Contents

Preface ix
Acknowledgments xiii
Introduction 1

PART I: The core of Bitcoin and the Blockchain
Chapter 1: Introduction to Bitcoin 7
Chapter 2: The concept of blockchains 11
Chapter 3: Building consensus 15
Chapter 4: Bitcoin basics 25
Chapter 5: Transacting in Bitcoin 31
Chapter 6: The settlement of transactions 41
Chapter 7: Security 55
Chapter 8: Challenges 67

PART II: Bitcoin’s ecosystem
Chapter 9: Wallets 87
Chapter 10: Exchanges and ATMs 111
Chapter 11: Merchants 121

PART III: Bitcoin’s nature
Chapter 12: What are money and currencies? 131

PART IV: Looking beyond Bitcoin
Chapter 14: The environment 155
Chapter 15: Alternative cryptocurrencies 191
Chapter 16: Blockchain beyond cryptocurrencies 217
Chapter 17: Potential to redefine the real world 231

Conclusion 263
I have more for you 267
Appendixes 269
Notes 275
Full table of contents 289
About the author 296
# Full table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>vii</td>
</tr>
<tr>
<td>Preface</td>
<td>ix</td>
</tr>
<tr>
<td>Reading tips</td>
<td>xii</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>xiii</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Introduction to Bitcoin</td>
<td>7</td>
</tr>
<tr>
<td>The end of the financial intermediary</td>
<td>8</td>
</tr>
<tr>
<td>A world with Bitcoin</td>
<td>10</td>
</tr>
<tr>
<td>The concept of blockchains</td>
<td>11</td>
</tr>
<tr>
<td>Stored in a distributed fashion</td>
<td>12</td>
</tr>
<tr>
<td>A chain of blocks</td>
<td>13</td>
</tr>
<tr>
<td>Blockchain explorers</td>
<td>14</td>
</tr>
<tr>
<td>Building consensus</td>
<td>15</td>
</tr>
<tr>
<td>The creation of a block</td>
<td>15</td>
</tr>
<tr>
<td>Cryptographic Hash</td>
<td>16</td>
</tr>
<tr>
<td>Competition to generate a valid hash</td>
<td>17</td>
</tr>
<tr>
<td>The 10-minute rule</td>
<td>20</td>
</tr>
<tr>
<td>Mining evolution and mining pools</td>
<td>21</td>
</tr>
<tr>
<td>Computing power increased</td>
<td>21</td>
</tr>
<tr>
<td>Mining pools appeared</td>
<td>22</td>
</tr>
<tr>
<td>Consensus</td>
<td>22</td>
</tr>
<tr>
<td>How is this difference reconciled?</td>
<td>23</td>
</tr>
<tr>
<td>Bitcoin basics</td>
<td>25</td>
</tr>
<tr>
<td>Bitcoin achieves trust by consensus</td>
<td>26</td>
</tr>
<tr>
<td>Supply</td>
<td>26</td>
</tr>
<tr>
<td>Divisibility</td>
<td>29</td>
</tr>
<tr>
<td>Average time per block</td>
<td>30</td>
</tr>
<tr>
<td>Size of Blocks</td>
<td>30</td>
</tr>
<tr>
<td>Transacting in Bitcoin</td>
<td>31</td>
</tr>
<tr>
<td>Bitcoin Wallets</td>
<td>31</td>
</tr>
<tr>
<td>Digital keys</td>
<td>31</td>
</tr>
<tr>
<td>Getting your first bitcoins</td>
<td>33</td>
</tr>
<tr>
<td>Friends</td>
<td>33</td>
</tr>
<tr>
<td>---------</td>
<td>----</td>
</tr>
<tr>
<td>ATMs</td>
<td>34</td>
</tr>
<tr>
<td>Local sellers</td>
<td>34</td>
</tr>
<tr>
<td>Exchanges</td>
<td>34</td>
</tr>
<tr>
<td>Sending bitcoins</td>
<td>35</td>
</tr>
<tr>
<td>Signing a transaction</td>
<td>36</td>
</tr>
<tr>
<td>Pseudo-Anonymity</td>
<td>38</td>
</tr>
<tr>
<td>The settlement of transactions</td>
<td>41</td>
</tr>
<tr>
<td>Pool of pending transactions</td>
<td>41</td>
</tr>
<tr>
<td>Record transactions in the Blockchain</td>
<td>43</td>
</tr>
<tr>
<td>Double spending</td>
<td>46</td>
</tr>
<tr>
<td>How bitcoins are transferred and recorded in the Blockchain</td>
<td>47</td>
</tr>
<tr>
<td>Splitting and merging records</td>
<td>47</td>
</tr>
<tr>
<td>Examples of bitcoin ownership transfer</td>
<td>49</td>
</tr>
<tr>
<td>Single input for a single output</td>
<td>49</td>
</tr>
<tr>
<td>Single input for multiple outputs</td>
<td>49</td>
</tr>
<tr>
<td>Multiple inputs for a single output</td>
<td>51</td>
</tr>
<tr>
<td>Multiple inputs for multiple outputs</td>
<td>51</td>
</tr>
<tr>
<td>Full transparency and auditability</td>
<td>52</td>
</tr>
<tr>
<td>Irreversibility of transactions</td>
<td>53</td>
</tr>
<tr>
<td>Security</td>
<td>55</td>
</tr>
<tr>
<td>Private keys are everything</td>
<td>55</td>
</tr>
<tr>
<td>Hot and Cold Storage</td>
<td>56</td>
</tr>
<tr>
<td>51% Attack</td>
<td>57</td>
</tr>
<tr>
<td>Finney attack</td>
<td>61</td>
</tr>
<tr>
<td>Quantum computers and Cryptographic Standards</td>
<td>63</td>
</tr>
<tr>
<td>Challenges</td>
<td>67</td>
</tr>
<tr>
<td>Volatility</td>
<td>67</td>
</tr>
<tr>
<td>Acceptance</td>
<td>70</td>
</tr>
<tr>
<td>Scalability</td>
<td>71</td>
</tr>
<tr>
<td>Segregated witness (SegWit)</td>
<td>73</td>
</tr>
<tr>
<td>Payment channels</td>
<td>75</td>
</tr>
<tr>
<td>Sidechains</td>
<td>76</td>
</tr>
<tr>
<td>Lightning networks</td>
<td>78</td>
</tr>
</tbody>
</table>
Forking 81

WALLETS 87

Four properties of wallets 88
  1. Hot vs. Cold wallets 88
  2. Full node vs. Non-full node clients 89
  3. Non-deterministic vs. Deterministic wallets 92

Six types of wallets 97
  1. Desktop wallet 97
  2. Mobile wallets 98
  3. Online wallets 100
  4. Brain wallets 104
  5. Hardware wallets 105
  6. Paper wallets 106

Exchanges and ATMs 111

Exchanges 111
  Platforms to exchange fiat and digital currencies 111
  Using an exchange 112
  Application Programming Interface (API) 113
  Links to the Blockchain 113
  Mt. Gox 114
  Audit of exchanges 114
  The Chinese take it all 115

ATMs 118

Merchants 121
  Bitcoin in commerce 121
    Silk Road 121
    Bitcoin in mainstream commerce 122
  Payment processors 124
    Bitcoin debit cards 127

What are money and currencies? 131
  Money 132
  Currencies 132

Is Bitcoin money? Currency? 135
Bitcoin as a safe haven? 135
   Cyprus 135
   MH17 and Trump 137
Is Bitcoin money? 140
   Bitcoin as a medium of exchange 140
   Bitcoin as a unit of account 141
   Bitcoin as storage of value 142
   Conclusion 143
Is Bitcoin a currency? 144
   Portable 144
   Acceptable 144
   Durable 144
   Recognizable 145
   Fungible 146
   Divisible 147
   Scarce 147
   Conclusion 148
What about the future? 150
   Conclusion on Bitcoin’s nature 152
The environment 155
   PESTEL 155
      Political 156
      Economic 160
      Social 165
      Technological 167
      Environmental 169
      Legal 169
Hype cycle 176
   Does Bitcoin’s price reflect the adoption stage or is it the other way around? 177
Adoption Cycle 178
SWOT 180
   Strengths 181
   Weaknesses 183
<table>
<thead>
<tr>
<th>Opportunities</th>
<th>185</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats</td>
<td>186</td>
</tr>
<tr>
<td>Conclusion</td>
<td>189</td>
</tr>
<tr>
<td>Alternative cryptocurrencies</td>
<td>191</td>
</tr>
<tr>
<td>Different purposes and innovations</td>
<td>192</td>
</tr>
<tr>
<td>Different consensus mechanisms</td>
<td>198</td>
</tr>
<tr>
<td>Proof-of-Work (PoW)</td>
<td>199</td>
</tr>
<tr>
<td>Auxiliary PoW (Merged Mining)</td>
<td>200</td>
</tr>
<tr>
<td>Proof-of-Stake (PoS)</td>
<td>203</td>
</tr>
<tr>
<td>Proof-of-Burn (PoB)</td>
<td>205</td>
</tr>
<tr>
<td>Other consensus mechanisms</td>
<td>208</td>
</tr>
<tr>
<td>Hybrid consensus mechanisms</td>
<td>210</td>
</tr>
<tr>
<td>Different ways to supply new coins</td>
<td>210</td>
</tr>
<tr>
<td>Pre-sale (aka Initial Coin Offering [ICO])</td>
<td>211</td>
</tr>
<tr>
<td>Pre-mined</td>
<td>212</td>
</tr>
<tr>
<td>Airdrop</td>
<td>212</td>
</tr>
<tr>
<td>Burning coins</td>
<td>212</td>
</tr>
<tr>
<td>Mining</td>
<td>213</td>
</tr>
<tr>
<td>Cryptocurrencies at war</td>
<td>213</td>
</tr>
<tr>
<td>Conclusion</td>
<td>215</td>
</tr>
<tr>
<td>Blockchain beyond cryptocurrencies</td>
<td>217</td>
</tr>
<tr>
<td>Purely Private, Permissioned, and Public Distributed ledgers</td>
<td>218</td>
</tr>
<tr>
<td>Data storage</td>
<td>219</td>
</tr>
<tr>
<td>Traceability of ownership</td>
<td>219</td>
</tr>
<tr>
<td>Smart contracts</td>
<td>220</td>
</tr>
<tr>
<td>A simple bet</td>
<td>221</td>
</tr>
<tr>
<td>Delayed flight insurance</td>
<td>222</td>
</tr>
<tr>
<td>Oracles</td>
<td>223</td>
</tr>
<tr>
<td>Limitations</td>
<td>223</td>
</tr>
<tr>
<td>Updating and canceling smart contracts</td>
<td>224</td>
</tr>
<tr>
<td>Decentralized applications (Dapps)</td>
<td>224</td>
</tr>
<tr>
<td>Uberizing Uber</td>
<td>225</td>
</tr>
<tr>
<td>The future of cloud: Decentralized cloud</td>
<td>226</td>
</tr>
<tr>
<td>Decentralized Autonomous OrganizationS (DAO)</td>
<td>227</td>
</tr>
</tbody>
</table>
Potential to redefine the real world

Machine-to-machine payments

A washing machine paying for you

Slock.it, a lock for your Airbnb apartment

Conclusion

DLT for businesses

DLT to disrupt financial audits?

Your identity on a DLT?

Today’s form of identity

Building an identity on a distributed ledger

Considerations

DLT for basic income

A basic income? Are you crazy?

The role of DLT

A word of caution

DLT for new forms of governance and democracies

A brief history of democracy

Today’s democracies are under pressure

The opportunities and threats of the Internet

DLT as an enabler

Breaking borders

Caution

Conclusion

The promises of blockchains

The pitfalls of blockchains

Conclusion

I have more for you...

Appendixes

Appendix 1: Block header

Appendix 2: Merkle tree

Appendix 3: Gartner’s hype cycle 2017

Notes

Full table of contents

About the author
Additional information and references
About the author

Jean-Luc Verhelst is a Strategy Consultant working for Monitor Deloitte and is a founding member of BlockchainHub Brussels, a non-profit think tank and information hub part of the global BlockchainHub network. He holds an applied Bachelor’s degree in Information Technology and a Master of Science in Business Administration.

In 2014, his master thesis on Bitcoin received the award for best financial thesis of Belgium by ING Bank. In 2016, he won the world’s largest blockchain hackathon in Dublin. He is recognized as a global blockchain expert within the consulting firm Deloitte and has facilitated and conducted the first EMEA and US trainings. He is currently involved in the development of blockchain projects in multiple industries.

Finally, Jean-Luc is a well-regarded speaker within the Belgian Bitcoin and blockchain community. He is known for his ability to explain technical topics in an inspiring and understandable way, coming up with innovative use-cases while being knowledgeable on the more technical aspects.

Twitter: @JLVerhelst
LinkedIn: Jean-Luc Verhelst
Facebook page: Jean-Luc Verhelst
YouTube channel: jeanlucverhelst
Instagram: BitcoinBlockchainBook

www.jeanlucverhelst.com
www.bitcoinblockchainbook.com

Contact is possible via www.jeanlucverhelst.com
Acknowledgments

“No man is an island,
Entire of itself,
Every man is a piece of the continent,
A part of the main.”

~ John Donne

These verses from John Donne perfectly articulate how nothing can be achieved by one person alone. Everything we are and everything we do is shaped by our environment, the people inspiring us, the people surrounding us, the people helping us, and the people supporting us.

This book is no different.

You are holding in your hands the achievement of a four-year journey. It would, however, not exist had it not been for the many people involved in the process.

First, there are those who contributed to my environment. I am grateful to my parents who made it possible for me to study what I wanted and who respected the choices I made. I am thankful to my professors for their lessons in an academic environment fostering intellectual challenge. To the Jury of the ING Thesis Award and Frederic Helsen, who confirmed the quality and uniqueness of my message.

Then there are the people who inspired me. This list would be endless, and most of the people on it are people I have never met. These are world leaders in their domains, entrepreneurs, and people who changed things; those who hold a passion or a message and do not give up.

Finally, thank you to the people surrounding me, the many colleagues across all levels at Deloitte who were positive and interested in this adventurous project, and who welcomed my different initiatives with
enthusiasm and trust. To **my friends** in Belgium and the people I met in Dublin, for being there when I needed small “escapes” from the “overloaded life.”

Thanks to:

Moe **Adham** (Co-founder, BitAccess)
Dr. Adam **Back** (Co-founder and CEO, Blockstream)
Damian **Barabonkov** (Slimcoin)
Thomas **Bertani** (CEO, Oraclize – Founder, InsurETH)
Iddo **Bentov** (Cornell University)
David **Birch** (Director of Innovation, Consult Hyperion)
Michelle **Brinich** (Head of Marketing, Blockstream)
Francisco **Cabañas** (Monero)
Luke **Dashjr** (Bitcoin Core developer)
John **Frazer** (External Relations Lead, Ethereum Foundation)
Nick **Gogerty** (Solarcoin and MIT Media Lab)
Cedric **Hauben** (Lawyer, DLA Piper)
Haitch (member of forums.burst-team.us)
Eitan **Katchka** (Founder of La’Zooz and Commuterz)
Arnaud **Kodeck** (Founder, EBTM)
Claire **LaRocca** (Everledger)
Louis **Larue** (Basic income, Catholic University of Louvain)
Christophe **Lejeune** (Catholic University of Louvain)
Christoph **Jentzsch** (CEO, Slock.it)
Daniel **Kraft** (Namecoin)
Sunny **King** (Founder, Peercoin)
Gilles **Mitteau** (Founder, YouTube Channel Heu?reka)
Bach **Nguyen** (SatoshiLabs)
Jean-Grégoire **Orban de Xivry** (Co-founder, Solarly)
David **Osojnik** (CTO, Bitstamp)
John **Quinn** (Co-founder, StorJ)
Luca **Pensieroso** (Macroeconomics, Catholic University of Louvain)
Paige **Peterson** (Zcash)
Andrew **Poelstra** (Mathematician, Blockstream)
Joseph Poon (Lightning network)
Veena Pureswaran (IBM)
Jeremy Rand (Namecoin)
Ripple
Ted Rogers (President, Xapo)
Pavol Rusnak (SatoshiLabs)
Fabian Schuh (BitShares)
Matthew Spoke (Co-founder and CEO, Nuco)
David Schwartz (Member of bitcoin.stackexchange.com)
Martin Swende (Ethereum Developer)
Alan Szepieniec (Cryptographer, KU Leuven)
Ryan Taylor (CEO, Dash)
Susanne Tarkowski Tempelhof (Founder, Bitnation)
Stephan Tual (COO, Slock.it)
Roger van de Berg (Lawyer, Baker & McKenzie)
Patrick van der Meijde (Founder, BitKassa)
James Walpole (BitPay)
Tyler Welmans (Deloitte Digital)
Bas Wisselink (Nxt Foundation)
Lon Wong (President, NEM.io Foundation Ltd)
Vasja Zupan (COO, Bitstamp)

For their help, insights, content review, and feedback to this book.

Special thanks to Mallory Miles and Vidya Vijayan, for helping in the editing process and answering my endless requests. Your feedback and work have truly made a difference and contributed immensely to the quality of this book. Thanks to the teachers of universities who trusted me to be a guest lecturer and to Deloitte for bringing me to the executive boards.

To my dear friends: Gerard Salvador for his continuous and extreme enthusiasm: every author needs someone like you around. To Jérémie Denis, for his feedback, ideas, positivity, and the time he invested voluntarily. To Quentin Nederlandt for his feedback.
Thanks to Kim Bracke and Lieven Verbrugge for their personal time investments in creating the first YouTube video.

On an almost final note, I would like to thank many people in the Bitcoin and blockchain community who helped me in the writing of my thesis during 2013–2014. The developers of the community who make things real as well as the connectors for connecting, opening doors, and giving me opportunities. To all the people who believed I was not crazy after receiving my speeches and who welcomed my opinions with great enthusiasm and challenge.

A huge thank you to all those who like, follow, share, and subscribe to my social media pages for spreading the message! Your impact is much larger and more valuable than you would expect. I will be extremely grateful if you post a picture of this book and let me know what you think!

Finally, I would like to thank you as a reader for believing this work is worth your time. I am grateful and humbled by your attention, and I hope this book will meet your expectations.
Notes

1. Original title in Dutch: “Innovatie en disruptie in het economisch recht”
2. The paper was shared via the Cryptography Mailing List and can be viewed at: http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html
6. A function is a programmed procedure that performs the same algorithm every time it is called. It can receive information to treat as input and returns a value as output.
7. This is called a collision in cryptography. All functions in cryptography can have collision; the art of a strong hashing function resides in the enormous number of guesses one must make before finding a collision, and thus this unlikelihood of finding a collision.
8. Open source means that the code is publicly available and can be reviewed by anyone. It is 100% transparent.
10. A bit is a zero or one in computing language. Together, 256 bits offer $2^{256}$ (roughly 1 followed by 77 zeros) possible combinations.
11. Addresses are inspired from https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses (consulted July 10, 2016) where you can also find further information on the used functions.
12. In fact, there will be a signature for every transaction input. More on transaction inputs in Chapter 6.
13. Going short in finance consists of betting that the price of something will go down
14. July 2017
15. GHash.IO, Bitcoin mining pool GHash.IO is preventing accumulation of 51% of all hashing power https://ghash.io/ghashio_press_release.pdf
20. Further reading on Lamport Signatures: https://gist.github.com/karlgluck/8412807
22. Alan Szepieniec (PhD Researcher in Cryptography at the KU Leuven), July 2016
23. Alan Szepieniec (PhD Researcher in Cryptography at the KU Leuven), July 2016
24. Pieter Wuille at the Scaling Blockchain conference in Hong Kong, December 7, 2015 - https://www.youtube.com/watch?v=zchzn7aPQjI
25. Off-chain bitcoin payments are bitcoin payments that happen on alternative platforms and require only a limited number of re-transactions in the Bitcoin Blockchain.
26. Technically speaking, Johanna is rewriting a transaction waiting for John's signature to be broadcasted. The new transaction uses the same input but sends a higher amount to John. The transaction will be broadcasted once the channel is closed.
27. The complete white paper can be found at: https://blockstream.com/sidechains.pdf
30. Routing tables facilitate communication on networks. In this case, they would keep track of the different existing channels and how to transfer cryptocurrencies across channels.
33. https://blockchain.info/charts/hash-rate
36. August 15, 2017
37. April 2017
38. http://www3.weforum.org/docs/WEF_Internet_for_All_Framework_Accelerating_Internet_Access_Adoption_report_2016.pdf, consulted August 16, 2017
42. https://blockstream.com/satellite/blockstream-satellite, consulted August 16, 2017
43. https://en.bitcoin.it/wiki/Thin_Client_Security
44. The initial chaincode at the master level is an input generated from random data. As from the next level, the chaincode is generated from a function hashing the parent key, the previous chaincode, and the index of the child key.
45. Mastering Bitcoin, Andreas
46. Coin Desk, how to store your Bitcoin – consulted June 1, 2016 - http://www.coindesk.com/information/how-to-store-your-bitcoins/
47. Coin-mixing is a method of mixing Bitcoin transactions in order to make them less traceable. A mixing service receives different transactions from different users (the initial owners), then sends the funds of these transactions to multiple addresses before sending them back to an address controlled by the initial owner. The multitude of transactions splitting and merging bitcoins recorded on the Bitcoin Blockchain is supposed to increase the difficulty in retracing transactions.
48. Near-field communication (NFC) is a technology allowing devices to communicate in a contactless way.
49. Blockchain is the technology behind Bitcoin but there is also a wallet company based in Luxembourg, called Blockchain, which operates the website Blockchain.info. In this case, we are referring to the wallet provider.
50. “A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a
large number of consecutive guesses as to the value of the desired data.”
- https://www.techopedia.com/definition/18091/brute-force-attack
51. You can generate a paper wallet online at https://bitcoinpaperwallet.com/
52. Some offline generators can be downloaded at https://github.com/cantonbecker/bitcoinpaperwallet
54. https://ihb.io/paper-wallet
55. In this case, we use the term digital currencies instead of cryptocurrencies because a few currencies are not backed by a distributed ledger or by cryptography and, as a consequence, do not fall under the denomination of cryptocurrencies.
61. http://in.reuters.com/article/china-bitcoin-idINL3N0JX2FH20131218
62. Automated teller machines
63. Phone Interview, Jean-Wallemacq, Belgian Bitcoin Foundation
64. Phone Interview, Moe Adham, BitAccess
65. Phone Interview, Moe Adham, BitAccess
67. Phone interview with Arnaud Kodeck, EBTM
68. Phone interview with Arnaud Kodeck, EBTM
69. Phone Interview, Moe Adham, BitAccess
75. “Exchange risk exists (...) when a financial transaction is denominated in a currency other than that of the base currency of the company. (...) The risk is that there may be an adverse movement in the exchange rate of the denomination currency in relation to the base currency before the date when the transaction is completed.” Wikipedia, consulted August 14, 2016.
76. Skype interview with Patrick van der Meijde, December 2016
78. Skype interview with James Walpole, BitPay. January 6, 2017
79. Skype interview with James Walpole, BitPay. January 6, 2017
80. Skype interview with James Walpole, BitPay. January 6, 2017
81. Email exchange with James Walpole, BitPay. January 17, 2017
82. Skype interview with James Walpole, BitPay. January 6, 2017
83. Smallest storage unit on a computer, represented by 0 or 1
93. The European troika is a decision group formed by the European Commission (EC), the European Central Bank (ECB) and the International Monetary Fund (IMF).
96. Author’s experience in the Philippines
97. In Keyna, more than 45% of money transaction are done through M-Pesa (a cellphone-based money transfer service) while 30% are done by hand.
98. Messenger call, Jean-Gregoire Orban de Xivry
100. Unlike standard formatting, zero-fill formatting overwrites every bit on a hard drive to zero. It is estimated that a hard drive has to undergo three cycles of zero-fill formatting to make it impossible to recover any data.
105. Thousand millions of millions in the American system.
108. Author’s personal experience in India
119. Verhelst J., The Bitcoin e-currency: historical genesis, current situation and empirical analysis compared to traditional currencies and commodities
120. https://www.cryptocoinsnews.com/ghostsec-isis-bitcoin-wallet-worth-3-million/
125. https://www.ft.com/content/c5do8c5c-339c-11e6-bdao-04585c31b153
127. Recent events include the transatlantic trading agreement. On the other hand, the Ukrainian conflict tends to reinforce old trading barriers.
128. For example, credit cards offer not only a faster payment method but also extra protections to their users at the cost of higher transaction fees.
130. https://www.youtube.com/watch?v=GplUE1NGqgA
132. The blockchain is one of the more secure and world’s more widespread database. Some people use the blockchain to store valuable information (i.e., Dutch notaries for storing the hashtag of documents). Source : Spaes T., De pro’s en contra’s van de Bitcoin, http://deredactie.be/cm/vrtnieuws/videozone/programmas/devrijemartk/2.31526?video=1.1838058 – consulted April 6, 2014
134. http://www.youtube.com/watch?v=mpE8UMMZa9w
135. https://letstalkpayments.com/which-countries-are-close-to-a-cashless-world/
NOTES

146. This has been the case in the Netherlands, from where Bitcoin start-ups are interested to operate but the national bank has warned companies not to work with Bitcoin start-ups. Source: Skype interview with Van de Berg R. *Tax Lawyer at Baker & McKenzie Amsterdam N.V.* (2014) following publication "Fiscaal beleid overheid rond bitcoin remt innovatie", Dutch Financial Times, June 17, 2014.
147. https://www.asfi.gob.bo/images/ASFI/DOCS/SALA_DE_PRENSA/Notas_de_prensa/2017/N_20_Nota_Prohibici%C3%B3n_de_uso_y_circulaci%C3%B3n_de_monedas_virtuales.pdf
149. Perkins Coie report, *Virtual Currencies: International Actions and Regulations*
153. Perkins Coie report, *Virtual Currencies: International Actions and Regulations*
161. Roger Van de Berg, email exchange July 2017
166. IRS Notice 2014-21
169. Van de Berg et al., Decision on Landmark Case Regarding the VAT Treatment of Bitcoin, Bloomberg BNA - Tax Planning International (Indirect Taxes) - Volume 13
176. Assuming no legal measures decide to ban the Internet.
178. https://www.youtube.com/watch?v=fE_OWNEbH_k
179. August 15, 2017
180. Coinmarketcap.com, consulted August 15, 2017
181. The “pump and dump” of altcoins is similar to the pump and dump of penny stocks; both having relatively small market capitalization. You can buy a lot of coins at a cheap price, and then create a buzz about the coin to attract other investors willing to buy the coin. As more and more
investors buy in, the price increases (pump). While the price increases, the initial buyer starts selling his coins (dump). Ultimately, people realize that there was a lot of buzz about nothing, and the price decreases.

182. January 2017
184. https://chainz.cryptoid.info/slr/
185. The full list of metadata posted in the transaction can be consulted at https://solarcoin.org/en/viewing-transactions-on-the-solarcoin-blockchain/
186. Facetime interview with Jean-Gregoire Orban de Xivry, Early adopter of Solarcoin and Founder of Solarly, a start-up bringing solar energy to African villages.
187. Email exchange Ryan Taylor, February 28, 2017
188. Email exchange Ryan Taylor, March 5, 2017
189. https://www.dash.org/team/
190. Email exchange with Bas Wisselink, Nxt Foundation, February 27 2017
191. Francisco Cabanas, Monero, Email exchange March 14, 2017
194. Ripple.com December 29, 2016
198. Email exchange with Daniel Kraft, February 27, 2017.
199. https://nameid.org/?
201. Remember, the coinbase transaction is the transaction in which the miner allocates newly generated bitcoins to himself.
202. Or another cryptocurrency backed by many times more computing power.
205. This example is inspired from Peercoin
209. Email exchange with Nick Gogerty, Founder of Solarcoin
White paper can be found at https://eprint.iacr.org/2014/452.pdf
214. Iddo Bentov (Cornell University)
217. Email exchange with Nick Gogerty, May 12, 2017
218. This was the case for Chancecoin, one of the first altcoins to experiment with burning.
219. This assumes that the mechanism to go from private key to address is the same on both chains.
221. https://techcrunch.com/2015/06/29/everledger/
222. https://blog.oraclize.it/understanding-oracles-99055c9c9f7b, consulted April 16, 2017
223. Martin Swende, peer-review, May 2017
227. www.lazooz.org
233. https://www.youtube.com/watch?v=LVlT4sX6uVs
234. See https://t.co/mAMFrXCTiX for more technical details
235. Find demo at https://youtu.be/U1XOPlqyP7A
236. https://www.youtube.com/watch?v=49wHQoJxYPo
237. See Blockcharge
238. Find demo at https://youtu.be/U1XOPlqyP7A
239. https://www.youtube.com/watch?v=qlBQfv85g6I
244. https://www.youtube.com/watch?v=9PaHinkJlvA
248. Tyler Welmans, Blockchain and Digital Identity specialist Deloitte, Email exchange May 2017
249. https://www.youtube.com/watch?v=zpO7eH5FYdo
252. https://www.youtube.com/watch?v=loQchIoA-k
253. https://www.youtube.com/watch?v=hs15p5V3slg
257. https://medium.com/basic-income/why-milton-friedman-supported-a-guaranteed-income-5-reasons-da6e628f6070#.modlnxi4s
258. https://www.weforum.org/agenda/2017/01/why-we-should-all-have-a-basic-income?
259. https://www.youtube.com/watch?v=_wYywEW9aTY
261. https://www.youtube.com/watch?v=_wYywEW9aTY
264. https://www.youtube.com/watch?v=PJy8vTu66tE
268. http://www.independent.co.uk/voices/facebook-fake-news-fact-check-google-ad-save-journalism-a7645706.html
271. https://www.youtube.com/watch?v=UajbQTHnTfM
274. https://www.youtube.com/watch?v=M4Dg3mo3cAc Susanne Tarkowski Tempelhof
276. https://www.youtube.com/watch?v=fEfgCdy1mwE
In this book, you will learn:

- What is Bitcoin and what is blockchain
- How it works, step-by-step
- Why it is important
- What is “mining”
- The security threats that plague it
- The challenges it faces
- The solutions to these challenges
- How to acquire bitcoins
- How to store your bitcoins safely
- Four characteristics and six types of wallets, their advantages, and disadvantages
- How and where to spend your bitcoins
- The ecosystem landscape
- If Bitcoin is, or can become, money or currency
- Political, economic, and social implications
- Regulations
- Other cryptocurrencies
- Different consensus mechanisms
- What are smart-contracts, Dapps, and DAOs
- Concrete examples of blockchain applications
- What it means for business and financial audits
- What it means for identity, basic income and democracies
- The promises of blockchain
- The pitfalls of blockchain