Blockchain Challenges and Opportunities: A Survey

Zibin Zheng*

School of Data and Computer Science,
Sun Yat-sen University,
Guangzhou, China
E-mail: zhzibin@mail.sysu.edu.cn
and
Collaborative Innovation Center of High Performance Computing,
National University of Defense Technology,
Changsha 410073, China
*Corresponding author

Shaoan Xie

School of Data and Computer Science,
Sun Yat-sen University,
Guangzhou, China
E-mail: xieshan3@mail2.sysu.edu.cn

Hong-Ning Dai

Faculty of Information Technology,
Macau University of Science and Technology,
Macau SAR
E-mail: hndai@ieee.org

Huaimin Wang

National Laboratory for Parallel & Distributed Processing,
National University of Defense Technology,
Changsha 410073, China

Abstract:

Blockchain, as one of the core technologies in Bitcoin that is the most representative cryptocurrency, has received extensive attentions recently. Blockchain can be used as a peer-to-peer (P2P) decentralized system to store the pseudonymous transaction records in a trustless environment. It is believed that blockchain can be used in a diversity of future Internet interaction systems, such as smart contracts, public services, Internet of Things (IoT), reputation systems and security services rather than financial systems only. However, a number of technical challenges prohibit the wide application of blockchain. Therefore, we present a comprehensive survey on blockchain technologies. In particular, we first provide an overview of blockchain technologies and a taxonomy of various blockchain systems. We then enumerate a number of both current and future

blockchain applications. We also discuss the challenges in this promising area and discuss the future directions.

Keywords: Blockchain; Evolution; Application; Decentralization.

Biographical notes: Zibin Zheng is an associate professor at Sun Yat-sen University, Guangzhou, China. He received Ph.D. degree from The Chinese University of Hong Kong in 2011. He received ACM SIGSOFT Distinguished Paper Award at ICSE'10, Best Student Paper Award at ICWS'10, and IBM Ph.D. Fellowship Award. His research interests include services computing, software engineering, and data mining.

Shaoan Xie is a graduate student at Sun Yat-Sen University, China. He received his bachelor degree in Computer Science at Sun yat-sen University in 2016. His current research interests include blockchain and data mining.

Hong-Ning Dai is an associate professor in Faculty of Information Technology at Macau University of Science and Technology. He obtained the Ph.D. degree in Computer Science and Engineering from Department of Computer Science and Engineering at the Chinese University of Hong Kong in 2008. His research interests include wireless networks, mobile computing, and distributed systems.

Huaimin Wang received the PhD degree in computer science from the National University of Defense Technology (NUDT) in 1992. He has been awarded the Chang Jiang Scholars professor by Ministry of Education of China, and the National Science Fund for Distinguished Young Scholars, and so on. He has published more than 100 research papers in international conferences and journals. His current research interests include middleware, software agent, trustworthy computing.

1 Introduction

Recently, *cryptocurrency* has received extensive attentions from both industry and academia. Bitcoin that is often called the first cryptocurrency has enjoyed a huge success with the capital market reaching 10 billion dollars in 2016 (*State of Blockchain Q1 2016: Blockchain Funding Overtakes Bitcoin* 2016; *Crypto-Currency Market Capitalizations* 2016). The core technology to construct Bitcoin is *blockchain*, which was first proposed in 2008 and was implemented in 2009 (Nakamoto 2008). Blockchain is essentially a public ledger, in which all committed transactions are stored in a list (or a chain). This chain continuously grows when the new transactions have been confirmed. In order to protect blockchain from tampering in distributed systems, a complicated but secure mechanism (based on asymmetric cryptography and distributed consensus) has been implemented. The blockchain technology essentially has the key characteristics, such as decentralization, persistency, anonymity, fault-tolerance and auditability, which allows a transaction to take place in a decentralized fashion without the need of central intermediary. As a result, blockchains can greatly save the cost and improve the efficiency.

Blockchain can not only be used in various current financial services such as digital assets, remittance and online payment (Peters, Panayi, and Chapelle 2015; Foroglou and Tsilidou 2015), but also become one of the most promising technologies for the next generation of Internet interaction systems, such as smart contracts, public services, Internet

of Things (IoT), reputation systems and security services (Mattila 2016; Coeckelbergh and Reijers 2016; Shrier, Wu, and Pentland 2016; Pilkington 2016a). Blockchain can work in a decentralized and trustless environment, which is enabled by integrating several core technologies such as cryptographic hash, digital signature (based on asymmetric cryptography) and distributed consensus mechanism. In blockchain, every compatible client can be completely involved with all the operations including initiating a new transaction, receiving a transaction, verifying transaction, participating in the competition of creating new blocks (also named as mining procedure).

Although the blockchain technology has the great potential for the construction of the future Internet interaction systems, it is facing a number of technical challenges. In particular, current blockchain systems need to be further improved so that they can be scalable to fulfill the requirement of processing millions transactions in real-time fashion. Besides, a new mechanism needs to be proposed to avoid selfish miners in blockchain systems (Eyal and Sirer 2014). Moreover, other technical challenges such as the privacy leakage and deficiency of current consensus algorithms need to be solved before blockchain can be widely used in various Internet interaction systems.

There is a lot of literature on blockchain from various sources, such as blogs, wikis, forum posts, codes, conference proceedings and journal articles. To the best of our knowledge, there are few rigor surveys on blockchain from the technical perspective. It is true that there are some surveys such as (Tschorsch and Scheuermann 2016)(NRI 2015). However, (Tschorsch and Scheuermann 2016) is too specific to Bitcoin blockchain (no technical details about other types of blockchain) while (NRI 2015) lacks of the in-depth technical details of blockchain technologies. Therefore, it is the purpose of this paper to conduct a comprehensive survey to let readers gain a full in-depth understanding of blockchain technologies.

In particular, this survey presents an overview of blockchain technologies including the blockchain architecture, consensus approaches, key characteristics of blockchain and the taxonomy of various blockchain systems. Besides, this article enumerates both current and future applications of blockchain. Moreover, this paper presents the research challenges in blockchains and discusses some future directions that lead us to explore open issues in this promising area.

The rest of this paper is organized as follows. Section 2 introduces an overview of blockchain technologies. Section 3 discusses the applications of blockchain. Section 4 summarizes the technical challenges of blockchain and the recent advances in this area. Finally, this paper is concluded in Section 5.

2 Overview of blockchain technologies

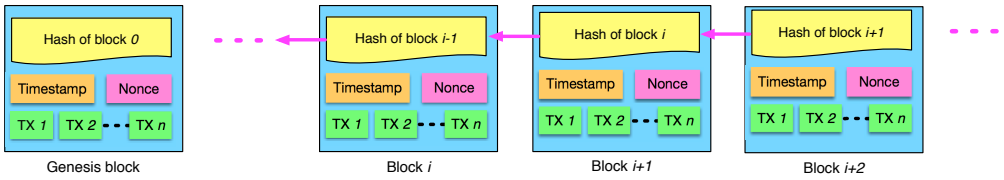
This section surveys the core technologies of blockchain. In particular, Section 2.1 provides a blockchain system architecture. Section 2.2 surveys the consensus approaches used in blockchain. Section 2.3 summarizes the key characteristics of blockchain and Section 2.4 offers a taxonomy of existing blockchain systems.

2.1 Blockchain architecture

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger (Chuen 2015). Figure 1 illustrates an example, in which a number

of blocks form a chain of blocks or a *blockchain*. Each block points to the immediately previous block via a reference that is essentially a hash value of the previous block called *parent* block. The first block of a blockchain is called a genesis block, which has no parent.

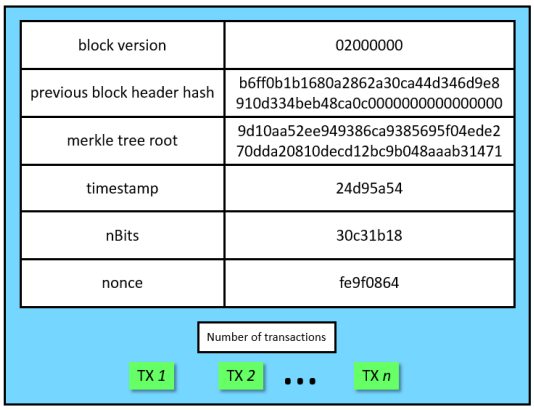
Figure 1 An example of blockchain, in which a sequence of blocks are backwardly ordered via the hash values of the previous blocks with the exception of the first block (called the genesis block).



We then explain the internals of blockchain in details.

2.1.1 Block

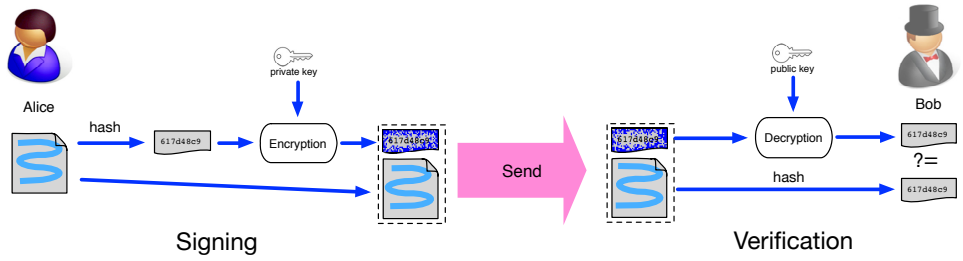
Figure 2 Block structure



A block consists of the *block header* and the *block body* as shown in Figure 2. In particular, the block header includes: (i) block version, (ii) previous block header hash, (iii) merkle tree root hash, (iv) timestamp, (v) nBits, (vi) the nonce. More specifically, block version number indicates which set of block validation rules to follow. The hash value of the previous block is a 256-bit hash value that points to the previous block. The Merkle tree root is the hash value of all the transactions in the block. The time stamp field represents the current time stamp as seconds in universal time since January 1, 1970. The nBits is the target threshold of a valid block hash. A nonce is an 4-byte field, which usually starts with 0 and increases for every hash calculation, which will be explained in details in Section 2.2. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction.

The block body includes the number of transactions and the collection of transactions. A valid transaction is mainly composed of two individual parts: inputs and outputs. Transaction

Figure 3 Digital Signature used in blockchain



ids in inputs is a reference to the unspent transaction outputs (UTXO) of the sender while the sender has to specify the destination address and amount in outputs. Furthermore miners would check the signature in inputs to validate a transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions (NRI 2015). The asymmetric cryptography can ensure authentication, integrity and non-repudiation (Christidis and Devetsikiotis 2016). In particular, digital signature based on asymmetric cryptography is used in an untrust environment. We next briefly illustrate the workings of digital signature.

2.1.2 Digital Signature

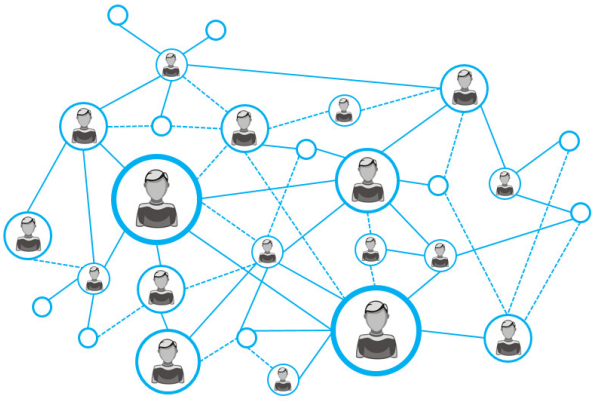
Each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is used to sign the transactions. The digital signed transactions are spread throughout the whole network and then are accessed by public keys, which are visible to everyone in the network. Figure 3 shows an example of digital signature used in blockchain. The typical digital signature is involved with two phases: the signing phase and the verification phase. Take Figure 3 as an example again. When a user Alice wants to sign a transaction, she first generates a hash value derived from the transaction. She then encrypts this hash value by using her private key (that is confidential to her) and send to another user Bob the encrypted hash with the original data (i.e., the transaction). Bob verifies the received transaction through the comparison between the decrypted hash (by using Alice's public key) and the hash value derived from the received data by the same hash funcation as Alice's. The typical digital signature algorithms used in blockchains include elliptic curve digital signature algorithm (ECDSA) (Johnson and Menezes 2001).

2.1.3 Decentralized Network

Each user interacts with the blockchain network via a dedicated node in which a blockchain client is installed. A large number of nodes across the whole network form a decentralized network as shown in Figure 4. Once a node receives data from another node, it verifies the authentication of the data. It then broadcasts the validated data to every other node connected to it. In this way, the data is spread across the whole network.

One of benefits of such decentralized systems is the independence of the central server or the third-party, which can greatly save the costs. However, the decentralized system also brings the challenge in verifying the transaction authentication in the untrust environment. We discuss the solutions to this challenge in Section 2.2.

Figure 4 Decentralized network



2.2 *Consensus on the network*

Once the transactions have been created, they need to be verified by the network. However, there may exist a divergence of branches of a blockchain as shown in Figure 5 since each node may have a different view of the whole network state. Therefore, a distributed mechanism to mitigate the branches in a blockchain is needed.

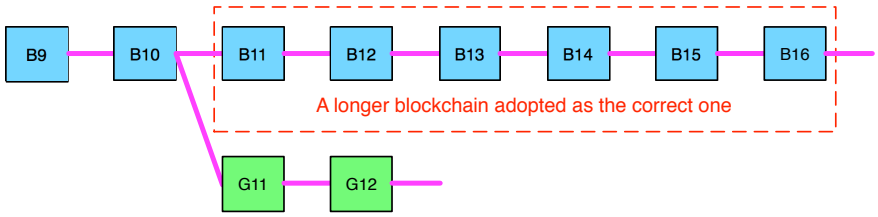
In the blockchain network, how to reach consensus on a transaction among the untrusted nodes is a transformation of Byzantine Generals (BG) Problem, which was raised in (Lamport, Shostak, and Pease 1982). In BG problem, a group of generals who command a portion of Byzantine army circle the city. Some generals prefer to attack while other generals prefer to retreat. However, the attacks would fail if only part of the generals attack the city. Thus, they have to reach an agreement to attack or retreat. How to reach a consensus in distributed environment is a challenge. We next survey the common approaches to reach a consensus in blockchain.

2.2.1 *Approaches to consensus*

There are four representatives of the modern consensus algorithms, which are listed as follows.

POW (Proof of work) is a consensus strategy used in Bitcoin network (Nakamoto 2008). POW requires a complicated computational process in the authentication. In POW, each node of the network is calculating a hash value of the constantly changing block header. Recall that a nonce is a value starting from 0 and increasing for each hash calculation (see Section 2.1). The consensus requires that the calculated value must be equal to or smaller than a certain given value. In the decentralized network, all participants have to calculate the hash value continuously by using different nonces until the target is reached. When one node obtains the relevant value, all other nodes must mutually confirm the correctness of the value. After that, transactions in the new block would be validated in case of frauds. Then, the collection of transactions used for the calculations is approved to be the authenticated result, which is denoted by a new block in the blockchain. The nodes which calculate the hashes are called *miners* and the POW procedure is called *mining* in Bitcoin. Since the calculation of the authentication is a time consuming process, an incentive mechanism (e.g., granting a small portion of Bitcoins to the miner) is also proposed (Nakamoto 2008).

Figure 5 An scenario of blockchain branches



Note that the target value is automatically adjusted by the network to ensure that a block generating process takes about 10 minutes on average.

In the decentralized network, valid blocks might be generated simultaneously when multiple nodes find the suitable nonce nearly at the same time. As a result, branches (or forks) may be generated as shown in Figure 5. However, it is unlikely that two competing forks will generate next block simultaneously. In POW protocol, a chain that becomes longer thereafter is judged as the authentic one. Take Figure 5 as an example again. Consider two forks created by simultaneously validated blocks B11 and G11. Miners work on both the forks and add the newly generated block to one of them. When a new block (say B12) is added to block B11, the miners working on fork G11-G12 will switch to B12. Block G12 in the fork G11-G12 becomes an orphan block since it is no longer increased. Generally, when approximately six blocks are generated, the relevant blockchain is considered to be the authentic one (e.g., the chain of blocks B11, B12, B13, B14, B15 and B16 in Figure 5). Since a block is generated in about 10 minutes, a blockchain is authenticated in about a hour (i.e., 60 minutes).

POS (Proof of stake) is an energy-saving alternative to POW. Instead of demanding users to find a nonce in an unlimited space, POS requires people to prove the ownership of the amount of currency because it is believed that people with more currencies would be less likely to attack the network. The idea of POS originated from (Szabo 2004), which essentially discusses alternative proof systems. Since the selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network, many solutions are proposed with the combination of the stake size to decide which one to forge the next block. In particular, Blackcoin (Vasin 2014) uses randomization to predict the next generator while Peercoin favors coin age based selection (King and Nadal 2012). Compared to POW, POS saves more energy and is more effective. Unfortunately, as the cost to mine is nearly zero, the attacks might come as a consequence.

PBFT (Practical byzantine fault tolerance) is a replication algorithm to tolerate byzantine faults (Castro, Liskov, et al. 1999). Hyperledger (*Hyperledger Project* 2015) utilizes the PBFT as its consensus algorithm since PBFT could handle up to 1/3 malicious byzantine replicas. A primary that is responsible for multicasting requests to other replicas is selected in a view. The validating process is divided into three phase: pre-prepared, prepared, commit. A service operation would be valid if it has received approvements from over 1/3 different replicas. Additionally, if a client does not receive the replies, it will send the request to all replicas instead of only sending it to the primary in case of the primary is faulty. A primary is responsible for ordering the transaction and each replica commits the transaction in the same order.

Table 1 Comparisons of consensus algorithms

Property	POW	POS	PBFT	DPOS
Node identity management	open	open	permissioned	open
Throughput	limited	excellent	excellent	excellent
Latency	high	low	low	low
Energy saving	no	yes	yes	yes
Tolerated power of adversary	<=25% computing power	<=49% stake	<=33.3% faulty replicas	<=49% validators
Example	Bitcoin	Peercoin	Hyperledger	Bitshares

DPOS (Delegated proof of stake). Similar to POS, miners get their priority to generate the blocks according to their stake. The major difference between POS and DPOS is that POS is a direct democratic while DPOS is representative democratic. Stakeholders elect their delegates to generate and validate a block. With significantly fewer nodes to validate the block, the block could be confirmed quickly, making the transactions confirmed quickly. Meanwhile, the parameters of the network such as block size and block intervals could be tuned by the delegates. Additionally, users do not to need worry about the dishonest delegates who could be voted out easily. DPOS has already been implemented, and is the backbone of Bitshares (*Delegated Proof of Stake (DPOS) vs Proof of Work (POW)* 2015).

2.2.2 Comparisons of consensus approaches

Different approaches have different constraints, advantages and disadvantages. Table 1 gives a high level comparison between different consensus algorithms, where we use the properties given by (Vukolić 2015). In particular, we summarize our findings as follows.

- *Node identity management*. Only PBFT needs to know the identity of each miners in order to select a primary in every view.
- *Throughput*. Since the POW has restrictions on block size and block interval, the throughput of a blockchain is extremely limited.
- *Latency*. POW generates a new block for nearly 10 minutes, thus the confirmation time is nearly 1 hour, which is so long for a normal transaction.
- *Energy saving*. Miners hash the nonce to reach the target until a solution is given. As a result, the amount of electricity required to process has reach an immense scale. As for POS, DPOS, PBFT, less mining or no mining saves energy.
- *Tolerated power of adversary*. Generally 51% of hash power is regarded as the threshold for one to gain control of the network. But selfish mining strategy in POW systems could help miners to gain more revenue and only 25% of the power is enough. PBFT is designed to handle up to 1/3 faulty nodes.
- *Example*. Bitcoin is based on proof of work while Peercoin is a new peer-to-peer proof-of-stake cryptocurrency. Further, Hyperledger, a cross-industry standard platform for

distributed ledgers, utilizes PBFT to reach consensus. Bitshares, a smart contract platform, adopts DPOS as their consensus protocol.

2.3 Key characteristics of blockchain

In summary, blockchain has the following key characteristics.

- *Decentralization.* In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank) inevitably resulting the cost and the performance bottlenecks at the central servers. Differently, a transaction in the blockchain network can be conducted between any two peers (P2P) without the authentication by the central agency. In this manner, blockchain can significantly reduce the server costs (including the development cost and the operation cost) and mitigate the performance bottlenecks at the central server.

- *Persistency.* Since each of the transactions spreading across the network needs to be confirmed and recorded in blocks distributed in the whole network, it cannot be modified and the falsification is difficult. No entity can delete or rollback transactions once they are included in the blockchain stored in the distributed network.

- *Anonymity.* Each user (or entity) can interact with the blockchain network with a generated address (through the public key), which does not reveal the read identity of the user. This mechanism preserves a certain amount of privacy on the transactions included in the blockchain. Note that blockchain can not guarantee the perfect privacy preservation due to the intrinsic constraint (details refer to Section 4).

- *Auditability.* Since each of the transactions on the blockchain is validated and recorded with a timestamp, it accounts for a global truth that users can easily verify and trace the previous records through accessing any node in the distributed network. It definitely improve the traceability and the transparency of the data stored in the blockchain.

2.4 Taxonomy of blockchain systems

Vitalik, the founder of ethereum (Wood 2014), roughly categorized the current blockchain systems into three types: public blockchains, private blockchains and consortium blockchains (Buterin 2015). A public blockchain is a traditional blockchain, in which all records are visible to the public and everyone could take part in the consensus process. Differently, a group of pre-selected nodes would be dominant in the consensus process of a private blockchain. Transactions on a private blockchain would be likely visible to the participants rather than everyone in the world. Note that a private blockchain could not be defined as a decentralized network any more since it is fully controlled by one organization. The consortium blockchain is partially decentralized since the validators in a consortium blockchain are selected by the nodes.

The comparison among the three types of blockchains is listed in Table 2. In particular, we summarize our findings as follows.

- *Consensus determination*. All miners have to reach consensus in the public blockchain while only a selected set of nodes are needed to validate the block. Private chain is fully controlled by one organization.

- *Read permission*. Transactions in a public blockchain are visible to the public undoubtedly while the read permission depends on a private blockchain or a consortium blockchain.

- *Immutable*. Since the records are stored on different miners, the transactions could not be tampered in a public blockchain. Differently, transactions in a private blockchain or a consortium blockchain are editable as long as the major participants have reached an agreement.

- *Efficiency*. Since the public blockhain requires all miners to validate and reach consensus, the transaction throughput and the latency are limited. With fewer validators, consortium blockchain and private blockchain could be more efficient.

- *Centralized*. The main difference among the three types of blockchains is that public blockchain is decentralized and consortium blockchain is partially centralized and private blockchain is fully centralized.

- *Consensus process*. Everyone in the world could join the consensus process of public blockchain. Different from public blockchain, both consortium blockchain and private blockchain are the permissioned blockchain.

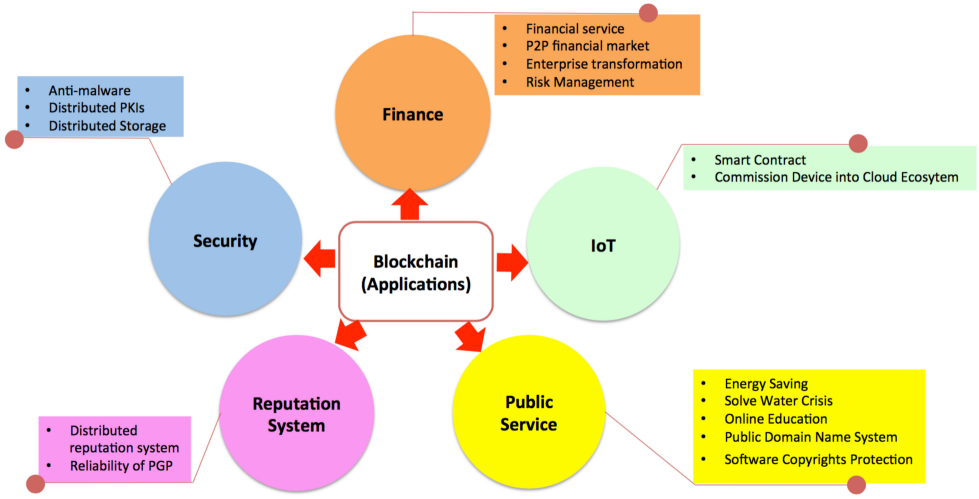
Table 2 Comparisons among public blockchain, consortium blockchain and private blockchain

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus	all miners	selected set of nodes	one organization
Read permission	public	could be public or restricted	could be public or restricted
Immutable	yes	could be tampered	could be tampered
Efficiency	low	high	high
Centralized	no	partial	yes
Consensus process	permissionless	permissioned	permissioned

3 Applications of blockchain

There is a diverse of applications of blockchain technologies. In this section, we summarize the typical applications of blockchain. We roughly categorize the applications of blockchain into financial services in Section 3.1, public services in Section 3.3, IoT in Section 3.2, reputation system in Section 3.4 and security in Section 3.5. Figure 6 illustrates 6 representative application domains of blockchain.

Figure 6 Representative application domains of blockchain.



3.1 Financial and business services

The emergency of blockchain systems (such as Bitcoin (Nakamoto 2008) and (*Hyperledger Project* 2015)) has brought a huge impact on traditional financial and business services. Peters and Panayi provided an overview of blockchain technology and the impacts brought by blockchain on traditional financial services (such as remittance, smart contracts, automated banking ledgers and digital assets) (Peters and Panayi 2015). Besides, Trautman (Trautman 2016) discussed the disruptive changes taking place in financial services with the rapid development of blockchain technology. Furthermore, many researchers argue the suitability of blockchain technology as the backbone of financial market infrastructure due to the vulnerability to bugs and hacking of blockchain.

On the other hand, many other researchers claim that blockchain technologies will improve financial and business services instead of disrupting them. This is because blockchain can reduce the costs and eliminate inefficiencies of the existing financial systems. In particular, Morini (Morini 2016) showed that there are real business cases for improving financial markets. Besides, Noyes explored ways of combining peer-to-peer mechanisms and multiparty computation protocols to create create a P2P financial market (Noyes 2016b). Furthermore, Malinova and Park (Malinova and Park 2016) capture features of blockchain technology in a theoretical model of peer-to-peer trading systems. By the way, blockchain has caught tremendous attention in the eyes of large software companies: Microsoft Azure and IBM are begining to offer Blockchain-as-a-Service (*Microsoft Azure: Blockchain as a Service* 2016; *IBM Blockchain* 2016).

In addition to the evolution of financial and business services, blockchain can help traditional organizations to complete the enterprise transformation smoothly. Consider an example of postal operators (POs). Since traditional postal operators (POs) act as a simple intermediary between merchants and customers, blockchain and cryptocurrency technology can help POs to extend their simple roles with the provision of new financial and un-financial services. In (Jaag, Bach, et al. 2016), Jaag and Bach explored opportunities of arising blockchain technology for POs and claimed that each PO could issue their own

postcoin which is a kind of colored coin of Bitcoin. Since the POs are viewed as a trusted authority by the public, postcoin could be prevailed quickly with their dense retail network. In addition, it is also shown in (Jaag, Bach, et al. 2016) that blockchain technology offers business opportunities for POs in identity services, device management and supply chain management.

Risk management framework plays a significant role in financial technology (FinTech) and now it can be combined with blockchain to perform better. Pilkington (Pilkington 2016b) provided a novel risk-management framework, in which blockchain technology is used to analyze investment risk in the Luxembourgish scenario. Investors who nowadays hold securities through chains of custodians tend to face risk of any of these failings. With the help of blockchain, investments and collaterals can be decided quickly instead of going through long-term consideration. Micheler and Heyde indicated in (Micheler and Heyde 2016) that a new system combined with blockchain can reduce custody risk and achieve the same level of transactional safety. Since the separate databases cause much trouble and efficiency, blockchain could help it to establish a distributed decentralized single shared database (Gerstl 2016). Besides, blockchain-based smart contract enables the decentralized autonomous organizations (DAO) to engage in business-work collaborations. Moreover, a highly dependable DAO-GaaS conflict model (Norta, Othman, and Taveter 2015) was proposed to safeguard business-semantics induced consistency rules.

3.2 Internet of Things (IoT)

Internet of things (IoT), one of the most promising information and communication technologies (ICT), is ramping up recently. IoT is proposed to integrate the things (also named smart objects) into the Internet and provides users with various services (Atzori, Iera, and Morabito 2010; Miorandi et al. 2012). The typical killer applications of IoT include the logistic management with Radio-Frequency Identification (RFID) technology ("ISO/IEC 18000" 2013), smart homes (Dixon et al. 2012), e-health (Habib, Torjusen, and Leister 2015), smart grids (Fan et al. 2013), Maritime Industry (Wang et al. 2015), etc.

Blockchain technologies can potentially improve the IoT sector. In (Christidis and Devetsikiotis 2016), Christidis and Devetsikiotis investigated the integration of blockchain with IoT. In particular, they proposed that digital tokenized assets transfer can be achieved easily and in a cryptographically verifiable manner using a blockchain network that employs the Bitcoin transactional model. Besides, they also proposed to use *smart contracts* (Szabo 2004) that reside one the blockchain and are allowed to execute in a prescribed manner. In this manner, each reaction of the contract is predictable. In fact, smart contract has become the major part of blockchain 2.0 (*Blockchain 2.0 - Let a Thousand Chains Blossom* 2014). Furthermore, Zhang and Wen (Zhang and Wen 2015) propose a new E-business model based on IoT and realize the transaction of smart property based on blockchain and smart contract. Currently companies like Antshares (*Antshares Digital Assets for Everyone* 2016), Taiyiyun (*taiyiyun* 2016), Bubi (*bubi* 2016) in China are focusing on digitalizing assets on peer to peer network with the help of blockchain technology.

Privacy preservation is another important concern with IoT industry. Blockchain can also help in improving privacy in IoT applications. In particular, Hardjono and Smith (Hardjono and Smith 2016) proposed a privacy-preserving method for commissioning an IoT device into a cloud ecosystem. More specifically, a new architecture was proposed in (Hardjono and Smith 2016) to help device to prove its manufacturing provenance without the authentication of third party and it is allowed to register anonymously. Besides, in (IBM

2015), IBM unveiled its proof of concept for ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry), which is a system using blockchain technologies to build a distributed network of devices - a decentralized Internet of Things. In ADEPT, appliances in the home would be able to identify operational problems and retrieve software updates on their own.

3.3 Public services

In addition to the applications in financial and busies services, blockchains can also be widely used in public services. One of typical blockchain applications in public services is the land registration (NRI 2015), in which the land information such as the physical status and related rights can be registered and publicized on blockchains. Besides, any changes made on the land, such as the transfer of land or the establishment of a mortgage can be recorded and managed on blockchains consequently improve the efficiency of public services. Blockchains can also be used to other public services such as marriage registration, patent management and income taxation systems (Akins, Chapman, and Gordon 2013). In the new public services integrated with blockchains, mobile devices with digital signature embedded may replace seals to be affixed on documents, which are submitted to administrative departments. In this way, extensive paperwork can be greatly saved.

Besides, blockchains can be used in green energy. Gogerty and Zitoli proposed the solarcoin (Gogerty and Zitoli 2011) to encourage the usage of renewable energies. In particular, solarcoin is a kind of digital currency rewarding solar energy producers. In addition to the usual way of getting coins through mining, solarcoins could be granted by the solarcoin foundation as long as you have generated the solar energy. Nearly 98.5 billion solarcoins were pre-mined and set aside to reward solar energy producers. It is worth noting that the solarcoin network adopts the Proof of stake time (POST) (Pike et al. 2015) rather the traditional proof of work (POW) that costs much electricity power to reach consensus. Moreover, Johnson et al. (Johnson, Gogerty, and Zitoli 2015) conducted a study on the issue that crosses over between solar engineering, network engineering and finally blockchain development and FinTech.

Blockchain also contributes to solve water crisis. The fact that diseases from unsafe water and lack basic sanitation kill more people every year than all forms of violence is cruel. Nearly 1 billion people in the world live without clean drinking water. It is happening all over the world, especially in undeveloped areas. Clean waters projects are established to aim to solve the water crisis, and they have helped almost 6.3 million people to get clean drinking water since 2006. In 2015, the clean water coin was launched and The Clean Water Coin Initiative (TCWCI) is the first ever designed and developed to be a nonprofit organization (*Clean Water Coin* 2015). People who mine the clean water blockchain and make a new transaction with clean water coin will donate 1 percent of the coins to the charity wallet. The raised money will be used to build clean water projects.

Blockchain is originally devised to enable currency transactions to be carried out in trustless environment. However, if we regard the learning and teaching process as the currency, blockchain technology can potentially be applied to the online educational market. In (Devine 2015), blockchain learning was proposed. In blockchain learning, blocks could be packed and placed into blockchain by teachers and the learning achievements could be thought as coins.

Besides, blockchain can also be used in software copyright protection. Software license validation is one of typical countermeasures to minimize software piracy and protect software copyright. In (Herbert and Litchfield 2015), Herbert and Litchfield introduced a

novel method aiming to reduce software piracy with the help of bockchain technology. Moreover, blockchain can be used to secure Internet infrastructure such as DNS and identities. For example, Namecoin (*Namecoin* 2014) is an experimental open-source technology that improves decentralization, security, censorship resistance, privacy, and speed of DNS and identities (*Namecoin* 2014).

3.4 Reputation system

Reputation is an important measure on how much the community trusts you. The greater your reputation, the more trustworthy you are regarded by others. The reputation of a person can be evaluated on his/her previous transactions and interactions with the community. There is a rising number of cheating cases of personal reputation records falsification. For example, in e-commerce, many service-providers enroll a huge number of fake customers to achieve a high reputation (i.e., sybil attack).

Blockchain can potentially solve this problem. In (Prisco 2015), a quantified reputation system was proposed to aggregate reputation data and provide trust scores for individuals and organizations. This distributed reputation system that is essentially established on blockchain can maintain consensus across hosts while supporting high transaction rates. Besides, Sharples and Domingue proposed a blockchain-based distributed system for educational record and reputation (Sharples and Domingue 2015). Moreover, Carboni (Carboni 2015) proposed a reputation model based on blockchain, in which a voucher will be signed if customer is satisfied with the service and would like to give a good feedback. After signing a voucher, a service provider needs to take extra 3 precent of the payment to the network as the voting fee to discourage the sybil attack. A service provider's reputation is calculated based on the amount of the voting fee. A successful transaction includes three output: 1) the cost of the service directed to the producer, 2) the cost directed to the validate but fake Bitcoin address that links the payment with the service; 3) the change redirected to the consumer. Furthermore, Dennis and Owen (Dennis and Owen 2015) proposed a new reputation system that is practically applicable to multiple networks. In particular, they created a new blockchain to store single dimension reputation value (i.e., 0 or 1) from the completed transactions. Take the file sharing as an example. Entity A sends a file to entity B. Upon receiving the file, B sends a transaction consists of the score, the hash of file and private key of B to verify the identity. Then, the miners contact A and B to confirm that the transation happens with no suspicion.

Blockchain can also be used to enhance the reliability of PGP (pretty good privacy), which is a kind of data encryption and decryption program to transfer information. In particular, PGP is based on a concept of web of trust (*Web of trust* 2016). In a web of trust, everyone is linked with a public key and a private key. When A sends a message to B, PGP encrypts it using B's public key. Then B decrypts the message with his private key. In this way, the privacy is enhanced since the program does not know B's public key. Wilson and Ateniese (Wilson and Ateniese 2015) propose the novel design of distributed PGP key server that leverages the blockchain to store and retrieve the certificates. As a result, the reliability of PGP system has been further improved.

3.5 Security

We have seen the proliferation of various mobile devices and various mobile services, which are also exhibiting their vulnerability to malicious nodes. For example, many malware

(malicious software) developers can easily obtain the access to valuable data in mobile phones by exploiting the system vulnerability (*The MITRE Corporation: List of common vulnerabilities and exposures for all versions of Google Android* 2014). It is reported in (Garetto, Gong, and Towsley 2003) that the newly released malwares in the public Internet is exploding. There are a number of anti-malware filters proposed to detect the suspected files through pattern matching schemes, which a central server to store and update the virus patterns. However, these centralized countermeasures are also vulnerable to malicious attackers.

Blockchain can potentially help to improve the security in distributed networks. In particular, Charles (Noyes 2016a) proposed a novel anti-malware environment named BitAV, in which users can distribute the virus patterns on blockchain. In this way, BitAV can enhance the fault tolerance. It is shown in (Noyes 2016a) that BitAV can improve the scanning speed and enhance the fault reliability (i.e., less susceptible to targeted denial-of-service attacks).

In addition to the increasing risk of the exposure of our private data to malwares, various mobile services and social network providers are collecting our sensitive data. For example, Facebook has collected more than 300 petabytes of personal data since its inception (Vagata and Wilfong 2014). Usually, the collected data are stored at central servers of service providers, which are susceptible to malicious attacks. Blockchain has the potential to improve the security of privacy sensitive data. In (Zyskind, Nathan, et al. 2015), Zyskind et al. propose a decentralized personal data management system that ensures the user ownership of their data. This system is implemented on blockchain. The system can protect the data against these privacy issues: 1) Data ownership, 2) Data transparency and auditability, 3)Fine-grained access control. A similar system based on blockchain technology was also proposed to securely distribute sensitive data in a decentralized manner in (*Ethos* 2014).

Blockchain technologies can also be used to improve the reliability of security infrastructure. For example, conventional public key infrastructures (PKIs) are often susceptible to single point of failure due to the hardware and software flaws or malicious attacks. As shown in (Axon 2015), blockchain can be used to construct a privacy-aware PKI while simultaneously improving the reliability of conventional PKIs.

Furthermore, blockchain can also enhance the security and the reliability of decentralized systems, such as cloud systems and distributed databases. For example, in Metadisk project (Wilkinson, Lowry, and Boshevski 2014), the blockchain technology is adopted to improve the security and the efficiency of a peer-to-peer cloud storage system. Besides, blockchain is also used in BigchainDB project (McConaghy et al. 2016), that is featured with the decentralized control, immutability, and scalability. BigchainDB can be used in creation and movement of digital assets. Moreover, Hardjono and Smith propose a blockchain-based system named ChainAnchor, which can commission IoT devices into a cloud system in a privacy-preserving manner. Furthermore, Xu et al. in (Xu et al. 2016) propose to use blockchain to serve as a software connector to improve security, privacy, scalability and sustainability of shared data storage systems.

4 Challenges

This section presents the challenges and recent advances in blockchain.

4.1 Challenges in blockchain

Despite the great potential of blockchain, it faces numerous challenges, which limit the wide usage of blockchain. We enumerate some of them as follows.

- *Scalability*. With the increment of transactions, the blockchain becomes bulky. For example, Bitcoin blockchain is current around 80 GB (Chuen 2015). Each node has to store all transactions to validate them on the blockchain network, which definitely limits the scalability of blockchain (Sompolinsky and Zohar 2015). Besides, due to the original restriction of block size and the time interval used to generate a new block, the Bitcoin blockchain can only process nearly 7 transactions per second (Nakamoto 2008), which can not fulfill the requirement of processing millions transactions in real-time fashion.

- *Vulnerability*. Blockchain is susceptible to attacks of colluding selfish miners. In particular, in (Eyal and Sirer 2014), Eyal and Sirer showed that the network is vulnerable even if only a small portion of the hashing power is used to cheat. Besides, the blockchain cannot eliminate any unlawful transactions if a node with machine power exceeding 51% of mining power in the whole network (NRI 2015).

- *Deficiency of exisiting consensus algorithms*. POW has been criticized for its energy wasting for meaningless hashing to compete with others (Nakamoto 2008). POS however suffers from the monopoly and the complexity while PBFT has the weakness of lacking enough incentive sources and DPOS is less decentralized and less resilient (Buterin 2014) .

- *Tendency to centralization*. Blockchain is essentially designed to decentralize the system. However, there is a trend that miners tend to be centralized in the pool, which is invented to ensure the steady income for each miner and consequently attacks a large number of miners (NRI 2015). Besides, the emergence of private blockchains also results in blockchain centralization, i.e., the monopoly of blockchain by big firms, which essentially violates the motivation of blockchain (Christidis and Devetsikiotis 2016).

- *Privacy Leakage*. Blockchain can preserve a certain amount of privacy through the public key (an address for each entity). However, it is shown in (Meiklejohn et al. 2013; Kosba et al. 2016) that blockchain cannot guarantee the *transactional privacy* since the values of all transactions and balances for each (pseudonymous) public key are publicly visible. Besides, the recent study (Barcelo 2014) has shown that a user's Bitcoin transactions can be linked to reveal user's information. Moreover, Biryukov et al. presented an method to link user pseudonyms to IP addresses even when users are behind NATs or firewalls (Biryukov, Khovratovich, and Pustogarov 2014).

The above challenges are hindering the blockchain development and need to be addressed. We next present an overview on the recent advances in blockchain.

4.2 Recent advances

Improvements on scalability

There are a number of efforts proposed to address the scalability of blockchain. We roughly categorize the countermeasures into two types:

- *Storage optimization of blockchain*. In particular, Bruce proposed a novel cryptocurrency scheme, in which the old transaction records are removed (or forgotten) by the network (Bruce 2014). Besides, a novel schem named VerSum was proposed in (Hooff, Kaashoek, and Zeldovich 2014) to provide another way allowing lightweight clients to exist since they can outsource expensive computations over large inputs. Moreover, (Tsai et al. 2016) proposed a novel blockchain architecture, in which conventional blockchains are divided into two groups: one group of blockchains is used to store transactional information and another group is used to store account information. In this way, the storage of the whole system is optimized and consequently improving the scalability of blockchain.

- *Redesigning blockchain*. In (Eyal et al. 2016), Bitcoin-NG (Next Generation) was proposed. The main idea of Bitcoin-NG is to decouple conventional block into two parts: key block for leader election and microblock to store transactions. In this way, Bitcoin-NG can significantly reduce the delay and improve the capacity.

Advances on consensus protocols

A good consensus protocol means efficiency, safty and convenience. Recently, a number of endeavors have been made to improve consensus protocol in blockchain. In particular, Luu et al. designed a new computationally-scalable Byzantine consensus protocol (named SCP) for blockchains. Chepurnoy et al. presented a new consensus protocol for peer-to-peer blockchain system, in which anyone who provides non-interactive proofs of retrievability for the past state snapshots is agreed to generate the block(Chepurnoy, Larangeira, and Ojiganov 2016). Besides, Kraft proposed a new consensus method to ensure that a block is generated in a relatively stable speed(Kraft 2016). Moreover, inspired by POS, Pike et al. proposed a new consensus algorithm named proof of stake time (POST), which is a time-accepted nonlinear consensus algorithm (Pike et al. 2015). Most recently, PeerCensus (Decker, Seidel, and Wattenhofer 2016) was proposed to reduce the confirmation time of a transaction. The main idea of PeerCensus is to decouple block creation and transaction confirmation so that the consensus speed can be significantly increased.

The performance analysis of blockchain consensus protocols is also challenging. In particular, Pass et al. proved in (Pass, Tech, and Seeman 2016) that the blockchain consensus approach satisfies the strong consistency and maintains liveness asynchronously. A novel framework was introduced in (Kiayias and Panagiotakos 2016) to analyze blockchain protocols. Besides, Kiayias et al. (Kiayias and Panagiotakos 2015) provided a formal security proof of the Greedy Heaviest-Observed Sub-Tree (GHOST) rule that was first proposed in (Sompolinsky and Zohar 2015) is an alternative to the longest chain in Bitcoin. They also investigated the tradeoff between the provable security and transaction processing speed in (Kiayias and Panagiotakos 2015). Longo et al. provided an analysis of Business Information eXchange (BIX) protocol from the point of view of security (Longo et al. 2016).

Approaches to improve privacy and security

Recall that blockchain is vulnerable to disclose the privacy. There are a number of efforts proposed to improve the anonymity of blockchain. For example, Heilman et al. proposed a solution based on the micro-payment channel to achieve anonymity and fairness (Heilman, Baldimtsi, and Goldberg 2016). The micro-payment channel is implemented via blind signature and smart contract. Besides, CoinParty (Ziegeldorf et al. 2015) was proposed to ensure a secure environment, which is achieved through the integration of decryption mix networks (mixnets) with threshold signatures.

Besides, there are some advances in enhancing the vulnerability of blockchain. For example, Göbel et al. proposed a markov chain model to detect selfish miners (Göbel et al. 2015). Besides, Kiayias et al. considered two simplified mining games and found that a miner deviates from the expected behavior when it has higher computational power. In addition to detect selfish miners, there are some approaches proposed to solve the security problem. For example, Shultz proposed a method named proof of witness to eliminate block-withholding attacks (Shultz 2015). Moreover, Luu et al. identified the problem that miners failing to verify are vulnerable to attack and proposed a novel solution to this problem (Luu et al. 2015).

4.3 Future directions

Blockchain can potentially disrupt existing industries and create an economy model (Lundy 2016). We enumerate some of future directions in blockchain.

- *Application of blockchain in sharing economy.* One of benefits of blockchain is the decentralization. Eliminating the need for an intermediary agent will definitely improve the efficiency and save the cost of transactions. As a result, blockchain is a catalyst for sharing economy. Instead of using eBay, Taobao, Uber and Airbnb to connect with other people, new services based on blockchain technologies allow individuals to connect and transact directly, which can greatly save the cost (Lundy 2016). For example, Arcade City (*Arcade City Project* 2016), a ridesharing startup offers an open marketplace where riders connect directly with drivers by leveraging blockchain technology.

- *Application of blockchain in healthcare.* Healthcare becomes one of the major social problems and the economic problems. On the other hand, the proliferation of various wearable healthcare devices, such as smart bracelets, hair caps and smart watches, leads to the availability of the remote health care services at home or at clinic, which can potentially release the burden of the hospital resources (Zhang et al. 2015; Wang et al. 2016). The e-health devices can continuously measure their physiology information, such as heart beat rate, blood pressure, blood sugar etc. The e-health data shall be stored in blockchains so that they can be tractable and analyzed by medical doctors while the privacy can be preserved.

- *Big data analytics in blockchain.* To conduct data analysis in blockchain data is necessary due to the following reasons: (i) it can help to identify nefarious users; (ii) it can be helpful to fraud detection (e.g., identify money-laundering transactions); (iii) it can help to detect the faults of IoT devices; (iv) it can be beneficial to extract the valuable information from blockchain data. However, it is quite challenging to conduct data analysis in blockchain because of extensive volume of data (i.e., big data), real-time data generation and data anonymity (i.e., only the two entities of a transaction know each other's identifier). Therefore, novel big data analytical methods are expected to solve the above concerns in blockchain data.

5 Conclusion

In this paper, we present a comprehensive survey on blockchain. We first give an overview of blockchain technologies including blockchain architecture, consensus protocols, key

characteristics of blockchain and taxonomy of blockchain systems. We then discuss various applications of blockchain including financial and business services, IoT, public services, reputation system to security application. However, there are still a number of research challenges in this area that need extensive efforts to further improve blockchain. In summary, we believe that the evolvement of blockchain will definitely change our existing industries and create numerous opportunities in the near future.

Acknowledgement

The work described in this paper was supported by the National Key Research and Development Program (2016YFB1000101), the National Natural Science Foundation of China under (61472338), the Fundamental Research Funds for the Central Universities and Macao Science and Technology Development Fund under Grant No. 096/2013/A3. The authors would like to thank Gordon K.-T. Hon for his constructive comments.

References

Akins, Benjamin W., Jennifer L. Chapman, and Jason M. Gordon (2013). "A Whole New World: Income Tax Considerations of the Bitcoin Economy". In: *Pittsburgh Tax Review*.

Antshares Digital Assets for Everyone (2016). https://www.antshares.org.

Arcade City Project (2016). http://arcade.city/.

Atzori, Luigi, Antonio Iera, and Giacomo Morabito (2010). "The Internet of Things: A survey". In: *Computer Networks* 54.15, pp. 2787 –2805.

Axon, Louise (2015). "Privacy-awareness in blockchain-based PKI". In: *Cdt technical paper series*.

Barcelo, Jaume (2014). *User Privacy in the Public Bitcoin Blockchain*. Tech. rep. Universitat Pompeu Fabra.

Biryukov, Alex, Dmitry Khovratovich, and Ivan Pustogarov (2014). "Deanonymisation of clients in Bitcoin P2P network". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, pp. 15–29.

Blockchain 2.0 - Let a Thousand Chains Blossom (2014). https://letstalkbitcoin.com/blockchain-2-0-let-a-thousand-chains-blossom.

Bruce, JD (2014). *The mini-blockchain scheme*. Tech. rep.

bubi (2016). http://www.bubi.cn/.

Buterin, Vitalik (2014). *Slasher Ghost, and Other Developments in Proof of Stake*. https://blog.ethereum.org/2014/10/03/slasher-ghost-developments-proof-stake/.

— (2015). *On Public and Private Blockchains*. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

Carboni, Davide (2015). "Feedback based Reputation on top of the Bitcoin Blockchain". In: *arXiv preprint arXiv:1502.01504*.

Castro, Miguel, Barbara Liskov, et al. (1999). "Practical Byzantine fault tolerance". In: *OSDI*. Vol. 99, pp. 173–186.

Chepurnoy, Alexander, Mario Larangeira, and Alexander Ojiganov (2016). "A Prunable Blockchain Consensus Protocol Based on Non-Interactive Proofs of Past States Retrievability". In: *arXiv preprint arXiv:1603.07926*.

Christidis, K. and M. Devetsikiotis (2016). "Blockchains and Smart Contracts for the Internet of Things". In: *IEEE Access* 4, pp. 2292–2303.

Chuen, David Lee Kuo, ed. (2015). *Handbook of Digital Currency*. San Diego: Academic Press. ISBN: 978-0-12-802117-0.

Clean Water Coin (2015). `http://www.cleanwatercoin.org/`.

Coeckelbergh, Mark and Wessel Reijers (2016). "Cryptocurrencies as narrative technologies". In: *ACM SIGCAS Computers and Society* 45.3, pp. 172–178.

Crypto-Currency Market Capitalizations (2016). `https://coinmarketcap.com`.

Decker, Christian, Jochen Seidel, and Roger Wattenhofer (2016). "Bitcoin meets strong consistency". In: *Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN)*. ACM, p. 13.

Delegated Proof of Stake (DPOS) vs Proof of Work (POW) (2015). `http://bytemaster.github.io/bitshares/2015/01/04/Delegated-Proof-of-Stake-vs-Proof-of-Work/`.

Dennis, Richard and Gareth Owen (2015). "Rep on the block: A next generation reputation system based on the blockchain". In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, pp. 131–138.

Devine, Peter (2015). "Blockchain learning: can crypto-currency methods be appropriated to enhance online learning?" In: *ALT Online Winter Conference*.

Dixon, Colin et al. (2012). "An Operating System for the Home". In: *NSDI*. USENIX.

Ethos (2014). `http://viral.media.mit.edu/projects/ethos/`.

Eyal, Ittay and Emin Gün Sirer (2014). "Majority is not enough: Bitcoin mining is vulnerable". In: *International Conference on Financial Cryptography and Data Security*. Springer, pp. 436–454.

Eyal, Ittay et al. (2016). "Bitcoin-NG: A scalable blockchain protocol". In: *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, pp. 45–59.

Fan, Zhong et al. (2013). "Smart grid communications: overview of research challenges, solutions, and standardization activities". In: *IEEE Communications Surveys and Tutorials* 15.1, pp. 21–38.

Foroglou, George and Anna-Lali Tsilidou (2015). "Further applications of the blockchain". In: *12th Student Conference on Managerial Science and Technology*.

Garetto, Michele, Weibo Gong, and Don Towsley (2003). "Modeling malware spreading dynamics". In: *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*. Vol. 3. IEEE, pp. 1869–1879.

Gerstl, David S (2016). "Leveraging Bitcoin Blockchain Technology to Modernize Security Perfection Under the Uniform Commercial Code". In: *International Conference of Software Business*. Springer, pp. 109–123.

Göbel, Johannes et al. (2015). "Bitcoin Blockchain Dynamics: the Selfish-Mine Strategy in the Presence of Propagation Delay". In: *arXiv preprint arXiv:1505.05343*.

Gogerty, Nick and Joseph Zitoli (2011). "DeKo: An electricity-backed currency proposal". In: *Social Science Research Network*.

Habib, Kashif, Arild Torjusen, and Wolfgang Leister (2015). "Security Analysis of a Patient Monitoring System for the Internet of Things in eHealth". In: *The Seventh International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED)*.

Hardjono, Thomas and Ned Smith (2016). "Cloud-Based Commissioning of Constrained Devices using Permissioned Blockchains". In: *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*. ACM, pp. 29–36.

Heilman, Ethan, Foteini Baldimtsi, and Sharon Goldberg (2016). "Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions". In: *Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN, VOTING, and WAHC*. Berlin, Heidelberg: Springer, pp. 43–60.

Herbert, Jeff and Alan Litchfield (2015). "A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology". In: *Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015)*. Vol. 27, p. 30.

Hooff, Jelle van den, M Frans Kaashoek, and Nickolai Zeldovich (2014). "Versum: Verifiable computations over large public logs". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, pp. 1304–1316.

Hyperledger Project (2015). `https://www.hyperledger.org/`.

IBM (2015). *IBM ADEPT Practictioner Perspective - Pre Publication Draft*.

IBM Blockchain (2016). `http://www.ibm.com/blockchain/`.

"ISO/IEC 18000" (2013). In: URL: `http://en.wikipedia.org/wiki/ISO/IEC\_18000`.

Jaag, Christian, Christian Bach, et al. (2016). *Blockchain Technology and Cryptocurrencies: Opportunities for Postal Financial Services*. Tech. rep.

Johnson, Don and Scott Menezes Alfredand Vanstone (2001). "The Elliptic Curve Digital Signature Algorithm (ECDSA)". In: *International Journal of Information Security* 1.1, pp. 36–63.

Johnson, Luke Patrick, Nick Gogerty, and Joseph Zitoli (2015). "Connecting the Blockchain to the Sun to Save the Planet". In: *Social Science Research Network*.

Kiayias, Aggelos and Giorgos Panagiotakos (2015). *Speed-Security Tradeoffs in Blockchain Protocols*. Tech. rep. IACR: Cryptology ePrint Archive.

— (2016). "On Trees, Chains and Fast Transactions in the Blockchain". In: URL: `https://eprint.iacr.org/2016/545.pdf`.

King, Sunny and Scott Nadal (2012). "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake". In: *self-published paper, August* 19.

Kosba, Ahmed et al. (2016). "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts". In: *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 839–858.

Kraft, Daniel (2016). "Difficulty control for blockchain-based consensus systems". In: *Peer-to-Peer Networking and Applications* 9.2, pp. 397–413.

Lamport, Leslie, Robert Shostak, and Marshall Pease (1982). "The Byzantine generals problem". In: *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4.3, pp. 382–401.

Longo, Riccardo et al. (2016). "On the security of the Blockchain Bix Protocol and Certificates". In: *arXiv preprint arXiv:1607.08401*.

Lundy, Lawrence (2016). *Blockchain and the sharing economy 2.0*.

Luu, Loi et al. (2015). "Demystifying incentives in the consensus computer". In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, pp. 706–719.

Malinova, Katya and Andreas Park (2016). "Market Design for Trading with Blockchain Technology". In: *Social Science Research Network*.

Mattila, Juri (2016). *THE BLOCKCHAIN PHENOMENON*. Tech. rep. BRIE Working Paper 2016-1, UC Berkeley.

McConaghy, Trent et al. (2016). "BigchainDB: A Scalable Blockchain Database". In:

Meiklejohn, Sarah et al. (2013). "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names". In: *Proceedings of the 2013 Conference on Internet Measurement Conference (IMC'13)*.

Micheler, Eva and Luke von der Heyde (2016). "Holding, Clearing and Settling Securities Through Blockchain Technology Creating an Efficient System by Empowering Asset Owners". In: *Social Science Research Network*.

Microsoft Azure: Blockchain as a Service (2016). `https://azure.microsoft.com/en-us/solutions/blockchain/`.

Miorandi, Daniele et al. (2012). "Internet of things: Vision, applications and research challenges". In: *Ad Hoc Networks* 10.7, pp. 1497 –1516. ISSN: 1570-8705.

Morini, Massimo (2016). "From'Blockchain Hype'to a Real Business Case for Financial Markets". In: *Social Science Research Network*.

Nakamoto, Satoshi (2008). *Bitcoin: A peer-to-peer electronic cash system*.

Namecoin (2014). `https://www.namecoin.org/`.

Norta, Alex, Anis Ben Othman, and Kuldar Taveter (2015). "Conflict-Resolution Lifecycles for Governed Decentralized Autonomous Organization Collaboration". In: *Proceedings of the 2015 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia*. ACM, pp. 244–257.

Noyes, Charles (2016a). "BitAV: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning". In: *arXiv preprint arXiv:1601.01405*.

— (2016b). *Efficient Blockchain-Driven Multiparty Computation Markets at Scale*. Tech. rep. URL: `https://www.overleaf.com/articles/blockchain-multiparty-computation-markets-at-scale/mwjgmsyybxvw/viewer.pdf`.

NRI (2015). *Survey on Blockchain Technologies and Related Services*. Tech. rep.

Pass, Rafael, Cornell Tech, and Lior Seeman (2016). "Analysis of the Blockchain Protocol in Asynchronous Networks". In:

Peters, Gareth William and Efstathios Panayi (2015). "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money". In: *Social Science Research Network*.

Peters, Gareth William, Efstathios Panayi, and Ariane Chapelle (2015). "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective". In: *Social Science Research Network*.

Pike, Douglas et al. (2015). "Proof-of-Stake-Time". In: *POST White Paper*.

Pilkington, Marc (2016a). "Blockchain technology: principles and applications". In: *Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar*.

— (2016b). "Does the Fintech Industry Need a New Risk Management Philosophy? A Blockchain Typology for Digital Currencies and e-money Services in Luxembourg". In: *Social Science Research Network*.

Prisco, G (2015). *The World Table Launches a Quantified Reputation System*. URL: `https://bitcoinmagazine.com/articles/world-table-launches-quantified-reputation-system-1431633676`.

Sharples, Mike and John Domingue (2015). "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward". In: *Proceedings of 11th*

European Conference on Technology Enhanced Learning (EC-TEL 2015). Springer, pp. 490–496.

Shrier, David, Weige Wu, and Alex Pentland (2016). *Blockchain & Infrastructure (Identity, Data Security)*. Tech. rep. URL: http://cdn.resources.getsmarter.ac/wp-content/uploads/2016/05/MIT_Blockchain_Infrastructure_Report_Part_Three_May_2016.pdf.

Shultz, Brian L. (2015). *Certification of Witness: Mitigating Blockchain Fork Attacks*. Tech. rep. URL: http://www.bshultz.com/uploads/7/3/8/7/73876901/shultz_thesis_2016_02_24.pdf.

Sompolinsky, Yonatan and Aviv Zohar (2015). "Secure high-rate transaction processing in Bitcoin". In: *International Conference on Financial Cryptography and Data Security*. Springer, pp. 507–527.

State of Blockchain Q1 2016: Blockchain Funding Overtakes Bitcoin (2016). http://www.coindesk.com/state-of-blockchain-q1-2016/.

Szabo, Nick (2004). "The idea of smart contracts". In: *IEEE International Workshop on Electronic Contracting (WEC),*

taiyiyun (2016). https://taiyiyun.com/.

The MITRE Corporation: List of common vulnerabilities and exposures for all versions of Google Android (2014). http://www.cvedetails.com/product/19997/Google-Android.html?vendor\id=1224/.

Trautman, Lawrence J (2016). "Is Disruptive Blockchain Technology the Future of Financial Services?" In: *The Consumer Finance Law Quarterly Report (forthcoming)*.

Tsai, Wei-Tek et al. (2016). "A System View of Financial Blockchains". In: *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*. IEEE, pp. 450–457.

Tschorsch, F. and B. Scheuermann (2016). "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies". In: *IEEE Communications Surveys Tutorials* 18.3, pp. 2084–2123.

Vagata, Pamela and Kevin Wilfong (2014). *Scaling the Facebook data warehouse to 300 PB*. Tech. rep. URL: https://code.facebook.com/posts/229861827208629/scaling-the-facebook-data-warehouse-to-300-pb/.

Vasin, Pavel (2014). *Blackcoin's proof-of-stake protocol v2*. Tech. rep. URL: http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf.

Vukolić, Marko (2015). "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication". In: *International Workshop on Open Problems in Network Security*. Springer, pp. 112–125.

Wang, Hao et al. (2015). "Big Data and Industrial Internet of Things for the Maritime Industry in Northwestern Norway". In: *IEEE Region 10 Conference (TENCON)*.

Wang, K. et al. (2016). "Mobile big data fault-tolerant processing for ehealth networks". In: *IEEE Network* 30.1, pp. 36–42.

Web of trust (2016). https://en.wikipedia.org/wiki/Web_of_trust.

Wilkinson, Shawn, Jim Lowry, and Tome Boshevski (2014). *Metadisk a blockchain-based decentralized file storage application*. Tech. rep. Technical Report. http://metadisk.org/metadisk. pdf.

Wilson, Duane and Giuseppe Ateniese (2015). "From Pretty Good to Great: Enhancing PGP Using Bitcoin and the Blockchain". In: *International Conference on Network and System Security*. Springer, pp. 368–375.

Wood, Gavin (2014). “Ethereum: A secure decentralised generalised transaction ledger”. In: *Ethereum Project Yellow Paper*.

Xu, Xiwei et al. (2016). “The blockchain as a software connector”. In: *Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*.

Zhang, K. et al. (2015). “Security and privacy for mobile healthcare networks: from a quality of protection perspective”. In: *IEEE Wireless Communications* 22.4, pp. 104–112.

Zhang, Yu and Jiangtao Wen (2015). “An IoT electric business model based on the protocol of BitCoin”. In: *Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on*. IEEE, pp. 184–191.

Ziegeldorf, Jan Henrik et al. (2015). “Coinparty: Secure multi-party mixing of bitcoins”. In: *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*. ACM, pp. 75–86.

Zyskind, Guy, Oz Nathan, et al. (2015). “Decentralizing privacy: Using blockchain to protect personal data”. In: *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE, pp. 180–184.