows:

$$\text{groupLeaderThreshold}(u)$$

The algorithm to identify the group leader in a node $u$’s ego-network is defined in Algorithm 1.

```
identifyGroupLeader(Node u, EgoNetwork A)
{
    degreeList ← empty list
    densityList ← empty list

    foreach Node n in A do
    {
        degree ← (indegree(n) + outdegree(n))/2
        degreeList.add(degree)
        density ← density(getEgoNetwork(n))
        densityList.add(density)
    }

    bestNode ← highestValue(degreeList, densityList)

    if (bestNode > groupLeaderThreshold)
        return bestNode
    else
        return no group leader
}
```

**Algorithm 1: Identify group leader**

Algorithm 1 determines which nodes are group leaders by iterating through its neighbours and storing the density and degree centrality measure of each neighbour. It then determines which neighbour has the highest value, where highest value compares the degree and density centrality according to the function, highestValue. This is specified in the Trustcv implementation but is defaulted to take the average of the node’s degree and density centralities and compare them to other nodes. The node with the highest value is considered the best candidate for group leader. If this node’s value, in terms of degree and density, is greater than the groupLeaderThreshold then this node is considered as a group leader of node $u$’s ego-network.
If a recommendation is received from a group leader it is given a higher recommendationValue. The recommendationValue received from a group leader, is increased by node $u$, who receives the recommendation. The increase value is defined as:

$$\text{groupLeaderRecommendationValue}(u)$$

The recommendations received from a group leader, along with the associated recommendationValue for each node is added to potentialPartnersList. In the case of SpazaShop A, Supplier B is identified as the group leader. Supplier B recommends 2 other SMMEs, SpazaShop D, and another SMME unknown to SpazaShop A, known as SMME1. These recommendations are then added to potentialPartnersList.

The Trustcv model satisfies the two collectivist cultural trust properties through the identification of group leaders and receiving of recommendations from group leaders. The collectivist cultural trust property - Influential nodes such as group leaders are trusted more – is satisfied by the identification of a group leader and the assigning of more weight to a recommendation received from a group leader. Consequently, the collectivist trust property - Members of a group that maintain group harmony are trusted more – is satisfied in a similar manner. Group leaders are considered as members of the group that keep group harmony and are therefore trusted more by assigning more weight to their recommendation.

SpazaShop A has other options which are used to seek recommendations about potential transaction partners, such as querying its own group for recommendations.

c) Recommendations from my in-group

SpazaShop A can ask the neighbours in its own ego-network social graph to provide recommendations for other SMMEs that offer the specified serviceType. However, in the collectivist digital business ecosystem, if a SMME in a dense group wants to transact with another SMME that is not a member of the group, a recommendation from an in-group member is required.

There are two situations which can occur in the collectivist digital business ecosystem scenario:

i. A group member has already identified a potential transaction partner outside the group and they get an in-group member(s) to provide a recommendation for the potential transaction partner, if possible.
ii. An in-group member requires a transaction partner that offers serviceType and another in-group member(s) recommend a candidate from within the group, for the transaction.

These two situations ensure that the group plays a role in other in-group member’s transactions, since the group’s harmony is at stake. To identify a recommendation, a node \( v \) would query its own ego-network \( A \) to determine if the potential transaction partner (\( w \) or serviceType) is an alter in the ego-network. If it is, then an in-group recommendation can be provided, where the recommendationValue is the level of trust it has in this potential transaction partner. This process is defined in Algorithm 2.

\[
\text{provideRecommendation} \ (\text{EgoNetwork} \ A, \ \text{int} \ \text{serviceType}, \ \text{Node} \ w) \\
\{ \\
\quad \text{If (serviceType} = -1 \ \text{AND w } != \text{null)} \\
\quad \{ \\
\quad\quad \text{foreach Node} \ n \ \text{in} \ A \ \text{do} \\
\quad\quad\quad \{ \\
\quad\quad\quad\quad \text{If (n} = v) \\
\quad\quad\quad\quad \quad \text{then return getTrustLevel(n)} \\
\quad\quad\quad\} \\
\quad\quad \text{return null} \\
\quad\} \\
\text{else} \\
\quad \{ \\
\quad\quad \text{foreach Node} \ n \ \text{in} \ A \ \text{do} \\
\quad\quad\quad \{ \\
\quad\quad\quad\quad \text{If (n.serviceType} = \text{serviceType) } \\
\quad\quad\quad\quad \quad \text{then return getTrustLevel(n)} \\
\quad\quad\quad\} \\
\quad\quad \text{return null} \\
\quad\} \\
\}
\]

**Algorithm 2: Providing a recommendation**

Once algorithm 2 is executed and a recommendation is provided, the recommendation of a node’s trust level (TI) from another in-group member \( v \) about a node \( w \), in \( v \)’s ego-network is modelled as:

\[ T_{\text{group_rec}} (v, w) \] where \( T_{\text{group_rec}} \in [0,1] \)

Consider the use case. SpazaShop A asks its group members for recommendations. SpazaShop F and SpazaShop G both recommend an unknown SMME, known as SMME2, and SMME1. Supplier B once again recommends SMME1. The potentialPartnersList is updated and SMME2 is added to this list. Since out-group members are recommended by in-
group members and are considered for transactions, the collectivist cultural property - Out-
group members can be trusted if they are recommended by in-group members – is supported.

The neighbours that provide the recommendation are also stored, so they can be rewarded or
punish if their recommendation is good or bad, respectively. Therefore Supplier B, SpazaShop
F, and SpazaShop G are all added to recommendations list. This approach supports the
collectivist cultural property - Members of a group that maintain group harmony are trusted –
but this is discussed further in a later section.

d) Recommendations from other influential SMMEs

To support the collectivist digital business ecosystem, SpazaShop A can request
recommendations from another SMME with a high betweenness value. A node with a high
betweenness has previously been shown as influential and highly trusted in the network.
Additionally, a node with a high betweenness is not required to be an in-group member. Such
a scenario can provide reliable recommendations that are otherwise not possible if
recommendations are limited to only in-group members.

A node is considered to have a high betweenness value if the betweenness centrality of a
node is above a specified threshold. This threshold is not explicitly specified since it is
dependent on the specific network and average betweenness in the particular collectivist
digital business ecosystem. This is handled by the Social Graph component in the system
architecture. The following value is used to represent the threshold for determining if a node
u has a high betweenness value:

\[
\text{betweennessInfluentialThreshold}(u)
\]

To identify a node with a high betweenness, a SMME may have to search outside of its own
group. Therefore, recommendations from nodes with a high betweenness are limited to
specific situations. For example, if SpazaShop A could not obtain recommendations from its
in-group members or group leader, it could proceed to identify nodes elsewhere in the network
with a high betweenness value. Additionally, SpazaShop A may want to extend its business
opportunities, it can then indicate via a setting, that a recommendation from a node with a high
betweenness should be obtained.

To model the process of obtaining recommendations from nodes with a high betweenness
value, Algorithm 3 is defined. This algorithm queries all the nodes in a node u’s ego-network.
These nodes are requested to identify any nodes in their own ego-network that have a high betweenness value. If such a node is identified, they are asked for a recommendation.

```
getBetweennessRecommendation(EgoNetwork A, int serviceType, Node w) {
    foreach Node v in A do
    {
        If (betweenness(v) > betweennessInfluen
tialThreshold(v))
        then return provideRecommendation(n.getEgoNetwork, serviceType, w)
    }
    return null
}
```

Algorithm 3: Recommendations from a node with a high betweenness

Algorithm 3 can be executed many times depending on how far a node wants to search for a node with a high betweenness value. Once algorithm 3 is executed and a recommendation is provided, the recommendation value from a node with a high betweenness value \( v \) about a node \( w \) is modelled as:

\[
T_{betweenness, rec}(v, w) \text{ where } T_{betweenness, rec} \in [0,1]
\]

Similarly to obtaining recommendations from group leaders, the recommendationValue of a recommendation received from a high betweenness node can be weighted more. This increase is represented as:

\[
\text{additionalInfluentialTrust}(u)
\]

The identification of nodes with high betweenness and the additional weight of recommendations received from such nodes support the collectivist cultural trust property - Influential nodes such as group leaders are trusted more. The collectivist cultural trust property - Members of a group trust in-group members more than out-group members – is also supported since recommendations from high betweenness nodes are obtain only when no recommendations from in-group members or group leaders are obtain or when specifically set by the SMME.

In the use case provided, SpazaShop A’s group is a strong cohesive group and recommendations have already been obtained from a group leader. Therefore, SpazaShop A does not request recommendations for nodes with a high betweenness.
The potentialPartnersList of SpazaShop A now contains potential transaction partners as well as recommendation values obtained according the behaviour of collectivist cultures. The potential partners list now consists of the following SMMEs:

potentialPartnersList = {SpazaShop B, D, E, SMME1, SMME2}

According to step 3, SpazaShop A will select a transaction partner from potentialPartnersList with the highest recommendationValue. The transaction will be established and feedback will be provided according to step 4 and 5. Step 6 requires that the network is updated. As mentioned previously, this step contains collectivist cultural specific behaviour and is therefore discussed in the next section.

7.5.3 Reward and punish for Trust\textsubscript{cv}

The final step of a transaction updates the information in the network based on the feedback received from the SMMEs participating in the transaction. In the PeerTrust model, this step updates the trust relation values that exist between the peers and the creation of a connection between the peers if one does not exist. The Trust\textsubscript{cv} model also achieves this. However, the Trust\textsubscript{cv} model performs an additional function to satisfy collectivist cultural trust properties. This is the function of rewarding and punishing SMMEs according to the recommendations they provide. This section discusses the process of rewarding and punishing SMMEs and how this affects trust in the collectivist digital business ecosystem.

SMMEs that provide recommendations for other in-group members about out-group nodes have to take responsibility for their recommendations, in the collectivist digital business ecosystem. This behaviour is in accordance with the behaviour of collectivist cultures. Group harmony is the main concern of collectivist cultures and in-group members should behave in a manner to maintain or enhances the group reputation or otherwise risk eventual expulsion from the group.

Consider the use case. When SpazaShop A requested recommendation from its group members, Supplier B, SpazaShop F and SpazaShop G provide recommendations. When an in-group member provides a recommendation, the recommending node along with the recommendationValue is added to a responsible list for a particular transaction. Once the SMMEs have provided their service, SpazaShop A provides transaction feedback for the other SMME involved in the transaction. If the other SMME was recommended by in-group
members, an analysis is done. SpazaShop A compares the transaction feedback it provides against the recommendation values received from in-group members.

The comparison identifies if any in-group member provided a recommendationValue that was significantly higher, significantly lower, or approximately the same as the transaction feedback given. If such in-group members exist, they are punished or rewarded for providing largely inaccurate or accurate recommendations that could have jeopardised or enhanced the group’s harmony, respectively. Table 7.2 provides an indication of the recommendationValue provided by in-group members and the difference between these values and the feedback provided by SpazaShop A, which is 0.76 for this scenario transaction.

**Table 7.2 Difference between recommended values and transaction feedback**

<table>
<thead>
<tr>
<th>Group Member</th>
<th>recommendationValue</th>
<th>Difference between actual feedback (0.76) and recommendation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier B</td>
<td>0.73</td>
<td>0.03</td>
</tr>
<tr>
<td>SpazaShop F</td>
<td>0.92</td>
<td>0.16</td>
</tr>
<tr>
<td>SpazaShop G</td>
<td>0.70</td>
<td>0.06</td>
</tr>
</tbody>
</table>

The in-group members are punished and rewarded as follows:

**a) Punish group members**

To determine if a transaction feedback \( T_1 \) is significantly higher or lower than a recommendationValue, a threshold for a node \( u \) is defined as:

\[
\text{responsibilityThreshold}(u)
\]

If the absolute value of the difference between the transaction feedback and the recommendation value is greater than the \( \text{responsibilityThreshold}(u) \) then the SMME(s) that provide the inaccurate recommendation is/are punished.

The SMME(s) is/are punished accordingly by decreasing their community context factor (CF) by the value \( \text{punishmentValue} \). This value can be defined by each node or can be a set value for a network depending on the collective digital business ecosystem configuration. Therefore, the community context factor for a node \( u \) is updated as follows:
\[ CF(u) = \frac{(CF(u) - \text{punishmentValue})}{2} \]  
(Equation 6)

b) Reward group members

Similarly to the punishment of a SMME, if the absolute value of the difference between the transaction feedback and the recommendation value is between 0 and the \( \text{responsibilityThreshold}(u) \) then the recommending SMME(s) is/are rewarded.

The SMME(s) is/are rewarded accordingly by increasing their community context factor (CF) by the value \( \text{rewardValue} \). This value can be defined by each node or can be a set value for a network depending on the digital business ecosystem configuration. Therefore, the community context factor for a node \( u \) is updated as follows:

\[ CF(u) = \frac{(CF(u) + \text{rewardValue})}{2} \]  
(Equation 7)

c) Impact on trust

In the use case provided, the community context factor (CF) of the in-group members, who provided recommendations to SpazaShop A, would be decreased or increases based on Equation 6 and Equation 7, respectively. For example, suppose \( \text{responsibilityThreshold}(\text{SpazaShop A}) \) is set to 0.1. SpazaShop F would then be punished since it provided a largely inaccurate recommendation value of 0.92. This occurs since the feedback provided by SpazaShop A, based on the behaviour of the recommended node, is 0.76 and hence a difference of 0.16. Conversely, Supplier B and SpazaShop G are rewarded for providing accurate recommendations.

The community context factor (CF) is a parameter in the trust computation presented in Equation 1. The changes made to it through punishing or rewarding of a node, therefore has members of a group that maintain group harmony are more trusted and out-group members can be trusted if they are recommended by in-group members.

In the next section, the final Trust\(_{cv}\) algorithm is provided, which has a direct impact on a node’s trust level (TI). To maintain or enhance their trust level, group members are required to provide accurate recommendations, which at the same time benefits the group’s harmony. Therefore, punishing and rewarding nodes that provide inaccurate and accurate recommendations, respectively, supports the collectivist cultural trust properties: algorithm is presented, based on the previous discussions.
7.5.4 The final Trust\textsubscript{cv} algorithm

Algorithm 4 presents the algorithm for Trust\textsubscript{cv}. A node \( w \) that wants to transact with another node that can perform \texttt{serviceType} in the collectivist digital business ecosystem would execute the Trust\textsubscript{cv} algorithm.

\begin{verbatim}
Trust\textsubscript{cv} (Node w, EgoNetwork A, int serviceType)
{
    Initialise potentialPartnersList

    potentialPartnersList.add(findInEgoNetwork(A, serviceType))
    potentialPartnersList.add(findViaGroupLeader(A, serviceType))
    potentialPartnersList.add(findViaGroupMembers(A, serviceType))

    if potentialPartnersList.size < 1 OR searchBetweenness
        then potentialPartnersList.add(findViaBetweennessNode(A, serviceType))

    sortByRecommendationValue(potentialPartnersList)

    idealPartner ← potentialPartnersList.first()

    if idealPartner = null
        then throw Exception(TransactionPartnerNotFound)

    transactionResults ← transact(w, idealPartner)
    updateData(transactionResults)
    rewardPunishGroupMembers(transactionResults)
}
\end{verbatim}

Algorithm 4: Trust\textsubscript{cv} for transactions

Algorithm 4 begins with the initialisation of an empty list to store potential transaction partners for this transaction. Firstly, the node stores any group members in its own ego-network, that offer \texttt{serviceType}, as potential transaction partners. Secondly, the node asks its group leader and its own group members for recommendations. The \texttt{potentialPartnersList} is extended with these recommendations. If there are not potential transaction partners at this stage or the \texttt{searchBetweenness} setting is set, transaction partners are identified via influential nodes in the network that have a high betweenness centrality. Such nodes have connections further in the network and may increase the possibility of identifying a node that can perform \texttt{serviceType}.

The \texttt{potentialPartnersList} is then sorted by the recommendation value provided by the recommending nodes. This results in the most highly recommended node being in the first position of the list. If the list is empty an exception is thrown to indicate that no transaction partner could be identified to perform \texttt{serviceType}. Otherwise, node \( w \) and the \texttt{idealPartner} node transact with each other. The results of the transaction are, such as transaction...
feedback, in the transactionResults variable. These results are used to update the data in the network and to determine if any group members are rewarded or punished based on their recommendations.

All these steps in the algorithm have been discussed in detail and together they result in the Trustcv algorithm that supports collectivist cultural trust properties in the collectivist digital business ecosystem. The next section summarises Trustcv support for collectivist cultural trust properties.

7.5.5 Trustcv support for collectivist cultural trust properties

In this section, a summary is provided in the form of a table, Table 7.3, to provide an indication of how the collectivist cultural properties are supported by the Trustcv model. Although the Trustcv model, in its entirety, works together to provide support for collectivist cultural behaviour, Table 7.3 provides a mapping to Trustcv model operations and algorithms that support the collectivist culture trust properties directly.

### Table 7.3 Trustcv satisfaction of collectivist cultural properties

<table>
<thead>
<tr>
<th>Collectivist cultural trust properties</th>
<th>Trustcv model operations</th>
<th>Trustcv algorithms and equations</th>
</tr>
</thead>
</table>
| Members of a group that maintain group harmony are more trusted | • The identification of group leaders  
• Obtain recommendations from group leaders  
• Obtain recommendations from in-group members  
• Reward and punish in-group members that provided inaccurate recommendations | • Algorithm 1  
• Algorithm 2  
• Equation 6  
• Equation 7 |
| Members of a group trust in-group members more than out-group members | • Identifications of high betweenness nodes  
• Recommendations from high betweenness nodes | • Algorithm 3 |
| Influential nodes such as group leaders are more trusted | • The identification of group leaders  
• Obtain recommendations from group leaders  
• Identifications of high betweenness nodes | • Algorithm 1  
• Algorithm 3 |
This table indicates that the collectivist cultural trust properties are supported by the Trust_{cv} model through recommendations and the adjustment of trust computation parameters based on the behaviour of SMMEs in the collectivist digital business ecosystem.

### 7.6 Conclusion

The purpose of this chapter is to formally define the Trust_{cv} model and ensure that the trust model supports collectivist cultural behaviour and the properties identified in chapter 4. To achieve this, a basic trust model is presented. The basic trust model describes the PeerTrust model in the context of Trust_{cv}, and forms the foundation of the Trust_{cv} model. Descriptions of trust constituents and operations for the basic trust model are provided; this includes an explanation of the trust environment, trust levels, the trust computation, the factors of the trust computation, and the trust threshold.

The basic trust model is then extended by defining the Trust_{cv} social graph constituents. A model of the ego social network graph and associated centrality measure calculations is provided. These constituents provide the environment and calculations that can be used by Trust_{cv} to support collectivist cultural trust properties.

The Trust_{cv} model operations and algorithms are presented. A use case is defined and the steps executed to establish and perform a transaction are provided. These steps are similar to PeerTrust but have differences when recommendations are requested and the network is updated. These differences are discussed and the key operations and algorithms are provide which distinct Trust_{cv} from PeerTrust.

Recommendations are requested from group leaders, in-group members, and influential SMMEs in the network. Additionally, in-group members are punished or rewarded based on
the recommendations provided. This Trustcv behaviour is combined and presented in the Trustcv algorithm. Finally, a table is provided which summarises how Trustcv supports collectivist cultural trust properties.

The next chapter discusses the implementation of the Trustcv model in a collectivist digital business ecosystem simulation environment, so as to determine its impact on such an environment, compared to PeerTrust.
Chapter 8

Trust$_{cv}$ Simulation and Evaluation

8.1 Introduction

In the previous chapter, the Trust$_{cv}$ model was defined. The purpose of the Trust$_{cv}$ model is to specifically address the trust properties of collectivist cultures and provide support for trust and reputation in the collectivist digital business ecosystem. To achieve this, Trust$_{cv}$ attempts to improve the number of successful transactions, assist in selecting reliable and trustworthy partners for transactions and grow a more cohesive community.

In this chapter, the PeerTrust model and the Trust$_{cv}$ model are compared to each other using multi-agent simulations. The purpose is to determine if the Trust$_{cv}$ model, relative to the PeerTrust model, can support trust and reputation for the collectivist digital business ecosystem by supporting the behaviour of collectivist cultures. A simulation of the PeerTrust model and the Trust$_{cv}$ model can provide a comparison between the behaviour of the two models. An analysis of the simulation results can indicate how supportive these models are at addressing collectivist cultures and the collectivist digital business ecosystem.

The simulation scenarios for evaluating the effectiveness of the Trust$_{cv}$ model are defined in this chapter. The PeerTrust model is simulated with standard settings and parameters to give a baseline for comparison. In order to gain a better understanding of the performance of the Trust$_{cv}$ model, an analysis is done of how PeerTrust behaves when used in collectivist communities. A direct comparison between PeerTrust and Trust$_{cv}$ gives insight into individualistic versus collectivist behaviours, but is not a comparison between collectivists forced to use tools designed for individualists versus collectivists using a tool specifically designed for them. To achieve this, the standard PeerTrust model’s simulation settings and parameters are adjusted to attempt to mimic the behaviour of collectivist cultures. Finally, the Trust$_{cv}$ model is simulated and all three simulation results are compared.

The section that follows discusses the simulation environment. Next, the simulation scenarios are discussed and introduced. Each scenario is then simulated and evaluated and finally the chapter is concluded.
8.2 Simulation Environment

For the purpose of this research, the PeerTrust model and the Trust\textsubscript{cv} model are both simulated using NetLogo (Wilensky, 2010). This section discusses NetLogo as a simulation environment. This is followed by a discussion on the use of NetLogo for the Trust\textsubscript{cv} and PeerTrust models and the description of the common simulation components.

8.2.1 NetLogo environment

NetLogo is a multi-agent programmable modelling environment built on Java and Scalar programming languages and is used by researchers worldwide (Sklar, 2007, Damaceanu, 2008, Sakellariou et al., 2008). This environment makes use of agents, known as turtles that can be programmed to behave in a particular way. NetLogo simplifies the process of agent interaction, movement, and connection to other agents through public APIs (Application Programming Interfaces) (Wilensky, 2010).

NetLogo has a customisable user interface to allow users to define input and view output for a simulation. Properties and settings can be defined which can directly impact a simulation during runtime. Simulation outputs are also impacted during runtime, which constantly provides dynamic and real-time results. A NetLogo simulation can also be visualised using the display provided by the environment, therefore creating a snapshot of the simulation at any time.

The NetLogo environment has features which can be used to simulate the Trust\textsubscript{cv} and PeerTrust models. The next section discusses how NetLogo is used for the simulation of these models.

8.2.2 NetLogo for the Trust\textsubscript{cv} and PeerTrust models

NetLogo is used to simulate a multi-agent environment where agents interact with each other through transactions and form connections with each other based on transactions. For PeerTrust, the multi-agent environment is simulated as a P2P environment where agents are peers. For Trust\textsubscript{cv}, the multi-agent environment is the collectivist digital business ecosystem, and the agents are SMMEs.

The Trust\textsubscript{cv} and PeerTrust models are both simulated in a decentralised P2P environment, using NetLogo. Additionally, they share common simulation components such as parameter
settings, visualisations, and outputs, which can be inspected during the scenario discussions that follow. These components provide an indication of how NetLogo provides support for the implementation of the Trustcv and PeerTrust models.

NetLogo is an appropriate simulation environment for the PeerTrust and Trustcv models. It has been used by other researchers to implement SMME environments (Azhar and Qureshi, 2013) and many other decentralised environments (Gonopolskiy and Nash, 2007, Sueur et al., 2012), where agents interact with each other. NetLogo’s customisation also makes it useful for this research as behaviour can be implemented based on the model requirements.

This section provides an introduction to NetLogo and the simulation environment for the PeerTrust and Trustcv models. In the sections that follow, scenarios to evaluate the effectiveness of these models are defined and the simulations and their results are discussed.

8.3 NetLogo Simulations

This section introduces three simulation scenarios for the evaluation, defines the common settings among these scenarios, and defines the evaluation metrics for the simulation of these scenarios.

8.3.1 Simulation scenarios for evaluation

The simulation scenarios attempt to define a practical implementation of the PeerTrust and Trustcv models, which can then be simulated and evaluated. Each scenario is fundamentally a P2P environment scenario where peers transact with other peers in the network. The three scenarios to be evaluated in this chapter are:

a) Standard PeerTrust scenario
b) Collectivist culture PeerTrust scenario
c) Trustcv scenario

These scenarios are now introduced.

a) Standard PeerTrust scenario
The standard PeerTrust scenario defines a standard P2P environment as defined by Xiong and Liu (2004). This P2P environment consists of peers, both malicious and non-malicious, that identify potential transaction partners, select a transaction partner, transact with them, and then provide feedback based on the transaction.
The purpose of this scenario is to determine how PeerTrust supports the traditional environment for which it was specifically designed. The simulation results provide a base line against which the other two scenarios and associated models can be compared.

b) Collectivist culture PeerTrust scenario

The collectivist culture PeerTrust scenario adjusts the standard PeerTrust scenario to create a scenario based on collectivist culture behaviour, discussed in previous chapters. This can give an indication of how collectivist cultures behave if they are supported by a model that is defined for individualist cultures. As the standard PeerTrust model does not support in-group decisions and the perseverance of group harmony, it is expected that the number of successful transactions in this scenario will be less. Therefore, in order to truly compare standard PeerTrust and Trustcv for collectivist cultures, this scenario is necessary. In this scenario, peers are more concerned about how the community and their direct connections behave. Also, peers place more emphasis on the trust level of nodes.

For this scenario, PeerTrust simulation settings are adjusted in an attempt to simulate the behaviour of collectivist cultures. The results of this model can then directly be compared to those achieved by the Trustcv scenario, to provide a real indication of the improvements achieved by the Trustcv model, designed specifically for collectivist cultural behaviour.

c) Trustcv scenario

The purpose of this scenario is to evaluate the effectiveness of the Trustcv model for the collectivist digital business ecosystem, through its support of collectivist cultures. This is the main purpose of the research conducted in this study and through a comparison against the previously introduced PeerTrust scenarios, conclusions are made. Therefore, the previously discussed scenarios are all a base line against which the Trustcv model can be compared to determine if is supportive of collectivist cultures and relevant to the collectivist digital business ecosystem.

Although these scenarios differ, there are a number of important settings that are constant among all scenarios so as to provide an accurate evaluation. These are discussed in the next section.

8.3.2 Common scenario settings

The three scenarios introduced previously have a number of common settings due to their support for trust and P2P architectures. PeerTrust and Trustcv simulation implementations are
both implemented using NetLogo. Additionally, the Trustcv simulation implementation is an extension of PeerTrust simulation implementation and therefore, they share similar settings.

To ensure an accurate simulation and evaluation, the settings presented in Table 8.1 are predefined for all scenarios. These settings are determined by the researcher, based on previous experiments and are the values which best portray the simulation of their associated model. Table 8.1 provides the setting, its value, and a brief description of the setting and why it is selected. Table 8.1 uses the term “agent” to refer to a peer or SMME.

**Table 8.1 Common scenario simulation settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Transactions</td>
<td>2000</td>
<td>Enough transactions to determine any change in the network over time.</td>
</tr>
<tr>
<td>No. of Agents</td>
<td>100</td>
<td>Computationally reasonable for the purpose of the proposed scenario simulations.</td>
</tr>
<tr>
<td>No. of Malicious Agents</td>
<td>20%</td>
<td>The percentage of malicious agents in the network.</td>
</tr>
<tr>
<td>No. of Services Available</td>
<td>7</td>
<td>Good representation for this environment for 100 agents.</td>
</tr>
<tr>
<td>Malicious Transactions of malicious agents</td>
<td>100%</td>
<td>A malicious agent should always act malicious.</td>
</tr>
<tr>
<td>Recent Time Window</td>
<td>500 transactions</td>
<td>The time frame in which a transaction is considered recent.</td>
</tr>
<tr>
<td>Adaptive Time Window</td>
<td>100 transactions</td>
<td>The time frame in which an agent’s recent behaviour (adaptive time window) is compared to a previous behaviour.</td>
</tr>
<tr>
<td>Time Threshold</td>
<td>0.2</td>
<td>The difference in agent’s behaviour allowed between the adaptive and recent time window.</td>
</tr>
</tbody>
</table>
Initial Trust Level | 0.5 | Each agent will have this trust level when the simulation starts.
Transaction Context Factor | On | This is set for all models to conform to the PeerTrust trust computation
Community Context Factor | On | This is set for all models to conform to the PeerTrust trust computation

The settings presented in Table 8.1 are set in the NetLogo simulation. Simulations of each scenario will be run against these settings and additional settings specified for each scenario. Similarly to Xiong and Liu (2004), all simulations are averaged over 5 runs, for each scenario. An evaluation of each scenario is conducted based on the simulation results. The metrics upon which each scenario is evaluated are discussed next.

### 8.3.3 Scenario evaluation metrics

To accurately compare each scenario and the results obtained from their simulation, evaluation metrics need to been defined. The NetLogo implementation of PeerTrust and Trust\textsubscript{cv} simulations provide a number of useful outputs which are considered as the evaluation metrics. The evaluation metrics are as follows:

- **a) Average trust level over time**
- **b) Percentage of successful transactions over time**
- **c) Number of malicious peers selected per number of transactions**

These metrics are now discussed.

**a) Average trust level over time**

The average trust level over time metric gives an indication of the change in trust levels within the environment, over time. Trust levels may drastically increase or decrease depending on the behaviour of peers in the network. However, the ideal situation arises when the trust levels remain relatively stable and constant in the environment. Additionally, a high average trust level could imply that malicious peers also have a high trust level, which is not desired. Therefore, an average trust level should remain stable and not be too high or too low. This implies that there is a balance among peers in the network. Few peers obtain significantly high
or significantly low levels of trust. The average trust level over time is calculated as the sum of all the peers trust level over the number of peers in the network, and plotted against time.

b) Percentage of successful transactions over time
The percentage of successful transactions over time metric gives an indication of how successfully peers are performing transactions in the environment. The definition of a successful transaction is derived from Xiong and Liu (2004) whereby a successful transaction occurs if no peer, involved in the transaction, behaves maliciously. Additionally, the author appends this definition with peers that have a satisfaction rating greater than or equal to 0.5 in the network, in order for a transaction to be considered successful. This creates a strict environment where peers, that are not malicious, still have to provide a satisfactory service. Although a malicious peer has the ability to provide a good satisfaction rating for a bad service the transaction is still considered as unsuccessful, due to the simulation’s knowledge of the malicious behaviour.

The ideal percentage of successful transactions would be 100%, however, such results would not be realistic if the environment contained malicious peers. Malicious peers are guaranteed to behave maliciously, which would flag the transaction as unsuccessful. Additionally, in a realistic environment, non-malicious peers may perform unsatisfactory services which also flag the transaction as unsuccessful. Such constraints provide a more accurate representation of the real world behaviour where both satisfactory and unsatisfactory service execution occurs. Therefore, the percentage of successful transactions in the environment should vary depending on the amount of malicious peers and their percentage of malicious behaviour. Since the PeerTrust and Trustcv models are compared relative to each other, the percentage of successful transactions can be compared with each other rather than identifying an ideal percentage.

c) Number of malicious peers selected per number of transaction
The number of malicious peers selected per number of transaction metric gives an indication of the extent to which the trust model recommends malicious peers for transactions. Ideally, a trust model should never recommend malicious peers, to other peers, for a transaction. A trust model has the purpose of providing information and recommendations that can assist peers to determine trustworthy and reliable partners to transact with. However, realistically the trust models are likely to recommend malicious peers. Therefore, comparing the extent to which a trust model recommends malicious peers provides insight into how the trust model performs according to its main purpose.
The comparison of the PeerTrust and Trust\textsubscript{cv} model with regards to the metrics provided in this section can give insight into the performance of the trust model in the specified environment. The sections that follow discuss each of the simulations and evaluations of the three scenarios defined in this section.

8.4 Standard PeerTrust scenario simulation and evaluation

The first scenario simulates a P2P environment where peers transact with other peers. In such an environment, peers need to transact with peers they can trust in order to ensure a successful transaction. This is the standard scenario for the PeerTrust model which is specifically designed for such an environment.

In this section, the P2P environment of the simulation is defined. Simulations are executed according to this scenario. Finally, the simulation results for this scenario are evaluated and discussed.

8.4.1 Peer-to-Peer simulation environment

To simulate the P2P environment for the PeerTrust model, the NetLogo implementation of PeerTrust is used. This implementation simulates a P2P environment where peers transact with each other and establish connections. Additionally, trust and reputation is facilitated in this implementation, and allows peers obtain reputation information about other peers and determine the trust level of potential transaction partners. Figure 8.1 is a screenshot of the PeerTrust implementation in NetLogo.
There are many settings and properties which can be set in the PeerTrust simulation environment, as depicted in Figure 8.1. These settings and properties are introduced in the sub-sections that follow. A description of additional settings, not relevant to this discussion, is provided in Appendix A.

A P2P environment, required for this scenario, consists of the following components:

a) Peers
b) Connections
c) Transactions
d) Trust computation

These components are now discussed in terms of the simulation environment.

a) Peers

Peers are modelled as agents in NetLogo and have the capacity to store information about itself and other nodes. Each peer maintains the following information about itself:

- serviceType – The service that this peer offers
- malicious – This indicates if a peer is malicious or not
- my_trust_value – The trust level of this peer calculated according to the PeerTrust model trust computation
- previous_transactions – This data object includes a list of peers, the satisfaction ratings received, credibility of peers, and the time of transactions this peer has previously participated in.
- connections – A list of peers to which a peer is directly connected.
• recommendation_value – This is the value another peer assigns to a peer when recommending this peer. This value is not necessarily the same as my_trust_value.

This information enables a peer to behave as a peer in the P2P environment of PeerTrust. Additionally, P2P environments contain peers that may behave maliciously. The malicious_peers and malicious_transactions settings, presented in Table 8.1, are included to simulate the behaviour of malicious peers. Malicious nodes are common in P2P environments and therefore, the simulation of such peers adds realism to the simulation. Additionally, it provides a good indicator as to how effective a trust and reputation model is at dealing with malicious peers.

These settings define the P2P environment in terms of peers and their behaviour. Additionally, peers create connections with other peers when transacting. These connections are discussed next.

b) Connections

For P2P environments to function correctly, connections are required between peers. The benefit of peers having connections is that they are, firstly, able to locate other peers in the network through their connections, and secondly, they can ask their connections for recommendations. In the PeerTrust simulation, peers maintain a list of peers they are connected to. This is easily achieved in NetLogo, as agents have standard APIs to support the establishment, maintenance, and removal of links to other agents.

Connections are established when two peers transact with each other. If a connection already exists between two peers performing a transaction, the connection information is updated to include the recent transaction results. Additionally, in the PeerTrust simulation, peers evaluate their connections whenever they are selected for a transaction. The evaluation of a peer’s connections, gives a peer the opportunity to remove any connections that they no longer consider trustworthy. This ensures that peers are not constantly associated with untrustworthy peers even if they have transacted with them once before.

The implementation of connections in the PeerTrust simulation environment conforms to the PeerTrust model. Peers only have access to other peers which they have transacted with which is enforced through the creating of connections when transactions occur. The next section discusses transactions in the PeerTrust simulation environment.
c) Transactions
The main purpose of the P2P environment is to facilitate transactions among peers. Suppose a peer in the P2P network, would like to transact, there are a number of steps that would occur in the PeerTrust simulation to facilitate the transaction. These steps have been discussed in previous chapters but are briefly revisited here. These steps are as follows:

1. Specify the service required
2. Identify peers in the network that offer the specified service
3. Select a peer to transact with
4. Establish a transaction and transact
5. Provide feedback based on the transaction
6. Update the network

These steps conform to the PeerTrust model and are implemented to achieve the PeerTrust simulation. In step 2, peers have to compute the trust level of another peer. The trust computation is an essential component of the PeerTrust model. The implementation of the PeerTrust trust computation, in terms of the PeerTrust simulation environment is discussed in the next section.

d) Trust computation
The core purpose of the PeerTrust model is to compute the trust level of peers so as to facilitate successful transactions among peers and guard against malicious nodes. Therefore, the PeerTrust trust computation needs to be implemented in the P2P environment to ensure the accurate simulation of the PeerTrust model. The PeerTrust trust computation is presented previously as Equation 1. For the purpose of this discussion, Equation 1 is presented again:

\[ T_l(u) = \alpha \times \sum_{i=1}^{l(u)} S(u, i) \times Cr(p(u, i)) \times TF(u, i) + \beta \times CF(u) \]  

(Equation 1)

This equation has a number of factors and according to Xiong and Liu (2004) these factors can be customised to the needs of the environment in which they are used. Therefore, the PeerTrust simulation environment provides the following settings, depicted in Figure 8.1, which can be adjusted and which have an impact on the trust computation and trust in the environment. These settings include global_initial_trust_value, transaction_context_factor, community_context_factor, recent_time_window, adaptive_time_window, and time_threshold which are already presented in Table 8.1. The additional settings, related to PeerTrust, which can be customised according to each scenario, are as follows:
- **trust_threshold** – This setting provides a threshold to determine if another peer can be considered as trusted by a peer.
- **alpha** – This value indicates the weighting that the PeerTrust trust computation assigns to personal past experience.
- **beta** – This value indicates the weighting that the PeerTrust trust computation assigns to the community context factor.

The next section discusses the setup of the simulation, indicating the values assigned to these settings, for the PeerTrust scenario.

### 8.4.2 Standard PeerTrust simulation

The standard PeerTrust simulation environment is discussed in the previous section. In this section, the focus is on adjusting the simulation environment settings to simulate the standard PeerTrust scenario. The simulation environment settings, and associated values, for the standard PeerTrust scenario are presented in Table 8.2.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>The weighting of personal experience (alpha)</td>
<td>0.8</td>
<td>PeerTrust is very reliant on personal experience</td>
</tr>
<tr>
<td>The weighting of the community context factor (beta)</td>
<td>0.2</td>
<td>PeerTrust does not place much emphasis on the community context factor</td>
</tr>
<tr>
<td>Trust Threshold</td>
<td>0.5</td>
<td>This is the average trust level possible and in this scenario, used as the threshold</td>
</tr>
</tbody>
</table>

The settings defined in Table 8.2 are taken from Xiong and Liu (2004). These values are used as they conform to existing PeerTrust simulations and represent the P2P environment in which PeerTrust has previously been evaluated. A simulation is now executed for this scenario, based on these settings. The results of the simulation are evaluated in the next section.

### 8.4.3 Standard PeerTrust simulation evaluation

In this section the results of the standard PeerTrust scenario simulation are evaluated according to the evaluation criteria. Recall that each simulation is run 5 times and the results
are averaged. The screenshot in Figure 8.2 depicts the visual result of the P2P network for one of the 5 simulations run.

Figure 8.2 has the following components:

- **Red nodes** – Red coloured nodes in the visual display indicate malicious peers in the P2P network.
- **Green nodes** – Green coloured nodes in the visual display indicated non-malicious peers in the P2P network.
- **Trust levels** – Each peer in the visual display has its trust value displayed on its node.

According to Figure 8.2, malicious peers have relatively low trust levels compared to those of non-malicious peers. The PeerTrust model ensures that malicious peers struggle to achieve high trust levels and are therefore less likely to be chosen as transaction partners. Additionally, malicious peers are not connected to many other peers. When peers evaluate their connections, they are capable of disconnecting themselves from malicious peers.
In Figure 8.3, the additional simulation outputs are depicted. This is the associated outputs of the simulation presented in Figure 8.2.

**Figure 8.3 Standard PeerTrust output results**

The components in this display are as follows:

- **Trust value graph** - This graph depicts the average trust level (y-axis) for all the nodes in the P2P network over the time in ticks (x-axis), which is the duration of the simulation.
- **Successful transactions graph** - This graph depicts the number of successful transactions (y-axis) over the number of total transactions (x-axis).
- **Successful Transactions** – This output result displays the number and percentage of successful transactions that have occurred during the simulation.
- **Average Trust** – This output result displays the average trust level of all the peers in the P2P network.
- **Number of Nodes** – This output result displays the total number of nodes currently in the P2P network being simulated.
- **Malicious Nodes** – This output result displays the total number of malicious peers currently in the P2P network being simulated.
- **Good Nodes** – This output result displays the total number of good (non-malicious) peers in the P2P network being simulated.
- **Malicious Nodes Selected** – This value indicates the number of times a malicious peer was selected to transact with.
Total Transactions – This value indicates the total number of transactions that have occurred in the P2P network being simulated.

The output results depicted in Figure 8.3 provide information that is used for the evaluation of the simulation scenario according to the evaluation metrics described previously. The standard PeerTrust scenario results are presented in Table 8.3 and are evaluated according to each metric.

Table 8.3 Standard PeerTrust evaluation metric results

<table>
<thead>
<tr>
<th>Evaluation Metric</th>
<th>Simulation Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average trust level over time</td>
<td>0.514</td>
</tr>
<tr>
<td>Percentage of successful transactions over time</td>
<td>53.72%</td>
</tr>
<tr>
<td>Number of malicious peers selected per number of transactions</td>
<td>396</td>
</tr>
</tbody>
</table>

a) Average trust level over time

The graph for the average trust level over time, in Figure 8.3, indicates that the trust level in the P2P network remains constant with very little change. Averaged over 5 runs, the average trust level is 0.514. This is a respectable value and indicates that few peers in the network have significantly high or significantly low levels of trust, unless they are malicious peers. Malicious peers have low trust levels which is the desired outcome.

b) Percentage of successful transactions over time

The standard PeerTrust scenario simulation achieves a successful transaction rate of 53.72% over 10000 transactions. This is not a very high success rate and indicates that, either many malicious peers are being selected for transactions, or peers are under performing when they render a service. In the case where peers are under performing, a random factor is involved for simulation purposes, therefore, in reality, the success rate may be higher or lower. However, all scenario simulations implement the same level of randomness, making their comparisons relatively accurate. In an environment where successful transactions are required, the PeerTrust model may not lead to the desired percentage of successful transactions.
c) Number of malicious peers selected per number of transactions

In each simulation run, an average of 396 malicious peers are selected for every 2000 transactions. This indicates that for 19.8% of the transactions, a malicious peer is recommended and chosen as a transaction partner. The PeerTrust model, therefore, has the vulnerability of being able to recommend malicious nodes. This percentage does not seem very high but compared to the other scenarios later, it may not be ideal.

The standard PeerTrust scenario is simulated and evaluated in the section. Overall, the PeerTrust model performs reasonably well in the environment for which it is designed. In the next section, the PeerTrust model is simulated in a more collectivist cultural environment, and its performance is evaluated.

8.5 Collectivist culture PeerTrust scenario simulation and evaluation

The collectivist culture PeerTrust scenario adjusts the settings of the standard PeerTrust scenario, based on the behaviour of collectivist cultures. However, modelling the trust behaviour of collectivist cultures is more complex than simply adjusting the settings of the PeerTrust model, as discussed in the previous chapters. For the purpose of this study, the PeerTrust model settings are adjusted to support collectivist cultural behaviour. Performing an evaluation of this simulation provides an indication as to the extent that PeerTrust, as it is, supports collectivist cultural behaviour. This section discusses the collectivist culture PeerTrust P2P environment. This is followed by a discussion on the simulation of this scenario and the results of the simulation are then evaluated.

8.5.1 Peer-to-peer environment according to collectivist cultures

To be able to properly evaluate the Trustcv model, a comparison is required of how collectivist cultures would use the PeerTrust model, with regards to their real behaviour. For this purposes, the collectivist cultural trust properties are recalled and discussed in terms of this scenario.

a) Members of a group that maintain group harmony are trusted more

The concept of groups is not defined in the PeerTrust model and therefore, it is not simple to identify if an in-group member maintains the group harmony. However, PeerTrust has a community context factor which increases when peers provide feedback based on
transactions. This encourages peers to actively participate in the P2P network. In the standard PeerTrust scenario, the weight of the community context factor, beta, is low. For the purpose of this scenario, this weight is increased and will largely influence the trust level of a peer. Therefore, peers that provide feedback and participate in the P2P network are said to maintain the group harmony.

b) Members of a group trust in-group members more than out-group members
Since the PeerTrust model does not directly identify groups it implies that it does not directly support the fact that in collectivist cultures, in-group members have preference over out-group members. However, the PeerTrust model enables peers to maintain connections to peers they have previously collaborated with, creating direct connections. The peers that a peer directly connects to, would have more accurate data relating to previous experience and therefore, by assigning a weighting to previous experience peers are encourage to select peers they have previously collaborated with, for transactions. Therefore, this scenario maintains the weighting, alpha, assigned to previous experience in the trust computation. However, this value is less than in the standard PeerTrust scenario, since community context is given extra weighting based on the previous property.

c) Influential nodes such as group leaders are more trusted
The PeerTrust model does not identify influential peers and therefore cannot assign more trust to influential nodes. Collectivist cultures have a lower dispositional trust and are risk adverse; they often require recommendations from group leaders or other influential peers. Since this is not directly modelled in PeerTrust, the trust level threshold of peers can be increased for this scenario to ensure that peers only transact with other peers they consider very trustworthy. In this way, highly trusted peers can be considered as influential in the PeerTrust model.

d) Out-group members can be trusted if they are recommended by in-group members
The fact that PeerTrust does not differentiate between in-group and out-group members makes it challenging to model this trust property for simulation purposes. However, in the PeerTrust model, a peer receives recommendations from its direct connections. Additionally, personal past experience is also considered in the PeerTrust trust computation. This increases the possibility of a peers direct connections being selected for a transaction. For the purposes of this simulation scenario, this can satisfy this trust property to a lesser extent.
Overall it is clear to see that PeerTrust does not directly support collectivist cultural behaviour. However, for the purpose of this study, simulations are run to attempt to determine the extent to which the PeerTrust model supports collectivist cultural behaviour. The simulation is defined in the next section.

### 8.5.2 Collectivist culture PeerTrust scenario simulation

This scenario is an adjustment of the standard PeerTrust scenario and therefore, many of the settings and components discussed in the standard PeerTrust scenario remain the same for this scenario. However, a few settings are adjusted according to the previous discussion. These settings are presented in Table 8.4.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>The weighting of personal experience (alpha)</td>
<td>0.4</td>
<td>Collectivist cultures rely more on community experience but also have preference towards in-group members.</td>
</tr>
<tr>
<td>The weighting of the community context factor (beta)</td>
<td>0.6</td>
<td>Collectivist cultures place more emphasis on how members maintain group harmony.</td>
</tr>
<tr>
<td>Trust Threshold</td>
<td>0.7</td>
<td>Collectivist cultures are more cautious when trusting strangers.</td>
</tr>
</tbody>
</table>

The settings provided in Table 8.4 are based on collectivist cultural behaviour as indicated in the discussion column of the table. The simulations for this scenario are now run 5 times and the results across them are averaged and evaluated according to the evaluation metrics, in the next section.

### 8.5.3 Collectivist culture PeerTrust scenario evaluation

The collectivist culture PeerTrust scenario provides interesting results. Figure 8.4 is a screenshot of the P2P simulation environment depicting the visual result of the one the simulation runs.
Figure 8.4 Collectivist culture PeerTrust result P2P network

Figure 8.4 indicates that adjusting the PeerTrust model settings to react according to collectivist cultural behaviour creates a high level of trust in the environment. However, this results in malicious peers having a high level of trust which could lead to their selection. Compared to the previous scenario, peers in this scenario have formed a very dense group. This is a result of many peers having high trust levels. When a peer evaluates its current connections many nodes are above the trust threshold and therefore, the relationship is maintained, which leads to the densely clustered group. The output results of this simulation are displayed in Figure 8.5.

The trust value graph in Figure 8.5 depicts that the average trust in the environment increases very soon after the first peers begin transacting and then stabilises over time. The successful transactions graph indicates that the percentage of successful transactions remain relatively low throughout the simulation run.
The results of all 5 simulation runs are averaged and presented in Table 8.5, according to each evaluation metric. This evaluation provides insight into the behaviour of the PeerTrust model adjusted for collectivist cultural behaviour.

### Table 8.5 Collectivist culture PeerTrust evaluation metrics results

<table>
<thead>
<tr>
<th>Evaluation Metric</th>
<th>Simulation Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average trust level over time</td>
<td>0.768</td>
</tr>
<tr>
<td>Percentage of successful transactions over time</td>
<td>33.55%</td>
</tr>
<tr>
<td>Number of malicious peers selected per number of transactions</td>
<td>400</td>
</tr>
</tbody>
</table>

**a) Average trust level over time**

Averaged over 5 runs, the average trust level over time is 0.768. This is a very high trust level and can be a result of adjusting the settings which influence the PeerTrust trust computation. Adjusting the alpha and beta weightings to place more emphasis on the community context factor can result in the high average trust level. According to the PeerTrust model, a peer’s community context factor is increased if a peer provides transaction feedback. This makes it easy for peers to obtain a high community context factor. Setting the weight of this factor to 0.6 greatly influences the trust computation. Therefore, peers will generally have a high trust level if they provide feedback which is common in this environment.
Malicious peers can also provide transaction feedback, whether malicious or not, the PeerTrust model does not differentiate. Therefore malicious nodes can increase their trust level by providing feedback and hence the high trust level of malicious peers in the network, as depicted in Figure 8.4. Consequently, this increases the average trust level of the entire environment, leading to a high average trust level of 0.768.

b) Percentage of successful transactions over time

The collectivist culture PeerTrust scenario simulation achieves a successful transaction rate of 33.55% over 10000 transactions. This is a very low success rate and indicates that, either many malicious peers are being selected for transactions, or peers are under performing when rendering a service. Malicious peers have high trust levels in this simulation which leads to them being selected for transactions. Additionally, the performance of peers plays less of a role in the trust computation since the weight of alpha is now 0.4, compared to the standard PeerTrust scenario which is 0.8. Therefore, poor performance does not result in a low trust level which explains why the average trust level is high but the percentage of successful transactions over time is low.

c) Number of malicious peers selected per number of transactions

In each simulation run, an average of 400 malicious peers are selected for every 2000 transactions. This indicates that for 20% of the transactions, a malicious peer is recommended and chosen as a collaboration partner. This is only slightly higher than the 19.8% achieved by the standard PeerTrust scenario simulation. As previously discussed, this is a result of malicious peers having a high trust level and are therefore selected as transaction partners.

Overall, the collectivist culture PeerTrust scenario simulation does not perform well. Although the average trust level in the environment is high, this leads to many malicious nodes being selected as transaction partners and therefore many unsuccessful transactions occur. The PeerTrust model is thus not designed specifically for collectivist cultural behaviour and attempting to adjust the parameters of the PeerTrust model to support collectivist cultural behaviour produces poor results. However, the PeerTrust model does support standard P2P environments, for which it is designed. Therefore, the Trustcv model uses the PeerTrust model as its foundation, to support the P2P nature of the collectivist digital business ecosystem. In the next section, the Trustcv model is simulated in the scenario for which it is designed – the collectivist digital business ecosystem.
8.6 Trust\textsubscript{cv} scenario simulation and evaluation

The Trust\textsubscript{cv} scenario is derived from the research conducted in the previous chapters. The collectivist digital business ecosystem is simulated by enforcing the behaviour of collectivist cultures in a P2P environment, similar to that defined in the standard PeerTrust scenario. In this section, the collectivist digital business ecosystem environment is defined. This is followed by a simulation of the Trust\textsubscript{cv} scenario and an evaluation of the Trust\textsubscript{cv} scenario.

8.6.1 Collectivist digital business ecosystem simulation environment

The collectivist digital business ecosystem is an environment where SMMEs transact with each other in order to accomplish business transactions. This environment extends the NetLogo implementation of the PeerTrust scenario, which is depicted in Figure 8.6.

The Trust\textsubscript{cv} model and collectivist digital business ecosystem environment have unique features which differentiate it from the standard P2P environment. Similarly, to the standard PeerTrust scenario, the following components of the collectivist digital business ecosystem environment are discussed in this section.

a) SMMEs  
b) Relationships
c) Transactions
d) Trust computation

These components have been extensively modelled in the previous chapter and are therefore, only discussed according to the simulation environment in this section.

a) SMMEs
SMMEs maintain the same information as peers in the previous scenarios. However, according to the $\text{Trust}_{cv}$ model, additional information is required. Therefore the simulation environment maintains the following information, in addition to the information a peer maintains in the previous scenarios:

- $\text{isGroupLeader}$ – This is a flag which indicates if this SMME is a group leader or not.
- $\text{degree}_\text{centrality}$ – This is the value of this SMME’s degree centrality measure.
- $\text{betweenness}_\text{centrality}$ – This is the value of this SMME’s betweenness centrality measure.
- $\text{density}_\text{centrality}$ – This is the value of this SMME’s density centrality measure.

This information enables a SMME to behave in a collectivist cultural manner in the collectivist digital business ecosystem environment. Additionally, SMMEs may behave maliciously and therefore, the same malicious peer settings used by malicious peers in the standard PeerTrust scenario are used by malicious SMMEs in the collectivist digital business ecosystem. This ensures that SMMEs behave in a ways similar to that in a real world collectivist digital business ecosystem environment. Some SMMEs may act maliciously to benefit their own business and/or cause harm to other businesses. Therefore, the $\text{Trust}_{cv}$ model should provide protection against malicious SMMEs.

The peers defined in the standard PeerTrust scenario maintain a list of connections. In the collectivist digital business ecosystem these are known as relationships and are discussed in the next section.

b) Relationships
Relationships play an important role in the collectivist digital business ecosystem, particularly for collectivist cultures. Relationships with other SMMEs define a SMME’s ego-network and therefore its in-group members. In terms of the NetLogo simulation, relationships are implemented in the same way as connections are implemented for peers, through the establishment, maintenance, and removal of links to other agents.
Similarly to the standard PeerTrust scenario, relationships are created when two SMMEs transact with each other, if no relationship already exists. Additionally, relationships can be removed if SMMEs do not maintain the group’s harmony. In the Trust\textsubscript{cv} simulation environment, SMMEs evaluate their group member’s community context factor and if it is below 0.5, the SMME will remove its relationship with that SMME. This simulates the behaviour of collectivist cultures that often ban members from the group that negatively disrupt the group harmony.

The relationships among SMMEs play a major role in determining many of the centrality measures required for the Trust\textsubscript{cv} model and therefore, the implementation of relationships conforms to the Trust\textsubscript{cv} model. Relationships also have an impact on the transaction partners that SMMEs select and recommend. The next section discusses the process of transacting in the collectivist digital business ecosystem environment.

c) Transactions

Suppose a SMME in the collectivist digital business ecosystem network would like to transact there are a number of steps that would occur in the Trust\textsubscript{cv} simulation to facilitate the transaction. These steps are extensively discussed in the previous chapter but are briefly presented again:

1. Specify the service required
2. Identify SMMEs in the network that offer serviceType
3. Select a SMME to transact with
4. Establish a transaction and transact
5. Provide feedback based on the transaction
6. Update the network

The transaction process differs from PeerTrust in step 2 and 6 as discussed in chapter 7. The extensive recommendation behaviour and punishing and rewarding behaviour of the Trust\textsubscript{cv} model is included in this simulation implementation. The next section discusses the trust computation for this scenario.

d) Trust computation

The Trust\textsubscript{cv} model computes trust according to the trust computation presented in Equation 1. However, as defined in the Trust\textsubscript{cv} model, several additional computations are performed which influence trust levels and transactions. The simulation environment for Trust\textsubscript{cv} provides
settings which can be adjusted based on the simulation requirements. These settings are in addition to those defined in standard PeerTrust scenario:

- **rate_random_partner_selection** – This setting defines the frequency at which members of a group in the collectivist digital business ecosystem select random members outside the group. This is required to establish groups in the collectivist digital business ecosystem upon initial transactions, for simulation purposes.

- **group_recommendation_error_rate** – This setting defines the frequency of significantly bad and significantly good recommendations group members make, when recommending potential transaction partners.

- **degreeInfluentialThreshold** - This setting defines the threshold value which determines if a SMME has a high degree centrality measure within the collective digital business ecosystem.

- **betweennessInfluentialThreshold** - This setting defines the threshold value which determines if a SMME has a high betweenness centrality measure within the collective digital business ecosystem.

- **additionalInfluentialTrust** - This value is used to enhance the recommendationValue of a SMME based on the Trustcv model computations.

- **groupLeaderThreshold** – This setting defines the threshold value which determines if a SMME is a group leader within its own ego-network social graph.

- **groupLeaderRecommendationValue** – This value defines the enhanced recommendationValue which is assigned to a recommendations provided by a group leader.

- **denseGroupThreshold** – This setting defines the threshold value which determines if a SMME belongs to a dense group within the collectivist digital business ecosystem.

- **densityMinimumMembers** – This setting defines the minimum number of members a group can have before it is considered dense.

- **responsibilityThreshold** – This setting defines the threshold value which determines if a recommendation from a SMME in another SMMEs group is accurate or inaccurate. This value allows the simulation to determine if a SMME is punished or rewarded for their recommendation.

- **punishmentValue** – This value defines the extent to which a SMME is punished for an inaccurate recommendation.

- **rewardValue** – This value defines the extent to which a SMME is rewarded for providing an accurate recommendation.
All these settings provide values that are specific to the Trust\textsubscript{cv} model and are used to ensure the accurate simulation of the Trust\textsubscript{cv} model. There are additional settings and controls implemented into the simulation environment for the Trust\textsubscript{cv} model but these are not relevant for the current discussion and can be viewed in Appendix A. In the next section, the Trust\textsubscript{cv} simulation is performed.

### 8.6.2 Trust\textsubscript{cv} scenario simulation

In the collectivist culture PeerTrust scenario, simulation settings were defined based on the behaviour of collectivist cultures. To maintain consistency, the same settings are used in the Trust\textsubscript{cv} scenario with the exception of the Trust Threshold setting, and are presented in Table 8.6. Since the Trust\textsubscript{cv} model is designed and implemented specifically for collectivist cultural behaviour, it is not required that the trust threshold is increased to handle the low dispositional trust and risk adverse behaviour of collectivist cultures.

#### Table 8.6 Trust\textsubscript{cv} scenario simulation settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>The weighting of personal experience (alpha)</td>
<td>0.4</td>
<td>Collectivist cultures rely more on community experience but also have preference towards in-group members.</td>
</tr>
<tr>
<td>The weighting of the community context factor (beta)</td>
<td>0.6</td>
<td>Collectivist cultures place more emphasis on how members maintain group harmony.</td>
</tr>
<tr>
<td>Trust Threshold</td>
<td>0.5</td>
<td>This is the average trust level possible and in this scenario, used as the threshold.</td>
</tr>
</tbody>
</table>

The specific Trust\textsubscript{cv} model settings contain values which have been predetermined by the researches, based on preliminary experiments, as appropriate for the simulation of a collectivist digital business ecosystem with 100 SMMEs. These are presented in Table 8.7.
Table 8.7 Trustcv scenario collectivist cultural settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate_random_partner_selection</td>
<td>20%</td>
<td>This value enables the bootstrapping of the environment so groups can form.</td>
</tr>
<tr>
<td>group_recommendation_error_rate</td>
<td>30%</td>
<td>This value is low enough so that group members can make mistakes but not often.</td>
</tr>
<tr>
<td>degreeInfluentialThreshold</td>
<td>10</td>
<td>For such an environment this value is a good representation of high degree SMMEs.</td>
</tr>
<tr>
<td>betweennessInfluentialThreshold</td>
<td>200</td>
<td>For such an environment this value is a good representation of high betweenness SMMEs.</td>
</tr>
<tr>
<td>additionalInfluentialTrust</td>
<td>0.6</td>
<td>This value can enhance a recommendationValue for a recommendation from an influential node.</td>
</tr>
<tr>
<td>groupLeaderThreshold</td>
<td>5</td>
<td>For such an environment this value is a good representation of a group leader.</td>
</tr>
<tr>
<td>groupLeaderRecommendationValue</td>
<td>0.4</td>
<td>This value enhances a recommendationValue for a group leader recommendation.</td>
</tr>
<tr>
<td>denseGroupThreshold</td>
<td>0.3</td>
<td>For such an environment this value is a good representation of dense groups.</td>
</tr>
<tr>
<td>densityMinimumMembers</td>
<td>3</td>
<td>For such an environment this value is a good representation of the minimum size for dense groups.</td>
</tr>
<tr>
<td>responsibilityThreshold</td>
<td>0.4</td>
<td>For such an environment this value is a good indication as to how</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>responsible group members should be.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>punishmentValue</td>
<td>0.4</td>
<td>This value decreases a SMME’s community context factor slightly.</td>
</tr>
<tr>
<td>rewardValue</td>
<td>0.4</td>
<td>This value increases a SMME’s community context factor slightly.</td>
</tr>
</tbody>
</table>

The simulation environment is setup according to these settings for the Trustcv scenario and simulation is run 5 times. The results of these simulations are presented and discussed in the next section.

### 8.6.3 Trustcv scenario evaluation

The simulation of the Trustcv model provides interesting results that are examined and discussed in this section. Figure 8.7 is a screenshot of the visual result of the collectivist digital business ecosystem for one of the simulations run.
Figure 8.7 Trust$_{cv}$ result for the collectivist digital business ecosystem

Figure 8.7 indicates that a tight cohesive group is formed over time where many SMMEs have a high trust level and malicious SMMEs have low trust levels. Malicious nodes are also not key members in the tight cohesive trust group which ensures they are not considered as influential nodes in any way. The additional output results of the Trust$_{cv}$ scenario simulation are depicted in Figure 8.8.
The trust value graph indicates that over time, the average trust level in the environment increases. This is a result of groups forming and becoming more cohesive. Consequently, SMMEs perform better so as to maintain and enhance group harmony thereby increasing their trust level. The successful transactions graph shows a slight increase over time. This is related to the formation of cohesive groups, which leads to more accurate and reliable recommendations from in-group members.

The results of all 5 simulation runs are averaged and presented in the Table 8.8 according to each evaluation metric. This evaluation is discussed to provide more insight into the behaviour of the Trustcv model relative to the PeerTrust model.

**Table 8.8 Trustcv evaluation metrics results**

<table>
<thead>
<tr>
<th>Evaluation Metric</th>
<th>Simulation Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average trust level over time</td>
<td>0.556</td>
</tr>
<tr>
<td>Percentage of successful transactions over time</td>
<td>70.57%</td>
</tr>
<tr>
<td>Number of malicious peers selected per number of transactions</td>
<td>26</td>
</tr>
</tbody>
</table>
a) Average trust level over time
The average trust level over time is 0.556 and remains relatively stable throughout the simulations. This value is very similar to the results of the standard PeerTrust scenario simulation. The Trust\textsubscript{cv} simulation indicated that the average trust level in the network increased over time, as strong cohesive groups are formed. However, in the beginning of the simulation, the average trust level decreases due to malicious nodes being identified for the first time and their trust levels consequently being reduced. This may be the cause for the Trust\textsubscript{cv} scenario simulation having a similar trust level compared to the standard PeerTrust scenario. It decreases slightly initially but then increases over time.

Compared to the collectivist culture PeerTrust scenario simulation, the average trust level over time is lower in the Trust\textsubscript{cv} scenario. However, the collectivist culture PeerTrust scenario concluded that the high average trust level was a result of malicious peers having high trust levels. Therefore, the Trust\textsubscript{cv} scenario provides a stable average trust level over time that is similar to the standard PeerTrust scenario but not as high as the collectivist culture PeerTrust scenario. This is the desired result, relative to the collectivist culture PeerTrust scenario.

b) Percentage of successful transactions over time
The Trust\textsubscript{cv} scenario simulation achieves a relatively high successful transaction rate of 70.57\% over 10000 transactions. Compared to both of the previous scenarios, this result is much higher. The reason for this may be that more reliable and trustworthy recommendations are provided when a SMME seeks recommendations from its in-group members, group leaders, and influential SMMEs. The PeerTrust model does not implement this feature whereas the Trust\textsubscript{cv} model makes use of social network analysis to implement this according to the behaviour of collectivist cultures. This result makes the Trust\textsubscript{cv} model useful for the collectivist digital business ecosystem which requires successful transactions to ensure the sustainability and growth of the ecosystem.

c) Number of malicious peers selected per number of transactions
Relative to the other scenarios, this is perhaps the most notable result of the Trust\textsubscript{cv} model. Only 26 malicious peers are selected for every 2000 transactions. That is, for only 1.3\% of the transactions, a malicious peer is recommended and chosen as a transaction partner. This is significantly less than both of the previous scenarios.

The reason for this result is supported by the fact that SMMEs, according to collectivist cultures, require and seek recommendations from in-group members, group leaders, and
influential SMMEs. These recommendations are proven, in the simulations, to be more reliable than just treating any recommendation evenly. Additionally, this improves the number of successful transactions in the environment, as reliable and trustworthy transaction partners are recommended and selected. Therefore, this can be considered as the most valuable contribution of the Trust\text{cv} model relative to the PeerTrust model.

The simulation and evaluation of the Trust\text{cv} scenario indicates that the Trust\text{cv} model performs well in supporting collectivist cultural behaviour and consequently the collectivist digital business ecosystem. In the next section, a summary of all the evaluations is provided so as to provide conclusions to the simulation of all the scenarios.

### 8.6.4 Scenario simulation summary and conclusion

All three scenarios are simulated, evaluated, and discussed and their evaluation results are depicted in Figure 8.9, Figure 8.10, and Table 8.9. In Figure 8.9, the average trust value graphs for each simulation scenario are combined and depicted in a single graph. This graph depicts that the collectivist culture PeerTrust scenario has the highest average trust level whereas the standard PeerTrust and Trust\text{cv} scenarios have a similar average trust level, with Trust\text{cv} having slightly more.

![Figure 8.9 Average Trust Value graph for all simulation scenarios](image)

In Figure 8.10, the percentage of successful transactions graphs for each simulation scenario are combined together and depicted in a single graph. This graph indicates that the Trust\text{cv}
scenario has the highest percentage of successful transactions whereas the collectivist culture PeerTrust scenario has the lowest percentage of successful transactions.

![Graph showing % of Successful Transactions](image)

**Figure 8.10 Percentage of Successful Transactions graph for all simulation scenarios**

Table 8.9 provides an overview of all the simulation scenario results according to the evaluation metrics.

**Table 8.9 Scenario simulation summary evaluation metrics results**

<table>
<thead>
<tr>
<th>Evaluation Metric</th>
<th>Standard PeerTrust</th>
<th>Collectivist culture PeerTrust</th>
<th>Trustcv</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average trust level over time</td>
<td>0.514</td>
<td>0.768</td>
<td>0.556</td>
</tr>
<tr>
<td>Percentage of successful transactions over time</td>
<td>53.72%</td>
<td>33.55%</td>
<td>70.57%</td>
</tr>
<tr>
<td>Number of malicious peers selected per number of</td>
<td>396</td>
<td>400</td>
<td>26</td>
</tr>
<tr>
<td>transactions</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 8.9 indicates that the collectivist culture PeerTrust scenario has the highest average trust level over time, followed by the Trustcv scenario and standard PeerTrust scenario, respectively. However, a high average trust level over time does not represent a desired environment, as malicious nodes may also have a high trust level. Therefore, the standard PeerTrust and Trustcv scenarios are more desired since they provide good average trust levels over time that remain consistent and provide a balance between malicious and non-malicious peer’s trust levels.

The percentage of successful transactions over time in the standard PeerTrust and Trustcv scenarios are acceptable and good respectively, whereas the collectivist culture PeerTrust scenario provides an unacceptably low successful transaction rate of 33.55%. Overall, the Trustcv scenario produces the best result, with a successful transaction rate of 70.57% which is much higher than the 53.72% of the standard PeerTrust scenario. The facilitation of successful transactions in an environment is one of the aims of a trust and reputation model and the Trustcv model achieves this for collectivist cultures in the collectivist digital business ecosystem.

The Trustcv model provides good performance in terms of preventing malicious peers from being selected for transactions. Compared to the approximate value of around 400 per every 2000 transactions achieved by the PeerTrust model, the Trustcv model ensures that only around 26 malicious peers are selected for every 2000 transactions. This is a very significant contribution by the Trustcv model since the purpose of a trust and reputation model is to provide information and recommendations so that trustworthy and reliable transaction partners can be identified and selected, and not malicious nodes.

Overall, the Trustcv model performs best, for each evaluation criteria, in the scenario for which it is designed. The PeerTrust model performs well in the standard P2P scenario but fails to provide support for collectivist cultural behaviour. In conclusion, the Trustcv model supports collectivist cultural behaviour in comparison to the PeerTrust model and provides good simulation results. Therefore, the results indicate that the Trustcv model achieves its objective of performing well in a simulation of the collectivist digital business ecosystem and in particular its support for collectivist cultural behaviour.

8.7 Conclusion

This chapter provides an introduction to the NetLogo simulation. The NetLogo environment is extremely customisable and allows for the adjustment of settings so that each the desired
simulation environment can be implemented. Therefore, NetLogo is used for the implementation and simulation of the PeerTrust and Trust\textsubscript{cv} models.

The main purpose of this chapter is to simulate and evaluate the PeerTrust and Trust\textsubscript{cv} models. Scenarios are defined and introduced. These scenarios are simulated and evaluated to determine the how the PeerTrust and Trust\textsubscript{cv} models behave in a specified environment. The simulation settings that are common among all the scenarios are defined and the evaluation metrics are provided.

The standard PeerTrust scenario defines a standard P2P environment and is simulated according to the settings proposed. The evaluation of this scenario simulation indicates that the PeerTrust model performs well in the environment for which it is specifically designed.

Adjusting the PeerTrust scenario settings to support the behaviour of collectivist cultures is defined and simulated. The simulation results are evaluated according to the evaluation metrics. This scenario performs poorly compared to the previous scenario, leading to the conclusion that the PeerTrust model does not support the behaviour of collectivist cultures.

The Trust\textsubscript{cv} scenario is defined and the simulation environment is setup accordingly. Settings are adjusted and set based on the definition of the Trust\textsubscript{cv} model defined in the previous chapter. The simulation and evaluation of the Trust\textsubscript{cv} model prove that it performs well in the collectivist digital business ecosystem simulation environment.

Finally, all the scenarios are compared in Table 8.9 and a conclusion is made. The chapter concludes that the PeerTrust model does not provide support for collectivist cultural behaviour, relative to the Trust\textsubscript{cv} model. The Trust\textsubscript{cv} model performs well in an environment based on the behaviour of collectivist cultures, and therefore supports this behaviour. Additionally, the Trust\textsubscript{cv} model has better performance in an environment that directly extends the standard P2P – the collectivist digital business ecosystem. Therefore, the Trust\textsubscript{cv} model can support the collectivist digital business ecosystem, according to the evaluation conducted in this chapter.
Chapter 9

Conclusion

9.1 Introduction

This dissertation proposes a trust model for collectivist cultures to support trust in a collectivist digital business ecosystem. Supporting trust in a collectivist digital business ecosystem can have a positive effect on the survival and success of SMME and the economy in Africa. The success of a collectivist digital business ecosystem is largely dependent of the digital business ecosystem facilitating successful business transactions among its members by supporting trust. SMMEs then have confidence in selecting transaction partners and are assured that they are likely to behave as expected during and after the business transaction.

In this dissertation, the concept of the collectivist digital business ecosystem was introduced, to empower SMMEs in Africa with existing and current technology. By identifying four trust properties that address collectivist behaviour, an appropriate and relevant trust model is proposed. Social network analysis was motivated as an approach to support the implementation of trust properties for collectivist cultures.

The formal Trust\textsubscript{cv} model is proposed by extending an existing trust and reputation model known as PeerTrust that supports trust in P2P environments such as a digital business ecosystem. The PeerTrust model gave the foundation for the Trust\textsubscript{cv} model, and the addition of a social graph made it possible to support the collectivist cultural trust properties through the use of social network analysis. The simulation of the PeerTrust and Trust\textsubscript{cv} models, using the same simulation underpinning, ensured that the Trust\textsubscript{cv} model more supportive of the collectivist digital business ecosystem than the PeerTrust model.

The motivation for this research was proposed in chapter 1 together with the objective of this research. The research has been conducted and in this chapter the research objective is revisited to determine the success of the dissertation. Additionally, the limitations of the research are presented and future research opportunities are discussed. Finally the chapter is concluded.
9.2 Revisiting the research objective

The primary objective of this research is to propose a trust model for collectivist cultures that can support trust in a collectivist digital business ecosystem. In order to determine if the research objective has been met, the research questions identified in chapter 1 are revisited.

1. How can SMMEs be supported by technology to grow their business?

The following secondary research questions are address:

a) What is the state of SMMEs in Africa and how do they conduct business?

Background research into the state of SMMEs in Africa shows that technology is not being used to its full potential. Currently, business operations among SMMEs in Africa, particularly very small enterprises, are manual, slow and error-prone. SMMEs in Africa use mobile devices as their main and sometimes only business technology infrastructure and therefore this technology needs to be supported. Access to the Internet is more readily available but other technology infrastructure is very limited.

Additionally, there are a number of benefits such as discounted buying and reduced travel costs associated to forming collaborations with other SMMEs. However, SMMEs tend to be very wary of transacting with other SMMEs due to lack of trust in other SMMEs. SMMEs in Africa SMMEs in Africa, particularly very small enterprises operate on a very informal level making their approach to business very personal and culture related. Recommendations from other SMMEs are required to assist SMMEs to make informed decisions regarding potential transaction partners.

b) What are the properties of a digital business ecosystem?

The research identified that the properties of a digital business ecosystem generally conform to the properties of P2P architectures implemented over Internet technology. A digital business ecosystem has the following properties: open environment, decentralised architecture, scalability, robustness, and self-organisation. Therefore chapter 2 defines the following requirements for the implementation of a digital business ecosystem in Africa:

i. Digital business ecosystem facilitates collaborations through mobile and cloud technology

ii. Digital business ecosystem supports trust and reputation in a decentralised architecture
iii. Digital business ecosystem complies to the cultural behaviour and beliefs of the participants

2. How can trust be supported by a collectivist digital business ecosystem?

The following secondary research questions are address:

a) What are the constructs and properties of trust?

The constructs of trust were presented by McKnight and Chervany (1996) and are, namely ‘dispositional trust’, ‘situational decision to trust’, ‘trusting beliefs’, ‘system trust’ that together support the construct ‘trusting intentions’, and eventually result in establishing ‘trusting behaviour’. However, the role of culture in the constructs of trust is not proposed.

b) Which existing trust models are appropriate to be used by a collectivist digital business ecosystem?

A number of trust models were analysed, yet the PeerTrust model provided the best support for a digital business ecosystem environment. This is a well reference trust model and addresses the properties of a collectivist digital business ecosystem. Additionally, it is flexibility and can therefore be extended to support additional properties such as cultural behaviour. The PeerTrust model can be used and extended as follows:

- Provides a P2P overlay network for the digital business ecosystem.
- Facilitates collaborations among SMMEs and other members of the digital business ecosystem.
- Provides trust and reputation data for SMMEs based on PeerTrust computations.
- Extend PeerTrust computation with cultural properties and social network information.

The secondary research questions are addressed in chapter 3 and provide a detailed and comprehensive understanding of trust and describe how trust can be supported in a digital business ecosystem in Africa.

3. How does cultural behaviour influences trust in a collectivist digital business ecosystem?

The following secondary research questions are address:

a) What is the dominant culture in Africa and how does it differ from other cultures?
The cultural dimension, individualist vs. collectivist, is considered as the main and most significant dimension for comparing cultures. Two use cases are presented by the research in this dissertation which describes the differences between individualist and collectivist cultures. People in Africa such as owners and employees of SMMEs generally belong to the culture identified as collectivist culture.

b) Which specific norms and behaviour of this culture influences the formation of trust?

Collectivist cultures are different from other cultures mainly because of their concern for group harmony and social standing. They are concerned about maintaining the group harmony and consider in-group members as largely preferential to out-group members. Also, they place value on influential nodes and consider their opinion very highly.

c) Can a set of trust properties be identified to support trust in a collectivist digital business ecosystem?

One of the main contributions of this research is the identification of for trust properties for collectivist cultures. These properties are identified as follows:

i. Members of a group that maintain group harmony are trusted more
ii. Members of a group trust in-group members more than out-group members
iii. Influential nodes such as group leaders are trusted more
iv. Out-group members can be trusted if they are recommended by in-group members

These secondary research questions are addressed in chapter 4 and provide an understanding of how cultures differ and the behaviour of collectivist cultures.

4. How can identified trust properties be implemented in a collectivist digital business ecosystem?

The following secondary research questions are address:

a) What are the benefits of using social network analysis when implementing trust?

The research conducted in chapter 5 discusses that social network analysis, which is includes techniques for analysing social networks, has several benefits. It can be used to extract communities in large social networks. Social network analysis can also be used to identify trusted, expert and prominent actors that are key nodes in a social network. Additionally, these techniques can be used to predict trust between actors in a social network, making social network analysis useful when implementing trust.
b) How can social network analysis be applied in a collectivist digital business ecosystem?

Culture is a social concept and social network analysis is able to analyse social relationships and derive useful information. Therefore, social network analysis is motivated to address the behaviour of collectivist cultures through the use of an ego-network social graph and centrality measures.

c) Which social network analysis measures influence trust?

Centrality measures are analysed and the following three centrality measures are considered as appropriate for the digital business ecosystem based on the predefined requirements: degree, density, and betweenness centralities. These centrality measures influence trust and conform to the decentralised nature of the digital business ecosystem.

d) What is the state-of-the-art when social network analysis measures are applied to trust models?

The state-of-the-art shows that the degree, density, and betweenness centrality are effectively used in popular, well-known trust and reputation systems, where the network is represented as a social graph. However, none of these centrality measures are used to address the cultural trust properties of collectivist cultures.

e) How can social network analysis measures be used to implement the identified trust properties?

Chapter 5 identifies a way of implementing these properties in a trust model using social network analysis. Firstly, an ego-network social graph is used to determine a SMMEs group so that in-group members and group leaders can be identified. Secondly, the degree and betweenness centrality measures are used to model influential nodes in the social graph. Finally, the density centrality is used to identify dense cohesive groups in the network, influencing the group leader selection.

These secondary research questions are addressed in chapter 5 where an understanding of social network analysis and its use in the collectivist digital business ecosystem is provided.
5. How can trust be incorporated by a collectivist digital business ecosystem?

The following secondary research questions are addressed:

a) What are the architectural components of such a trust model?

The architecture of Trust\textsubscript{cv}, proposed in chapter 6, supports mobile and cloud technology by allowing a software agent, representing a SMME, to be implemented on a mobile device or in the cloud. A Trust Manager, Data Locator, Trust Data and Transaction Tool are the main components of the Trust\textsubscript{cv} architecture. These components handle the computation of trust, transfer of data between SMMEs, storing of trust data, and the personalisation of the trust model. These components are extended from the PeerTrust model, to provide support for trust in the collectivist digital business ecosystem.

b) How are the collectivist trust properties modelled and implemented using social network analysis?

The Trust\textsubscript{cv} model consists of a trust environment and trust constituents and operations that are founded on the PeerTrust model but is extended for the collectivist digital business ecosystem. An ego network social graph for each SMME is modelled and social network analysis is performed on this graph. To support collectivist cultures, the collectivist trust properties are supported by social network analysis centrality measures. Group leaders are identified and recommendations from these SMMEs can be obtained. This is achieved using the degree and density centralities. Additionally, in-group members can provide recommendations and are rewarded and punished based on the accuracy of their recommendations. Influential nodes are also identified using the degree and betweenness centrality measures and recommendations can also be obtained from these nodes.

The addressing of these research questions defines how the Trust\textsubscript{cv} model incorporates trust in the collectivist digital business ecosystem. Chapter 7 discusses this in extensive detail.

6. Does the trust model proposed by this research in fact support collectivist behaviour?

The following secondary research questions are addressed:

a) Which multi-agent simulation tool can be used to simulate the use of trust in the collectivist digital business ecosystem?
NetLogo is used to simulate a multi-agent environment where agents interact with each other through transactions and form connections with each other based on transactions. For PeerTrust, the multi-agent environment is implemented and simulated as a P2P environment where agents are peers. As far as the researcher is aware, this is the first implementation of the PeerTrust model in the NetLogo environment. For Trust\textsubscript{cv}, the multi-agent environment is the collectivist digital business ecosystem, and the agents are SMMEs. NetLogo is a multi-agent programmable modelling environment built on Java and Scalar programming languages and is used by researchers worldwide and is provided a customisable simulation environment for the purpose of this study.

b) What simulation scenarios and evaluation criteria can be used to assess the effectiveness of the proposed trust model?

The research provides three scenarios that are used to evaluate the effectiveness of the Trust\textsubscript{cv} model. Firstly, the PeerTrust model is simulated in its standard P2P environment. Secondly, the settings and parameters of the standard PeerTrust simulation are adjusted to simulate the behaviour of collectivist cultural peers in this environment. Finally, the Trust\textsubscript{cv} is simulation in the collectivist digital business ecosystem environment.

To evaluate the performance of the PeerTrust and Trust\textsubscript{cv} model in these scenarios, the following evaluation criteria were defined:

i. Average trust level over time
ii. Percentage of successful transactions over time
iii. Number of malicious peers selected per number of transactions

These evaluation criteria, together with the simulation scenarios provide a means to evaluate the effectiveness of the Trust\textsubscript{cv} model.

c) To what extent does the proposed trust model meet the identified evaluation criteria and which deficiencies can be identified?

Overall, the Trust\textsubscript{cv} model performed best, for each evaluation criteria, in the scenario for which it is designed. It was able to provide very reliable recommendations and therefore contributed to a relatively high percentage of successful transactions while maintaining an average trust level in the ecosystem. The PeerTrust model performed well in the standard P2P scenario but failed to provide support for collectivist cultural behaviour.
The Trust\textsubscript{cv} model simulation performed well but nevertheless, took a relatively long time to simulate the environment and model compared to the other simulation scenarios. Since, the Trust\textsubscript{cv} model makes use of a social graph and performs additional social network analysis computation, it is more computationally expensive.

The satisfaction of the research objective gives an indication as to the success of the dissertation. Although the research provided positive results, there are still a number of limitations of the research which are discussed in the next section.

9.3 Limitations of the research

There are several limitations in the research which can be considered by future research. The limitations are related to the trust computation for Trust\textsubscript{cv}, the simulation of PeerTrust and Trust\textsubscript{cv}, and the evaluation of the Trust\textsubscript{cv} model. Each limitation is discussed in this section.

9.3.1 Limitations regarding the Trust\textsubscript{cv} trust computation

In chapter 7, the Trust\textsubscript{cv} model is comprehensively modelled. The Trust\textsubscript{cv} model uses social network analysis computations, such as determining degree, density, and betweenness centrality measures that come at the cost of computational resources.

The use of an ego-network social graph, rather than a socio network social graph, significantly reduces the computational requirements as a relatively smaller number of nodes are considered in the computation. The simulation of the PeerTrust and Trust\textsubscript{cv} indicated that the Trust\textsubscript{cv} simulation took longer to process the simulation than the PeerTrust simulations, due to the extra computations. Future enhancements to the Trust\textsubscript{cv} model and simulation implementation, should consider optimising the social network analysis computations that are performed.

9.3.2 Limitations regarding the simulation environment

In chapter 8, both the PeerTrust and Trust\textsubscript{cv} models are implemented using the NetLogo simulation tool. They are modelled as closely as possible to the research conducted in this study, but have not been validated against real world scenarios. People may behave differently in the real world when interacting with a digital business ecosystem agent on their computing device. Future work should consider validating the PeerTrust and Trust\textsubscript{cv} simulations against a real world scenario to determine their accuracy.
9.3.3 Limitations regarding the evaluation of Trust_{cv}

This limitation is closely related to the previous limitation. The evaluation of the Trust_{cv} model considers its effectiveness in supporting trust, against the PeerTrust model in a simulation environment. As mentioned previously, the accuracy of the Trust_{cv} simulation and PeerTrust simulation has not been proven against a real world scenario. Additionally, according to the evaluation conducted in chapter 8, the Trust_{cv} model can support trust in the collectivist digital business ecosystem through addressing collectivist cultures. However, in the real world, SMMEs in Africa might behave differently, or may not accept such a trust model. Future research should consider validating the Trust_{cv} model in a real world environment.

9.4 Further research

The research conducted in this dissertation provides a foundation upon which further research can build, particularly in the context of a trust model aimed at collectivist cultures. This section provides suggestions for further research.

9.4.1 Optimising the Trust_{cv} trust computation

Following from the limitations discussed previously, the Trust_{cv} model trust computation can be optimised. Caching social network analysis computation results as well as trust results can be a possible solution. This reduces the number of computation requirements as recent computation results can be accessed or passed to other agents. If agents have not been involved in any transactions which would have altered the computation results, then the cached results can be used. Additionally, the centrality measure computations could be optimised. This would also reduce the computational requirements by reducing the computation complexity of the algorithms. The current implementation does not optimise the social network analysis computations and therefore a future research opportunity exists.

9.4.2 Implementing the Trust_{cv} model in a real world scenario

Further research could also consider implementing the Trust_{cv} model in a real world environment. This would involve the implementation of the SMME agent which can be installed on a mobile device or accessed on the cloud. The implementation would have to satisfy the architecture requirements presented in chapter 6 and also make use of the algorithms defined in the model chapter (chapter 7). The algorithms could be extracted from the simulation which is implemented using a combination of Java and Scalar or be redeveloped in another
programming language. This implementation of the Trust$_{cv}$ model would enable the trust model to be tested in a real world scenario, where real SMMEs can provide feedback based on the recommendations and computations performed by the Trust$_{cv}$ model.

9.4.3 Verification of the simulation environment

The previously discussed further research suggestion can provide an opportunity to verify the Trust$_{cv}$ simulation implementation with a real world scenario. The same environment setup can be established in the real world and in a simulation and the results can be compared. This can provide an indication of how accurate the Trust$_{cv}$ simulation implementation is to real world scenarios. If the results are successful, the Trust$_{cv}$ simulation can be used to simulate a several scenarios, providing a means of testing certain situation before introducing them into the real world.

9.4.4 Collectivist digital business ecosystem implementation

The research conducted in this dissertation is based on a theoretical collectivist digital business ecosystem which is the extension of a comprehensively researched digital business ecosystem initiative arranged by the European Commission. Future research could consider a real world implementation of a collectivist digital business ecosystem based on the properties defined in chapter 2 of this dissertation. This would provide an environment for SMMEs in Africa to compete and collaborate. Additionally, this would be an ideal scenario to evaluate the effectiveness of the Trust$_{cv}$ model, as it is specifically designed for this environment.

9.4.5 Trust$_{cv}$ for other regions

In this dissertation, the Trust$_{cv}$ model addressed the properties of a digital business ecosystem as well as the trust properties of collectivist cultures in Africa. However, future research could map the trust properties of collectivist cultures with other cultures in other regions such as South America or Asia. This could provide an indication of the potential of the Trust$_{cv}$ model in regions other than Africa. With the foundation of the Trust$_{cv}$ model, other regions can be considered and their cultural trust properties specifically implemented. This may be a completely new implementation or an adjustment of the trust properties already implemented in the Trust$_{cv}$ model. This would enable the trust model to adapt to the environment and
support different cultures. Research in this area has already begun, particularly in emerging economy regions (Clarke et al., 2013).

9.5 Conclusion

The dissertation is concluded in this chapter, presenting the contribution of the research, the satisfaction of the research objective, the limitations of the research, and further research opportunities. The main goal of this dissertation was to propose a trust model for collectivist cultures that can support trust in a collectivist digital business ecosystem.

The research is conducted in a number of fields to reach the goal of the dissertation. These fields include digital business ecosystems, SMMEs in Africa, trust and reputation, culture and its influence on trust, social network analysis and simulation tools. Researching these areas, in the context of proposing a trust model, provided contributions that may not have been proposed otherwise.

In chapter 2, the researcher considers how the economy and state of ICT in Africa for SMMEs can be combined with the concept of digital business ecosystems to provide support to the economy of Africa. An analysis on existing trust models for their support of digital business ecosystems is conducted in chapter 3. Additionally, the influence of culture on trust is researched and the researcher appends the trust constructs proposed by (McKnight and Chervany, 1996) to consider culture as a major influence with regards to the way in which trust is constructed.

The study of extracting trust information from social network analysis is accomplished by combining centrality measures with collectivist cultural trust properties. Further, the implementation of social network analysis in a trust model has previously been researched and implemented but not to the extent achieved in the Trust\textsubscript{cv} model, where it directly impacts trust.

This simulation of the PeerTrust model could potentially be used by other researchers who wish to test their theories in a PeerTrust simulation environment. Similarly, the dissertation provides a simulation tool which implements the Trust\textsubscript{cv} model. This implies a simulation tool which simulations a digital business ecosystem, performs social network analysis, and computes trust according to collectivist cultures. Such an environment may be useful for future research.
The research conducted in this dissertation is successful according to the research objective and questions presented in chapter 1. The goal of proposing a trust model for collectivist cultures that can support trust in a collectivist digital business ecosystem has been achieved. Several contributions have been made by the research conducted in this chapter. Additionally, the research has limitations which, together with its success, provide several opportunities for future research.
References


References


References


Google+ 2013.


References


Kew, J. & Herrington, M. 2009. ICT usage amongst lower-end SMMEs in South Africa. The Graduate School of Business, University of Cape Town.


Mabuza, D. C. 2009. The cooperatives model as an approach to SMME development in South Africa with specific reference to the information, communication and technology (ICT) sector.


Mbigi, L. 2003. Leveraging emotional and spiritual resources to increase brand equity. PEOPLE DYNAMICS, 21, 10-16.


Padak, A. 2005. Developing a software to determine the microcontroller specifications for fuzzy logic control applications.


Ratnasingam, P. 2001. Interorganizational trust in business to business e-commerce, Erasmus University Rotterdam.


Schlägel, C. & Wolff, B. 2007. Country-Specific Effects of Reputation and Information: A Comparison of Online Auctions in Germany, the UK, and the US.


Twitter 2013.


Zimmermann, P. R. 1995. The official PGP user’s guide, MIT Press.

Appendix A

Simulation Environment for PeerTrust and Trust\textsubscript{cv}

In chapter 8, detailed descriptions of the PeerTrust and Trust\textsubscript{cv} NetLogo simulation environments are provided. However, some additional components exist in the implementation of these trust model simulations, which are not presented or discussed in chapter 8. Therefore, this appendix discusses the PeerTrust and Trust\textsubscript{cv} simulation environments with specific reference to the components not mentioned in chapter 8.

A.1 PeerTrust simulation environment

In Figure 1, the setting components of the PeerTrust NetLogo simulation environment are provided.

![Figure 1 PeerTrust NetLogo simulation settings](image)

There are several settings components which are not mentioned in chapter 8 which will be discussed in this section.
### Table 1. Additional PeerTrust simulation environment components and settings

<table>
<thead>
<tr>
<th>Setting/Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate_of_peer_removal</td>
<td>This defines the frequency at which peers are automatically removed from the P2P network being simulated.</td>
</tr>
<tr>
<td>rate_of_random_peer_adding</td>
<td>This defines the frequency at which peers are automatically added to the P2P network being simulated.</td>
</tr>
<tr>
<td>collusive_malicious_peers</td>
<td>This setting toggles the collusive behaviour of malicious peers in the P2P network. When this is toggled on, malicious peers will work together and create groups to behave maliciously.</td>
</tr>
<tr>
<td>collusive_transaction_frequency</td>
<td>If collusive_malicious_peers is toggled on, this setting defines the frequency at which malicious peers perform collusive transactions.</td>
</tr>
<tr>
<td>collusive_group_size</td>
<td>If collusive_malicious_peers is toggled on, this setting defines the size of the collusive group relative to the number of malicious peers in the P2P network.</td>
</tr>
<tr>
<td>psm_credibility</td>
<td>The default PeerTrust trust computation determines a peer's credibility by assigning its trust level as its credibility value. However, another computation is defined in the PeerTrust model, known as the Personalized Similarity Measure. This measure computes credibility as the similarity between the ratings that peers give to other common peers. The psm_credibility toggles the use of PSM instead of the default credibility.</td>
</tr>
<tr>
<td>Manually Add New Peer</td>
<td>This setting encapsulates the settings for manually adding a peer to the network while a simulation has been setup or started. A new peer can be set as malicious or not by toggling the new_malicious setting on or off, respectively. Additionally, the initial trust level of this peer can be set by the new_initial_trust setting. The Add button then adds a new peer to the P2P network, currently being simulated, according to the settings defined previously.</td>
</tr>
</tbody>
</table>
These settings are adapted from the PeerTrust model and can be used to simulate different behaviour in the P2P environment being simulated. Since the Trust\textsubscript{cv} simulation implementation extends the PeerTrust simulation implementation, these settings are also available to the Trust\textsubscript{cv} model but have not been specifically tested for the purpose of this research. Additionally, the Trust\textsubscript{cv} simulation environment provides a number of components that relate the Trust\textsubscript{cv} model, not mentioned in chapter 8. These are discussed in the next section.

A.2 Trust\textsubscript{cv} simulation environment

The Trust\textsubscript{cv} NetLogo simulation implementation provides functionality which can be used to visualise the social network analysis computations and Trust\textsubscript{cv} algorithms performed by Trust\textsubscript{cv}. Figure 2 depicts the buttons on the simulation environment that provide this additionally functionality.

![Figure 2. Additional Trust\textsubscript{cv} simulation environment functionality](Image)

All these buttons and associated functionality are now discussed.
a) Remove NB nodes

This button provides functionality to remove all NB nodes from the environment. NB nodes refer to nodes that are considered influential in the digital business ecosystem environment based on their betweenness, and degree centrality measures. Figure 3 depicts the structure of the digital business ecosystem network before ‘Remove NB Nodes’ is clicked. Red nodes are malicious SMMEs, green nodes are good (non-malicious) SMMEs, and blue nodes are good influential SMMEs. Figure 4 is the exact same digital business ecosystem network but after all influential nodes have been removed from the network.

![Figure 3. Before Remove NB Nodes](image1)

![Figure 4. After Remove NB Nodes](image2)

Figure 3 and Figure 4 indicate that influential nodes play a major role in maintaining the structure of the digital business ecosystem network. Such nodes ensure that connections exist between a large number of nodes and without them, the quality of the network structure and the connection potential of nodes can decrease.

b) Perform SNA

This button will perform social network analysis on the current snapshot of the digital business ecosystem network. The degree, density, and betweenness centrality measures will be computed. Additionally, the algorithms to determine if a node is influential, identify dense groups, and to identify group leaders are all executed. These results are cached so that functionality, discussed next, can make use of these results.
c) **Show Influential Nodes**

This button provides functionality to visually display SMMEs that are influential in the digital business ecosystem network. Figure 5 is an example of the visual display of influential nodes in a simulation. Blue nodes are good influential SMMEs.

![Figure 5. Influential nodes in a Trustcv simulation](image)

Figure 5 indicates the influential nodes are well connected and exist along many shortest paths connecting nodes. These nodes have influence over information, connections, and recommendations in the digital business ecosystem network making them important for the sustainability and success of the digital business ecosystem.

d) **Show Group Leaders**

This button provides functionality to visually display SMMEs that are group leaders in the digital business ecosystem network. Figure 6 is an example of the visual display of group leader nodes in a simulation. White nodes are group leader SMMEs. It is no surprise that in Figure 6, many group leaders are the same nodes that were identified as influential in the network. Group leaders are influential nodes that belong to dense groups in the network. In the Trustcv model, group leaders have influence in terms of providing recommendations. This is beneficial to the network since they are usually well connected and well established in the digital business ecosystem network.
e) **Show Dense Groups**

This button provides functionality to visually display SMMEs that belong to dense groups in the digital business ecosystem network. Figure 7 is an example of the visual display of nodes belonging to dense groups in a simulation. Pink nodes are good (non-malicious) SMMEs that belong to dense groups and orange nodes are malicious SMMEs that belong to dense groups.
Some dense groups contain malicious nodes but fortunately there are not many such groups and it is likely that in the near future, malicious nodes will be kicked out of these dense groups according to the Trust\textsubscript{cv} model.

f) Show Betweenness Nodes

This button provides functionality to visually display SMMEs that have a betweenness value greater than the betweennessInfluentialThreshold set in the simulation environment. Figure 8 is an example of the visual display of nodes with a high betweenness value in a simulation. Purple nodes are good SMMEs with a high betweenness value.

According to Figure 8, nodes with a high betweenness value are seen along many shortest paths and are in influential positions in the network. This is why the betweenness centrality is considered as an important factor in determining influential nodes in the digital business ecosystem network.

g) Show Degree Nodes

This button provides functionality to visually display SMMEs that have a degree value greater than the degreeInfluentialThreshold set in the simulation environment. Figure 9 is an example
of the visual display of nodes with a high degree value in a simulation. Yellow nodes are good SMMEs with a high degree value.

![Figure 9. Nodes with a high degree value in a Trustcv simulation](image)

Similarly to the betweenness centrality, the degree centrality also identifies many nodes that are considered as influential. As Figure 9 depicts, these nodes are well positioned in the digital business ecosystem network and they have many connections. This gives such SMMEs the ability to provide recommendations to other SMMEs in the digital business ecosystem network and control information flow.

The features discussed in this section add to the functionality already provided by Trustcv NetLogo simulation which is discussed in chapter 8. The Trustcv simulation environment can be used to perform social network analysis on networks such as the digital business ecosystem, providing adjustable thresholds and visual displays.

This appendix has introduced and discussed some of the additional features and functionality of the PeerTrust and Trustcv, NetLogo simulation environments developed for the purpose of this research and future research.
Appendix B

Papers Presented Based on this Research

B.1 Enhancing digital business ecosystem trust and reputation with centrality measures

This paper was accepted and presented at the IEEE accredited 11th annual ISSA (Information Security South Africa) conference at the Hayatt Regency Hotel, Rosebank, Johannesburg, South Africa in 2011.

Reference:

B.2 Towards trust and reputation for e-commerce in collectivist rural Africa

This paper was accepted and presented at the seventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2012) in Crete, Greece in 2012.

Reference: