Risks, Frauds, Cyberattacks, and Resilience of P2P systems

Summer 2017

Table of contents

List of Figures

List of Abbreviations

b2b: business to business

IP: Internet Protocol

p2p: peer to peer

qubits: Quantum Bits per Second

1. Abstract

Many start-ups want to simplify global payment transactions, store customer data based on counterfeit-proof security, or even carry out entire business processes in so-called smart contracts by computers instead of people. In the implementation, all rely on the same foundation: peer to peer (p2p) networks with blockchain technology. However, as numbers of users increases, an increasing incentive for fraud and cyber-attacks is emerging.

We will discuss risks, frauds, cyber-attacks, and resilience of p2p systems, their reliability and crowd based security implementations, furthermore how society handles them.

2. General underinvestment in IT technology

Users cannot evaluate the difference between secure and unsecured systems, a constant problem with modern IT systems. Developers have no incentive on building secure systems, rather deliver rapidly presentable products. The absence of investment in security implementations leads to weaknesses by design of many applications.[1]

3. The structure of peer to peer systems

Central server networks connect a client, e.g. smartphone or computer, to one dedicated server. The server controls the level of access granted to the client and provides the requested data. (Figure 1)

Peer to peer networks are decentralized networks, without a client to server connection, rather connect single nodes to other nodes directly. (Figure 2) Each node of the network keeps a list of IP addresses of other nodes within the network.

Through nodes, self-organization and symmetric communication, as well as control rights instructions, are distributed throughout the network.

Figure 1: Schematics of client to server networks

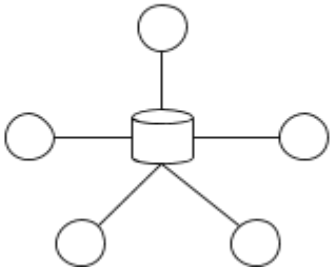
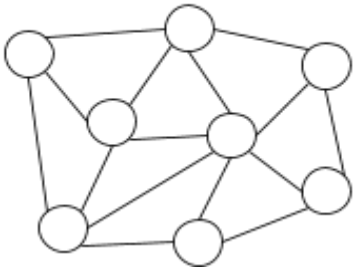


Figure 2: Schematics of peer to peer networks



[1] Simon (2017)

4. Benefits of peer to peer systems

Truly beneficial aspects of a p2p network are flexible storage through the network and no data restrictions.[2] Each file is distributed throughout many peers and thereby mirrored in the network. The performance and speed capability increases correlated to the nodes participating.[3] Historically early p2p networks were designed to encounter censorship with broad sharing of files between clients, to ensure a free speech.[4]

Today p2p networks are a base layer technology in various applications as file sharing, streaming, video communication and cryptocurrencies.

// Self organization of Node connectivity. The creation of artificial intelligence.

To be able to achieve a truly self deploying network, it has to be ensured that node connectivity can ameliorate itself. To able to do so, we are using the so called brownian motion of modelling randomness.

a) The process of Brownian motion modelling in a cell.

b) Adaption and implementation of brownian motion in a node for DHCP purposes.

c) Usage of the brownian motion for evaluation of network connectivity.

d) Single networks within GPU Units of a Node (Plasticity)

→ Brownian Motion on each node with personal “nodebook/DNA” results.

The usage of Technology which is already available and combining them.

[2] Moore & Ross (2006)

[3] Li (2007)

[4] Moore & Ross (2006)

5.Online transaction system.

a) Payment method.
b) Direct Ticket System
c) Derivative SMC Clearing

6. An introduction to blockchain and cryptocurrencies.

Modern cryptocurrencies are based on the blockchain technology. A blockchain is a public ledger of transaction data recorded and stored in chronologically- and linearly-connected blocks within a p2p network.[5]

Each blockchain participant has one pair of alphanumerical keys. A public key, a unique account number within the blockchain and often recognized as wallet-address and a private key used to legitimate outgoing transactions. Each transaction attempting to change the public ledger is published and checked for validation through miners, network nodes with high computational power. Cryptocurrencies use the blockchain technology to keep track of 'ownership' of value, in this case: Coins. Coins are generated as the reward for miners for using their computational power to calculate a validation for a transaction. Once processed it becomes a new block on the chain.[6] This mechanism is used to prevent double spending within the network.[7]

The blockchain has been regarded as one of the most important disruptive computing paradigms after the Internet.[8]

[5] Crosby, Nachiappan, Pattanayak, Verma & Kalyanaraman (2016)
[6] Swan (2015)
[7] Bitcoin-Wiki (2017)
[8] Crosby, Nachiappan, Pattanayak, Verma & Kalyanaraman (2016)

5.1 Risks associated the blockchain technology itself

Security of the blockchain comes through hard solvable mathematical formulas combined with cryptography. Nowadays no single supercomputer has enough computing capacity to recalculate private keys through brute force attacks, with the rapid development of quantum computers in a remote future, the keys may be easy enough to recalculate in a reasonable time, which could elaborate in a collapse of the blockchain system.[9]

Current innovation by Google's D-Wave quantum computer has already a combined power of 8 qubits, while 256 qubits are being necessary to be able to recalculate the algorithm.[10]

5.2 Blockchain manipulation democracy

Transactions are only executed on the blockchain if the seller can prove that he has previously been acquired these assets. The blockchain functions on a majority principle. 51% of the computing power of all nodes in the p2p network must confirm that these assets were previously transferred to the current vendor. If a single party dominates most of the computing power on the network, it could transfer any assets to itself without even obtaining them before. Nowadays, no supercomputer is strong enough for providing 51% or more of the computing power in the current networks;

as stated in 5.1 already, this may change with the rapid development of quantum computers in a remote future.

6. Virtual risks with cryptocurrencies on the blockchain

Since values of cryptocurrencies are rising[11] with a market value of currently 25 Billion USD, hackers and criminals try to attack users and try stealing virtual information and value.[12]

6.1 Non-traceability

Blockchains preserve anonymity and privacy, once a transaction is carried out, it cannot be reversed.[13] Anyone in the knowledge of a set of private and public keys is eligible to sign a transaction, once a private key is found or stolen by a third party, it is nearly impossible to

[9] Crosby, Nachiappan, Pattanayak, Verma & Kalyanaraman (2016)
[10] Bergmann (2015)
[11] The Economist (2017)
[12] Hileman & Rauchs (2017)
[13] Nakamoto (2008)

identify the thief. [14] The network itself cannot check if the key was used legitimate or by another party.[15] Therefore, it is often a goal of criminals to get into the possession of the private key or to get money transferred through fraud schemes, since it can not be traced back.

6.1.1 Knowledge gain via sniffing tools

Sniffing tools search infected computers for valuable data like identities, private keys or access information to bank accounts. Programs are recording screen images and key-logging every input of the user while sending all the data to the attacker.

Malware is distributed via mail and installed on target computers through known security exploits, where update patches are already available. Users tend to not install updates for security exploits right away, leaving a backdoor open for harmful programs.[16]

Some of these programs even encrypt the system, while cryptocurrency is asked in return for a key necessary for decryption.[17]

6.1.2 Fraudulent salesman

Fraudulent salesman on marketplaces take advantage of anonymity and insufficient traceability for scamming users. Criminals offer goods at an unbeatable cheap price, once purchased by customers and paid with cryptocurrency, the criminal takes benefit of the money and the non-traceability of him, but will not fulfill his counterpart to ship any goods.

6.2 Third party intermediates

Cryptocurrencies were designed to eliminate 3rd party intermediates originally, since the cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions.[18] Elimination is successful on the blockchain but also established new 3rd party intermediates as a mediator offering exchange between real and cryptocurrency while taking fees.

---

[14] Xu (2016); Peteanu (2014)
[15] Reid & Harrigan (2012)
[16] Moeller (2012)
[17] Gazet (2008)
[18] Nakamoto (2008)

6.2.1 Fraud and cyber-attack problematics

Trade platforms and stock exchanges or intermediates are normally not part of a p2p network, therefore interaction with these centralized authorities involves high risk. To be eligible to trade on the platform, 73% percent of cryptocurrency stock exchanges require private keys deposited of user cryptocurrencies as a collateral.[19] A central authority controlling multiple keys is an incentive for criminals and fraudsters as to attack these, or even participate there as fraudulent operators.[20]

6.2.2 Missing trust leads to volatility problematics and fees

The high volatility of cryptocurrencies makes it a problem for companies to accept and trust cryptocurrencies directly as a payment method, since they need real currency to pay their liabilities, e.g. employees paychecks.

Mediate companies like 'Coinbase' or 'BitPay' convert customer's cryptocurrencies, immediately into a pre-set cash amount, which then is directly deposited in a company's bank account. The usage of 3rd party intermediates for transaction adds high payment fees, therefore users might not have the incentive to pay with cryptocurrencies, leading to lower trust in the currency again. [21]

6.2.3 Time lag and exchange volatility risk

Exchanges of cryptocurrency, e.g. bitcoin, can take five to ten days; price changes between settlement and execution due to delays in transactions are high, creating a high counterparty risk while sending the exchange order.[22]

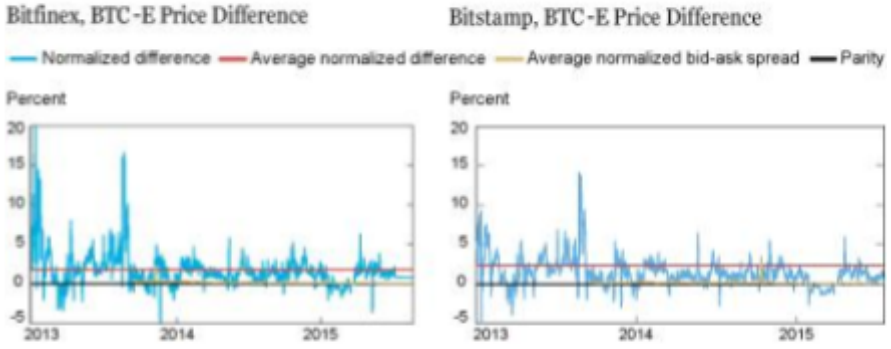
The large exchange rate volatility compared to traditional currency creates more problems. Not only while processing payment transactions, but using cryptocurrencies as a store of value seems irrational.[23]

Figure 3 shows that the three main exchanges differ up to 20% in exchange rates.

---

[19] Hileman & Rauchs (2017)
[20] Xu (2016)
[21] Davidson (2014)
[22] Kroege (2017)
[23] Kroege (2017)

Figure 3: Large and persistent Bitcoin price differences across Exchanges



Source: bitcoincharts.com; bitcoinity.org; authors' calculations.

Notes: We calculate normalized difference as the price difference between BTC-E and Bitfinex or Bitstamp, respectively, expressed as a percent of the BTC-E price (for example, (Bitfinex-BTC-E)/(BTC-E)). Differences above 20 percent and under -5 percent are truncated on the chart for readability.

Exchange failure also is not merely a theoretical possibility in cryptocurrencies markets - it occurs regularly. A study of Taylor Moore reported that eighteen of the forty bitcoin exchanges analyzed - almost half - ultimately failed. This is due to successful attacks of hackers and operators taking advantage of deposited keys. The median lifetime of exchange today is only 381 days with and has only a 45% survival rate.[24]

6.3 Liquidity trap

Transaction security is ensured by the fact that the blockchain technology verifies data with so called: 'Miners', which solve heavy mathematical formulas with high-performance computers. These miners are remunerated by automatic issuance of newly created cryptocurrency. However, the degree of difficulty of these mathematical solutions increases constantly, while the remuneration decreases for the mining process. If the payment for mining would be lower than the costs of mining, no one would verify these transaction data, a freezing of the liquidity would occur and the value of the currency would drop to zero. In the future, the prices of already established cryptocurrencies should rise even faster or nobody is willing to provide the needed computing power.[25]

[24] Moore & Christin (2013)
[25] Draupnir (2017)

7. Physical risks with cryptocurrencies on the blockchain

High-risk potential has the physical component within a p2p network, e.g. hardware failures and storage difficulty.[26]

7.1 Hardware failure

Data loss due to hard disk failure is a risk that computer systems of each kind generally have. In normal systems, a data reliability is created by redundancy, which means storing data at as many locations as possible. Private keys need to be stored safely, every redundancy of the key creates security in case of hard drive default, but also lays the foundation to another possible attack point for criminals.[27]

7.2 Offline Storage

Savings can be stored in offline wallets, called a 'cold storage'. Classical cold storage methods are to write down keys on a piece of paper or any other offline visualization, but even these can be destroyed. e.g. fire. [28]

By design, the blockchain system has no recovery option to restore forgotten keys. Finding a safe way for storage is difficult and involves high risk. Once lost, access to each wallet is ultimately gone.

7.3 Externality: Environmental impact

Each computer in a p2p network needs electricity to run. The energy needed for the validation and mining only of the 'bitcoin' network today has the same the consumption as 1.250.000 U.S. households. [29] Validation will always take place in regions with the cheapest supply of energy, which today is still mainly coal and nuclear power, counteracting climate change goals to reduce CO2 emissions.[30]

---

[26] Swan (2015)
[27] Reid & Harrigan (2012)
[28] Swan (2015)
[29] Zohair (2017)
[30] Quiggin (2015)

7.4 Regulation upcoming problems

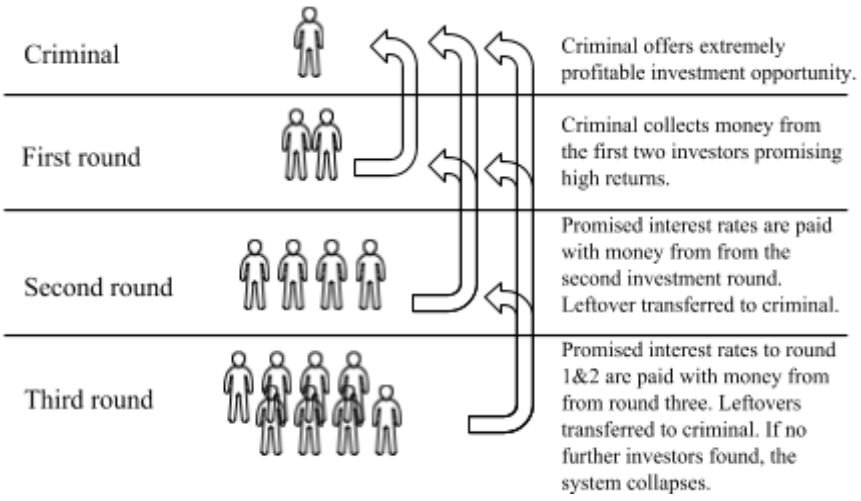
Cryptocurrencies are not regulated by any government authority so far. In short future, this can change and beares risk.

The Parliament and the Central Bank of Russia, for example, announced after the May 25th 2017 parliament meeting that the first set of regulations for bitcoin will be handed over to the lower house of the Federal Assembly of Russia in July 2017. This is the reaction to a rising popularity of cryptocurrency in Russian Federation. Russia plans to monitor all transaction to shorten over-the-counter markets and implement a taxation of hashed coins. The results for the current cryptocurrency ecosystem is difficult to predict.[31]

8. Fraud with cryptocurrency Ponzi scheme

Criminals advertise a Cryptocurrencies as an investment opportunity in online forums. Investors are promised up to 7% interest per week through Bitcoin arbitrage activities with special algorithms to generate the returns. Instead, invested deposited funds were allegedly used to pay existing investors and exchanged into U.S. dollars to pay the organizer's personal expenses (Figure 4). Once no new investors can be found, the system collapses, leaving investors with default.[32]

Figure 4: Schematics of Ponzi-Scheme



[31] Young (2017)
[32] SEC Investors Information (2017)

9. Outlook and Resilience: The Ethereum blockchain app platform

By market value, bitcoin is currently the leading cryptocurrency in the world. With the white paper of Nakamoto in 2008, the technology foundation for today's cryptocurrencies was laid. Over the last few years, this has been constantly developed. A large part of the risks of today's cryptocurrencies comes from third parties as already described above.

In close future, a couple of new blockchain innovations can lead to the total replacement of these third parties. We see Ethereum as the future platform of decentralized payment systems.[33]

The project is founded by Vitalik Buterin in 2014 and seek to build a blockchain application platform. Bitcoin and current cryptocurrencies are focused on money transfer, whereas Ethereum builds a private platform to build decentralized applications and smart contracts running autonomously.

“Smart Contracts are applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.”[34]

[33] Hileman & Rauchs (2017)
[34] Ethereum (2017)

Bibliography

Babaioff, M., Dobzinski, S., Oren, S., and Zohar, A. (2011): ‘On bitcoin and red balloons‘,http://research.microsoft.com/apps/pubs/?id=156072q.https://docs.google.com/document/d/1lPjn9KL3iihd3hOQP1oNkw8Op4QYphlLNFWmmBgotQo/edit#, accessed 15.06.2017.

Bergmann, Christoph (2015): ‘Ist Googles Quantencomputer eine Gefahr für den Bitcoin?‘,https://bitcoinblog.de/2015/12/17/ist-googles-quantencomputer-eine-gefahr-fuer-den-bitcoin/, accessed 20.06.2017.

Camp, L. Jean and Stephen Lewis (2004) ‘*Economics of Information Security (Advances in Information Security)‘,* Kluwer Academics Publisher.

Crosby, M., Nachiappan, N., Pattanayak P., Verma S. and V. Kalyanaraman (2016) ‘Blockchain technology: Beyond bitcoin‘. Applied Innovation Review: 6–19.

Davidson, Jacob (2015): ‘Bitcoin Not Really Being Accepted by Major Companies‘, *Time*.

Draupnir, Melvin (2017): ‘Will 2017 Be Profitable for Bitcoin Mining?" Everything You Need to Know about Bitcoin Mining. ‘https://www.bitcoinmining.com/is-bitcoin-mining-profitable-in-2017/, accessed 19.06.2017.

Ethereum (2017): ‘Ethereum - Homestead Release‘, https://www.ethereum.org/, accessed 19.06.2017.

Gazet, Alexandre (2008) ‘Comparative Analysis of Various Ransomware Virii‘, *Computer Virology 6.1:* 77-90.

Hileman, Garrick and Rauchs, Michel (2017) ‘2017 Global Cryptocurrency Benchmarking Study‘, *SSRN Electronic Journal*.

King, Sunny and Scott Nadal (2012): ‘PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake‘, http://peerco.in/assets/paper/peercoin-paper.pdf, accessed 16.06.2017.

Kroeger, Alexander and Asani Sarkar (2017) ‘Is Bitcoin Really Frictionless?‘, *Liberty Street Economics*.

Kroeger, Alexander (2017) ‘Why Bitcoin Exchanges Aren't as Straightforward as They Seem‘, *World Economic Forum*.

Laurie B. (2011): ‘Decentralised currencies are probably impossible (but let’s at least make them efficient)‘, http://www.links.org/files/decentralised-currencies.pdf, downloaded on 18.06.2017.

Moeller, Andreas (2012) ‘Update Behavior in App Markets and Security Implications: A Case Study in Google Play‘, https://www.researchgate.net/publication/235642535_Update_Behavior_in_App_Markets_an

d_Security_Implications_A_Case_Study_in_Google_Play, accessed 18.06.2017.

Moore, Tyler and Christin, Nicolas (2013) 'Beware the middleman: Empirical analysis of Bitcoin-exchange risk', *Financial Cryptography and Data Security* in Computer Science, vol. 7859. Springer: Berlin, Heidelberg.

Moore, Tyler and Anderson, Ross (2006) : *The Economics of Information Security*, published in Sciencemag 314 (E-Paper) p. 610-613, http://science.sciencemag.org/content/314/5799/610, accessed 18.06.2017

Nakamoto, Satoshi. (2008): 'Bitcoin: A peer-to-peer electronic cash system', http://bitcoin.org/bitcoin.pdf, downloaded on 19.06.2017.

Quiggin, John (2015) 'Bitcoins Are a Waste of Energy - Literally', *ABC News.* N.p., 05.10.2015.

Reid, Fergal and Martin Harrigan (2012) 'An Analysis of Anonymity in the Bitcoin System.' *Security and Privacy in Social Networks*, 197-223.

SEC The Office of Investor Education and Advocacy (2017): 'Investor Alert Ponzi schemes Using virtual Currencies', https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf, accessed 19.06.2017.

Secure Works (2017): 'Enterprise Best Practices for Crypto-currency Adoption', https://www.secureworks.com/resources/wp-cryptocurrency-adoption-best-practices, accessed 19.06.2017.

Simon, N. (2017): 'The Dangers of P2P Networks', http://www.computerweekly.com/feature/The-dangers-of-P2P-networks, accessed 19.06. 2017.

Swan, Melanie (2015) '*Blockchain: Blueprint for a New Economy*', Beijing, O'Reilly.

The Economist (2017): 'A Surge in the Value of Crypto-currencies Provokes Alarm', http://www.economist.com/news/finance-and-economics/21722235-bitcoin-far-only-game-town-surge-value-crypto-currencies, accessed 19.06.2017.

Tolentino, Mellisa (2014): 'Ask Dr. Bitcoin: Summer Is Here; How Do I Keep My Mining Rigs Cool?', https://siliconangle.com/blog/2014/05/02/dr-bitcoin-mining-rig-heat-management/, accessed 24.06.2017.

Peteanu, Razvan (2014): 'Fraud Detection in the World of Bitcoin', https://bitcoinmagazine.com/articles/fraud-detection-world-bitcoin-1395827419/., accessed

19.06.2017.

Wieczner, Jen (2017): ‘Bitcoin and Ethereum Just Crashed, Taking Coinbase Down With Them‘, http://ethereum-kaufen.de/ethereum-zukunft-der-ethereum-fahrplan/, accessed 18.06.2017.

Xu, Jennifer J. (2016) ‘Are Blockchains Immune to All Malicious Attacks?‘, *Financial Innovation* 2.1.

Young, Joseph (2017) ‘Russian Central Bank Plans to Legalize & Tax Bitcoin as Digital Commodity |Bitconnect.‘, Bitconnect. online publication 31.05.2017.

Zohair (2017): ‘How Much Energy Does Bitcoin Use? A Lot It Turns Out.‘, https://securitygladiators.com/2017/03/15/bitcoin-uses-energy-a-lot/, accessed 24.06.2017.