SURVEY ON BLOCKCHAIN: A COMPLETE TECHNOLOGIES COMPARISON

Tewfiq El-Maliki¹, Noria Foukia¹ and Oumayma Zelfani²

¹*University of applied Sciences of Geneva HES-SO, Switzerland*

²*SupCom, Tunis*

ABSTRACT

Blockchain is actually a decentralized database without any third party -controller- and could be the ground necessary to guarantee that any committed transaction is strong enough to meet basic expectations such as security and privacy requirements. This is where the blockchain technology comes handy. It is fundamentally a public distributed ledger of all transactions, has the ability to increase secure data exchange and to make that data transfer simpler and easier between entities. Therefore, the need of blockchain would be extensive in the near future.

In this paper, we firstly provide an overview of blockchain with emphasis on most famous blockchain technologies. Secondly, we will focus on evaluating them related to fundamental security requirements and different criteria. At the end, we conclude our comparison.

KEYWORDS

Blockchain, Crypto-money, Bitcoin, Security

1. INTRODUCTION

Until recently, any currency transaction needed a centralized authority to check the information consistency and validity within the transaction. Thanks to blockchain highlighted by bitcoin, we have a P2P direct transaction without any need to third party controller. Indeed, bitcoin was proposed in a white paper in 2008 and implemented in 2009 (Nakamoto, 2008). Unfortunately, this association still mislead people in seeing the benefit of blockchain. Indeed, they thought that blockchain is just bitcoin,

Definitely, blockchain could be used for wide range applications, such as smart contracts (Kosba et al., 2016), public services (Akins et al., 2013), internet of things (IoT) (Panarello et al, 2018) and reputation systems (Sharples et al, 2015).

There are a lot of literature on the blockchain. We focus on a comparison of main blockchains implementation under fundamental requirements. Thereby, any decision maker could have an exact opinion in choosing efficiently the most adapted blockchain to his needs. We have structured our paper in 5 sections. Section 2 introduces blockchain principles, components and functionalities. Section 3 describes and explains blockchain technologies. Section 4 summarizes different blockchains comparisons under fundamental requirements. Section 5 concludes our paper.

2. BLOCKCHAIN DESCRIPTION

A blockchain is essentially a distributed record database or public ledger of all transactions. Each transaction in the public ledger is verified based on Proof-of-Work mechanism and is accepted using the participant consensus in the system. In addition, once entered, information can never be erased (Müller et al., 2016).

2.1 The Difference between Blockchain and Centralized Database

In traditional databases, the control remains with a central authority, which defines the access permissions for users. Centralized storage typically employs higher-quality components and redundancy, which makes it more reliable than local storage. In addition, it provides comprehensive data access; but when a centralized system fails, database is unavailable to all users.

The disadvantages are especially high communication costs, a very low reliability and availability. Indeed, any error that blocks access to the database break all activity on the network (Murphy S., 2016).

Therefore, we have two interesting phenomena: the users have to trust the database controllers, which protect their data. In addition, the controllers themselves have to spend a lot of time and money developing systems that all do pretty much the same thing.

This is where the blockchain technology comes handy. It has the potential to revolutionize the digital world by enabling a distributed consensus. Thereby, each online transaction, past and present, involving digital assets can be verified at any time in the future (Müller et al., 2016).

2.2 The Concept of Blockchain

This section gives a technical overview of blockchain. The original blockchain is open-source technology, which offers an alternative to the traditional intermediary for data transfers.

Figure 1. A simplified blockchain representation

Figure 2. A complete blockchain process of transaction validation

The data in the blockchain (transactions) is divided into blocks as exposed in figure 1. A block is containing the hash of the last block to form a chain and at least one transaction. Thereafter, a mechanism allowing proof of work PoW is added to validate the block (e. g., including a random number within their block called a nonce to reach a target hash – hash starting with a fix number of zeros-). Each block depends on the previous one. Nodes are devices that are distributed across network to carry out many tasks. The system in which a blockchain serves as the database contains these nodes among them we find workers. They are responsible for appending new blocks to the blockchain based on PoW. A new block can only be added after it is validated. The system reach a consensus when all agree that this block is legitimate one and contains only valid transactions (Müller et al., 2016). The principal blockchain components are:

- Messages: a message is a submission of data (typically a transaction) for processing by nodes (participants' computers).
- Blocks: a message or messages relating to a transaction (or a status change) are bundled together by the software in a software-generated container known as a block and given a title known as a block header.

- Time stamp: a number representing a point in time at which the list of contents (for example messages) within a block header was created.
- Hashing: software causes the block header to be “hashed”. Hashing is the process that groups data and converted into a single size data, called a hash.
- Chaining: the block header for a new block contains a reference to the hash for the previous block in the chain.
- Consensus: a computer protocol in the form of an algorithm constituting a set of rules. It indicates how each participant in a blockchain should process “messages” –transactions- and how those participants should accept as correct (or reject) the processing done by other participants. Consensus called PoX may be implemented in different ways. Among others, we find lottery-based algorithms including Proof of Elapsed Time (PoET) and Proof of Work (PoW) or through the use of voting-based methods including Redundant Byzantine Fault Tolerance (RBFT) and Paxos (Schuster B., 2017). The lottery-based algorithms are faster in terms of adding blocks in the chain, but if two miners offer two different blocks, this will no longer be the case

A complete process is exposed in the figure 2. Different steps are carried out to validate a transaction. We are in a P2P network, which means that the links are N-to-N relations. Whenever a transaction is initiated, it will be broadcasted to all nodes of a P2P network for validation and consensus.

Thereafter, the network of nodes validates the transaction based on predefined algorithms. Once controlled, the transaction is placed within others to form a block in the chain. At this stage, the transaction is completed.

3. THE DIFFERENT BLOCKCHAIN TECHNOLOGIES

This section provides an overview of most known blockchain technologies. We have taken five main used technologies. Firstly, Bitcoin which is the first implementation and most famous practical blockchain implementation. Secondly, we explain Ethereum, which is the second most known practical implementation after bitcoin. In addition, we expose three others private or semi-private blockchain implementation; Ripple, Hyperledger Fabric of IBM and Corda from consortium of banks called R3.

3.1 Bitcoin

Blockchain technology was announced by Satoshi Nakamoto in 2008 through a white paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” (Nakamoto S., 2008). This paper talks about a “purely peer-to-peer version of electronic cash” where the network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.

The Bitcoin network is designed to mathematically generate no more than 21 million Bitcoins and the network is set up to regulate itself to deal with inflation. Bitcoins can be spent by initiating a transfer request from a Bitcoin address in the sender's wallet to a Bitcoin address in the receiver's wallet.

Bitcoins are put into circulation by mining (an act of participating in a given P2P network in consensus) and operates on a proof-of-work basis. The proof-of-work model, while it does help increasing security and validity, does have some negative effects; because, it does not motivate miners to collaborate and they do not have anything to loose. Accordingly, there is no consequence for malicious activity (Harm et al., 2016). Bitcoin's block mining time is currently at about 10 minutes, so security is Bitcoin's first priority followed by speed.

The major risks that threaten the wide usability of the Bitcoin payment systems are the social risks. Thereby, it may include risk of socio-economic relationship, the legal risks because bitcoin technology opposes rules and regulations. Therefore, it finds opposition from governments, the economic risks like deflation, volatility and timing issues in finding a block, which might lead the users to migrate towards other currencies that offer faster services. Moreover, the technological risks that includes the network equipment, and its loss and the security risks such as double spending (Conti et al, 2017). In general, the bitcoin is used for investment, mining, currencies, commodities and financial services and remittances. According to statistics, 2017 has been a record-breaking year for bitcoin. From transactions to trading volume, and from wallet installations to market cap with 16.67 million of current bitcoin supply, 58% of crypto market dominance and 96 countries where bitcoin usage is unrestricted (Sedgwick K., 2017).

3.2 Ethereum

Simply explained Ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications. Ethereum was initially described in late 2013 as a result of research and work in the Bitcoin community. In January 2014, it was formally announced by Vitalik at the North American Bitcoin Conference in Miami, Florida, USA.

The intent of Ethereum is to ensure that data and small computer programs called smart contracts are replicated and processed on all the computers on the network, without a central coordinator.

Ethereum does not have a maximum total number of ether (the cryptocurrency behind Ethereum) but does cap the amount released each year. Ethereum block times are currently at about 14 seconds and it currently operates on a proof-of-work basis but working on a proof-of-stake basis (Harm et al., 2016). Proof-of-stake is a consensus mechanism for digital currencies that is an alternative to proof-of-work used in Bitcoin and due to it; we do not need any more expensive computations for block generation.

Ethereum clients are analogous to virtual machines and allow developers to run Ethereum programs on their local machine. The most popular clients offered by the Ethereum foundations are go-ethereum(Go), cpp-ethereum (C++), and pyethapp (Python). Data and contracts in Ethereum are encoded but not encrypted, and all data is completely public. Therefore, if sending sensitive data through the Ethereum network the user should encrypt it locally before sending it (Macdonald et al., 2017).

The vulnerabilities in this type of blockchains can be divided to three classes, according to the level where they are introduced -Solidity, EVM bytecode, or blockchain- (Atzei et al., 2016). In fact, the complexity of the software makes it vulnerable to a large number of security issues.

Ether is the second-largest cryptocurrency, but in 2018, it was down more than 70%. Nevertheless, some analysts think that it will gain more market share than bitcoin (Georgiev G., 2018).

3.3 Ripple

The Ripple Transaction Protocol (RTXP), issued in 2012. It is a payment network built on blockchain, used to send money globally. The cryptocurrency behind Ripple is XRP.

XRP has no public ledger, but instead uses an “iterative consensus process”. This process entails a supermajority of Ripple servers mutually agreeing that a transaction within the network is valid before updating the ledger. Ripple servers use public/private key cryptography to verify whether transactions are valid or not (Schuster B., 2017).

The result is a shorter transaction time less than 4 s and much less computing power. Ripple has a very specific focus to be accepted by the banking system for cross-border, interstate and interbank payments and remittances.

According to China CERT report, Ripple has 223 of its 230 flaws classified as high threat, which is very disconcerting. The report mentions how hackers of Ripple flaws could cause unimaginable losses to financial institutions on the network (Buntinx J.P., 2017). Ripple is a specific blockchain application for banking domain.

3.4 Hyperledger Fabric

Hyperledger is not a blockchain in itself. Hyperledger is a hub for many blockchain projects under the Linux Foundation. Five projects reside under Hyperledger. We will focus on IBM Hyperledger called Fabric.

Hyperledger takes a novel approach compared to the traditional blockchain model, particularly by managing the admission of participants at its core. In other words, Hyperledger is a permissioned, shared ledger. It is based on the expectation that there will be many blockchain networks, with each network ledger serving a different goal (Androulaki et al., 2018).

In its context, nodes assume different roles and tasks in the process of reaching consensus. The default consensus algorithm of Hyperledger Fabric is called Sieve. It enhances the "standard" PBFT mechanism so that the validation nodes make maximum efforts to identify non-deterministic transactions. There is no crypto-currency for Hyperledger.

Consensus in Hyperledger Fabric is broken out into 3 phases: Endorsement, Ordering, and Validation and provides crash fault tolerance in least time (WG Hyperledger Architecture, 2017).

This type of blockchain is built on a modular architecture, therefore fewer trust and verification levels are required across node types, and network scalability and performance are optimized. It allows for different organizations and participants in a common network to use their own certificate authority. Doing so, they implement varying cryptographic algorithms for signing, verifying and identifying.

3.5 Corda

Historically, Corda is a response from a banks consortium -R3- to blockchains like Hyperledger, Ethereum or Ripple. Their idea was that they could not leave a technology in the hands of others; while these third parties covet a sector traditionally reserved for the bank.

Corda is an implementation of the permissioned DLT. It is a platform for the writing of “CorDapps”: applications that extend the global database with new capabilities (Hearn M., 2016).

Corda uses special Notary Nodes to reach consensus. The list of these nodes is known and fixed, and it has no native cryptocurrency. Smart contracts in Corda are defined using JVM (Java Virtual Machine) bytecode.

Corda is uncommon solution because it does not have key characteristics that would not have other solutions.

4. COMPARISON AND EVALUATION

We start this section by a general comparison of the over-mentioned technologies. Then, we define some fundamental requirements to compare them. First, there are three main types of Blockchain (Zheng et al., 2018): public, private and hybrid.

- A blockchain is public when someone is free to take part in the authentication, verification and consensus process. It typically uses a consensus protocol to determine the current blockchain state and is typically controlled by pseudonymous participants.

- A blockchain is private when its participants are pre-selected or subject to a blocking entry, that requires the satisfaction of certain requirements or the blockchain administrator approval. It can use a consensus protocol to determine the blockchain status, or it can use an administrator or subgroup of participants to do so.

- Hybrid blockchain: parameters, such as read permission, are generally related to the degree of centralization that the blockchain developers want to achieve.

Another type is added, it is a blockchain built on permission requirement from an authority to become a verifier in the system. This limits the access to verify the transaction in the blockchain. With permissioned blockchains, it may not involve at all PoX in some nodes. An advantage of a permissioned blockchain is scalability as only some nodes store and operate on the chain. Nevertheless, it is much easier for a group of users to collaborate in order to alter the rules (Müller et al., 2016).

4.1 Security Aspects

As crypto-money bitcoin and others are digital currencies with a prominent market value, it pushes people to exploit their weaknesses to make profit.

In order to use crypto-money, the first thing a user needs is a wallet, which is equivalent to user's account. It also holds a public key pair. It is fundamental to apply the usual caution to secure the wallet; otherwise, the flaws appear at the starting (Tschorsch et al, 2015). Indeed, ab-initio, adaptability and cross layering security mechanisms are necessary to protect any dynamic system (El-Maliki T., 2010).

Essentially some attacks are already known and the most famous one is double spending (i.e, in which an adversary attempts to use some of her coins for two or more payments). However, there are mechanisms to control the double spending (Karame et al, 2012). The attack vectors including key recovery and transaction malleability (Rajput et al., 2014) are mainly exploited and the most fundamental fear is the so-called 51% attack. Meaning that if there are more than or equal to 51% of compromised miners, the entire network could be compromised. In practice, more than 20% of compromised miners could act dangerously in case of Ripple. Selfish mining strategy could help miners to gain revenue only by using 25 % hashing power (Zheng et al., 2018).

Hacked systems, buggy software or incorrect usage is probably the highest security risk. However, the most prominent type of attack remains double spending. The first blockchain lifetime must be long to protect the

chain. Therefore, bootstrapping problem when blockchain starts from scratch is a real problem. Indeed, the first blocks are easy to compromise. For example, Garay (Garay et al., 2016) presents one solution to this problem.

4.2 Comparison based on General Aspects

This part summarizes selected blockchain technologies to show their respective approaches diversities. Our choice has been lead by the blockchain importance on the current market since each blockchain has its proper characteristics and its application field.

Table 1 illustrates a comparison limited to the five above-mentioned blockchains: Bitcoin, Ethereum, Hyperledger Fabric, Corda R3 and Ripple. It shows the blockchain technologies characteristics.

We have identified six criteria to compare general aspects of these technologies: the type of the chain – public, or private-, the platform governance, the industry sector where it should be used, the programming languages, the consensus used to validate the transactions, smart contract usage and the usability for crypto-money.

Table 1. Blockchain, a general comparison

Blockchain	Bitcoin	Ethereum	Hyperledger Fabric	Corda R3	Ripple
Type	Public	Public , Private Permissionless	Permissioned	Permissioned	Semi- Permissioned
Governance	Developers	Developers	Linux Foundation	R3 Consortium	Ripple Labs
Industry	Financial services	Many fields	Many fields	Financial services	Financial services
Language	C++	Golang, C++, Python	Golang, Python	Java and other JVM language	Python or C++
Consensus	PoW	PoW	PBFT, Practical byzantine fault- tolerant	Mix of approaches	Byzantine Altruistic Rational (BAR)
Smart contract	No	Yes	Yes	Yes	No
Crypto-money	bitcoin	Ether(ETH)	No	No	Ripple(XRP)

4.3 Detailed Comparison

Given the existing varieties among blockchain technologies, we decide to fine tune using metrics to choose one of them. We have also chosen particular criteria for comparison. These are summarized as follows:

- Scalability: The degree to which nodes can be increased in the blockchain
- Security: The management method to ensure the confidentiality, integrity, non-repudiation and authenticity
- Performance efficiency: The characteristics of the consensus algorithm that is used
- Portability: Degree to which a product or system can efficiently be adapted for different or evolving hardware, software or other operational or usage environments
- Availability: Degree to which a system, product or component is operational and accessible when required for use.

In order to make it clear, we will explain our comparison methodology. Note that consensus performance and scalability cannot exist optimally in the same blockchain using today's consensus method. Indeed, the more communication is needed to reach a consensus, the more the number of nodes that can participate in the blockchain is limited and the more we improve the consensus performance (Vukolic M., 2015).

For portability, we rely on the ability to offer features allowing the development of different applications. For security, we rely on the China CERT report and the difference between private and public blockchains. Finally, availability is almost offered by different blockchains. Five stars are the highest value and one star is the lowest one. The other value are in between. According to these requirements, Ethereum is the best relatively positioned blockchain technology. In term of scalability and performance, the public blockchains -Bitcoin and Ethereum- are very limited; however, they are more secure and available. In our opinion, if any combining the benefit each technology, we could converge to a better practical and well-designed technology. Table 3 illustrates this comparison in details.

Table 2. Blockchain technologies and relevant requirements * lowest value, ***** best value. Others in between

Blockchain	Scalability	Security	Performance efficiency	Portability	Availability
Bitcoin	**	*****	**	**	*****
Ethereum	***	*****	***	*****	*****
Ripple	*****	**	*****	*	*****
Hyperledger Fabric	*****	***	*****	*****	***
Corda	*****	***	*****	***	***

Table 3 depicts the detailed comparison between blockchain technologies according to the following criteria:

1. Transparency: all messages sent by participants are visible to all other participants.
2. irrevocability: transactions recorded on a blockchain can be made to be irrevocable and irreversible
3. Programmable: instructions can be included in code embedded within a block on a blockchain.
4. Scalability: how well a platform scales with network size and the number of transactions per second that need to be validated.
5. Security: the security of transaction data, user anonymity and the security of the blockchain itself.
6. Limitations and Flexibility: the number of different applications currently using the blockchain
7. Usability: the level of platform- specific knowledge required to develop with a platform
8. Cost: the cost of consensus (e.g. computational power, energy or time), the difficulty of consensus (e.g. is it random or deterministic) and whether it is difficult to alter the data were carefully considered.

Table 3. Blockchain technologies and specific requirements

	Transparency	irrevocability	Programmable	Scalability	Security	Limitations and Flexibility	Usability	Cost
Bitcoin	Accessible to all	Nearly	non	block time = 10 min	Significant number of cyber attack	The API for developing services is difficult to use.	No need	SHA-256 Hash + Proof of Work
Ethereum	Accessible to all	Nearly	Smart contract (Solidity)	block time = 14 sec	Scalability may expose it to more security threats	hundreds of blockchain-based apps	Language Solidity	EtHash + Proof of Work
Hyperledger Fabric	Access limited by permissions	Could be tampered	Chain code (Go or Node.js)	N/A	Designed as modular	targeted at businesses wanting to streamline their process	Golang and Java	Practical Byzantine Fault-Tolerant (PBFT) and others
Corda	Access limited by permissions	Could be tampered	Smart contracts (Kotlin, java)	N/A	Multi-signature support Signed identity	Suitable for a variety of applications.	Java and others	Mix of approaches
Ripple	Access limited by permissions	Could be tampered	non	block time = 4 sec	Ripple does not offer transaction anonymity	The API for developing services is difficult to use.	No need	Byzantine Altruistic Rational (BAR)

5. CONCLUSION

Data storage is a main component in computer systems; the blockchain becomes an important concept offering implementations that differ from one solution to another. Indeed, each solution has different approaches to process, validate and make data immutable.

We consider the blockchain as another alternative to store the data in a decentralized way that is complementary to centralized systems. This technology has the ability to create a private or public network of nodes that share data in a distributed manner. The blockchain potential depends on the ability to validate stored data by the different nodes based on a PoX.

This article aims to understand the different blockchain components and to know the limits of each implementation approach. We explore how the blockchain evolution allows finding new domains where this technology can be applied, such as financial institutions, hospitals and companies.

Bitcoin is the first implementation of crypto-money based on blockchain and still the most famous. Hyperledger Fabric and Ethereum were developed to solve different problems. Hyperledger Fabric is adapted to a business usage scenario. Whereas, Ethereum was carried out for public usage with the notion of fully transparent and objective transactions execution, even in an arbitrarily aggressive environment. Corda is uncommon solution, and does not have more key characteristics than others have. Ripple is a very specific solution especially for banking domain.

Each of these technologies has many applications and industrial fields' opportunity. In the near future, we will carry out a full study of almost all technologies of blockchain with an application in the academic field for articles, diplomas and certificates immutability.

REFERENCES

- Nakamoto S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. White paper
- Kosba A., 2006. *Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts*. IEEE Symposium on Security & Privacy (Oakland)
- Akins, B.W. et al, 2013. *A Whole New World: Income Tax Considerations of the Bitcoin Economy*. Pittsburgh Tax Review, Forthcoming. Available at SSRN: <https://ssrn.com/abstract=2394738>
- Panarello, A. et al, 2018. *Blockchain and IoT Integration: A Systematic Survey*. Published in Sensors
- Sharples, M. et al, 2016. *The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward*. Adaptive and Adaptable Learning: Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, Lecture Notes in Computer Science. Switzerland: Springer, pp. 490–496
- Abiteboul, S. et al, 2000. *Data on the Web: From Relations to Semi structured Data and XML*. Morgan Kaufmann Publishers, San Francisco, USA
- Müller, C. et al, 2016. *Blockchain: Technology and Applications*. Report of Department of Computer Sciences University of Salzburg
- Zheng, Z. et al, 2018. *Blockchain challenges and opportunities: a survey*. Int. J. Web and Grid Services, Vol. 14, No. 4
- Tschorsch, F. et al, 2015. *Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies*. Cryptology ePrint Archive: 2015/464
- El-Maliki, T., 2010. *Security adaptation in highly dynamic wireless networks*. University of Geneva, <https://archive-ouverte.unige.ch/unige:37196>
- Karame, G. et al, 2012. *Double-Spending Fast Payments in Bitcoin*. CCS'12, October 16–18, 2012, Raleigh, North Carolina, USA
- Rajput, U. et al., 2014. *A Simple Yet Efficient Approach to Combat Transaction Malleability in Bitcoin*. Information Security Applications: 15th International Workshop, WISA 2014, Jeju Island, Korea
- Murphy, S., 2016. *Unlocking the blockchain: A global legal and regulatory guide*. Norton Rose Fulbright LLP
- Garay, J. A. et al, 2016. *The Bitcoin Backbone Protocol with Chains of Variable Difficulty*. Cryptology ePrint Archive: Report 2016/1048
- Harm, J. et al, 2016. *Ethereum vs Bitcoin*. Creighton University case study
- Conti, M. et al, 2017. *A Survey on Security and Privacy Issues of Bitcoin*. arXiv:1706.00916v3 [cs.CR]
- Sedgwick K., 2017. *Bitcoin by Numbers: 21 Statistics That Reveal Growing Demand for the Cryptocurrency*. Bitcoin.com
- Macdonald, M. et al, 2017. *The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin*

- Atzei, N. et al, 2016. *A survey of attacks on Ethereum smart contracts*. The Cryptology ePrint
- Georgiev G., 2018. *Weiss Ratings: Bitcoin Will Lose 50% of Its Market Share to Ethereum in 5 Years*. bitcoinist.com
- Schuster B., 2017. *The Ripple Currency Problem: Why Permissioned Blockchains Will Devalue XRP*. hackernoon.com
- Buntinx J.P., 2017. *China Blockchain Report Blasts Ripple for High-risk Security Flaws*
- Androulaki, E. et al, 2018. *Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains*. arXiv: 1801.10228 [cs.DC]
- WG Hyperledger, 2017. *Introduction to Hyperledger Business Blockchain*. Design Philosophy and Consensus, Hyperledger Architecture, Volume 1 Hearn, M., 2016. *Corda: A distributed ledger*. Corde.net
- Vukolic M., 2015. *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*. IBM Research – Zurich