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

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

Xiangping Chen

Institute of Advanced Technology, National Engineering Research Center of Digital Life,
Sun Yat-sen University,
Guangzhou, China
E-mail: chenxp8@mail.sysu.edu.cn
*Corresponding author

Huaimin Wang

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

Abstract:

Blockchain has numerous benefits such as decentralization, persistency, anonymity and auditability. There is a wide spectrum of blockchain applications ranging from cryptocurrency, financial services, risk management, Internet of Things to public and social services. Although a number of studies focus on using the blockchain technology in various application aspects, there is no comprehensive survey on the blockchain technology in both technological and application perspectives. To fill this gap, we conduct a comprehensive survey on the blockchain technology. In particular, this paper gives the blockchain taxonomy, introduces typical blockchain consensus algorithms, reviews blockchain applications and discusses technical challenges as well as recent advances in tackling the challenges. Moreover, this paper also points out the future directions in the blockchain technology.

Keywords: Blockchain; Consensus Algorithms; Cryptocurrency; Internet of Things; Smart Contract

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 blockchain, 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.

Xiangping Chen is a research associate at Sun Yat-sen University, Guangzhou, China. She received Ph.D. degree from Peking University in 2010. Her research interests include data-driven software engineering, program comprehension, and web engineering.

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 attracted 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 [11]. The *blockchain* is the core mechanism for the Bitcoin. Blockchain was first proposed in 2008 and implemented in 2009 [60]. Blockchain can be regarded as a public ledger, in which all committed

transactions are stored in a chain of blocks. This chain continuously grows when new blocks are appended to it. The blockchain technology has the key characteristics, such as decentralization, persistency, anonymity and auditability. Blockchain can work in a decentralized environment, which is enabled by integrating several core technologies such as cryptographic hash, digital signature (based on asymmetric cryptography) and distributed consensus mechanism. With blockchain technology, a transaction can take place in a decentralized fashion. As a result, blockchain can greatly save the cost and improve the efficiency.

Although Bitcoin is one of the most famous blockchain applications, blockchain can be applied into diverse applications far beyond cryptocurrencies. Since it allows payment to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment [35, 69]. Additionally, blockchain technology is becoming one of the most promising technologies for the next generation of Internet interaction systems, such as smart contracts [46], public services [13], Internet of Things (IoT) [86], reputation systems [75] and security services [63].

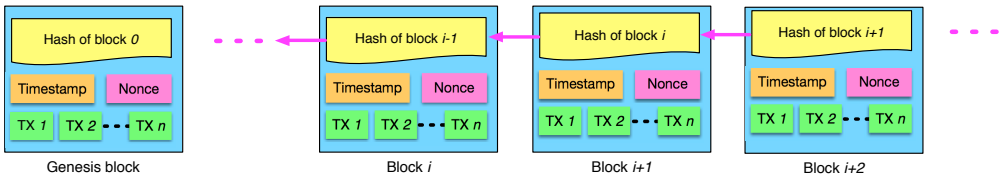
Despite the fact that the blockchain technology has great potential for the construction of the future Internet systems, it is facing a number of technical challenges. Firstly, scalability is a huge concern. Bitcoin block size is limited to 1 MB now and a block is mined about every ten minutes. Subsequently, the Bitcoin network is restricted to a rate of 7 transactions per second, which is incapable of dealing with high frequency trading. However, larger blocks means larger storage space and slower propagation in the network. This will lead to centralization gradually as users would like to maintain such a large blockchain. Therefore the tradeoff between block size and security has become a challenge. Secondly, it has been proved that miners can achieve larger revenue than their fair share through selfish mining strategy [33]. Miners hide their mined blocks for more revenue in the future. In that way, branches can take place frequently; this hinders blockchain development. Hence some solutions need to be put forward to fix this problem. Moreover, it has been shown that privacy leakage can also happen in blockchain even when users only make transactions with their public key and private key [19]. User's real IP address can even be tracked . Furthermore, current consensus algorithms like *proof of work* or *proof of stake* are facing some serious problems. For example, proof of work wastes too much electricity energy while the phenomenon that the rich get richer can appear in the proof of stake consensus process. These challenges need to be addressed quickly for blockchain technology development.

There is a substantial body of literature on blockchain from various sources, such as blogs, wikis, forum posts, codes, conference proceedings and journal articles. Tschorsch et al. [79] made a technical survey about decentralized digital currencies including Bitcoin. Compared with [79], our paper focuses on blockchain technology instead of digital currencies. Nomura Research Institute made a technical report about blockchain [65]. Contrast to [65], our paper focuses on state-of-art blockchain researches including recent advances and future trends. This paper is an extended version of the work published in [87] with the substantial extensions on blockchain technical details, consensus algorithms, applications of blockchains, research challenges and future directions.

The rest of this paper is organized as follows. Section 2 introduces blockchain architecture. Section 3 shows typical consensus algorithms used in blockchain. Section 4 introduces several typical blockchain applications. Section 5 summarizes the technical challenges and the recent advances in this area. Section 6 discusses some possible future directions and Section 7 concludes the paper.

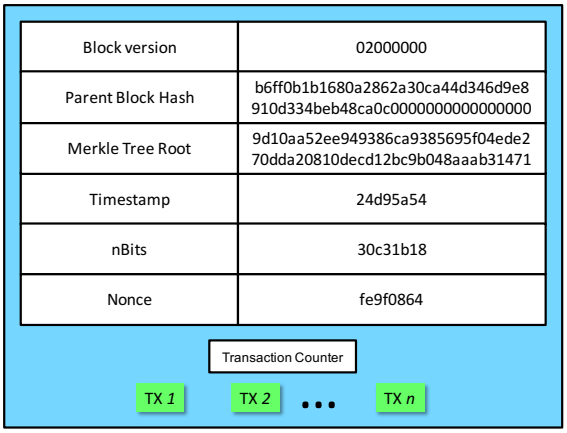
2 Blockchain architecture

Figure 1 An example of blockchain which consists of a continuous sequence of blocks.



Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger [50]. Figure 1 illustrates an example of 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. It is worth noting that *uncle blocks* (children of the block's ancestors) hashes will also be stored in ethereum blockchain [23]. The first block of a blockchain is called *genesis block* which has no parent block. We then introduce the block structure in section 2.1, digital signature mechanism in section 2.2. We also summarize blockchain key characteristics in section 2.3. Blockchain taxonomy is showed in section 2.4.

Figure 2 Block structure



2.1 Block

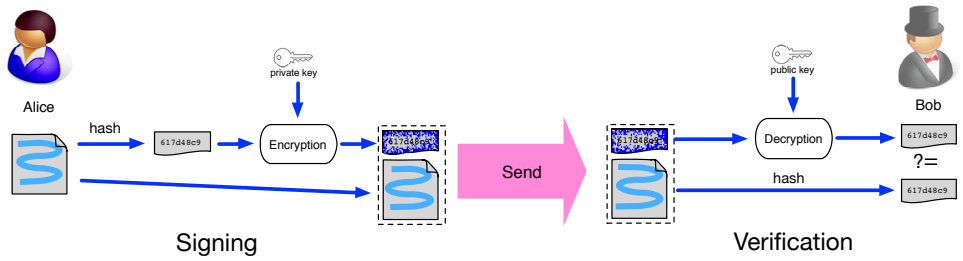
A block consists of the *block header* and the *block body* as shown in Figure 2. In particular, the block header includes:

(i) Block version: indicates which set of block validation rules to follow.
(ii) Parent block hash: a 256-bit hash value that points to the previous block.
(iii) Merkle tree root hash: the hash value of all the transactions in the block.
(iv) Timestamp: current timestamp as seconds since 1970-01-01T00:00 UTC.
(v) nBits: current hashing target in compact format.
(vi) Nonce: an 4-byte field, which usually starts with 0 and increases for every hash calculation (will be explained in details in Section 3).

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions [65]. Digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature.

2.2 *Digital Signature*

Figure 3 Digital Signature used in blockchain



Each user owns a pair of private key and public key. The private key 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 and sends to another user Bob the encrypted hash with the original data. 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 function as Alice's. The typical digital signature algorithms used in blockchains include elliptic curve digital signature algorithm (ECDSA) [43].

2.3 *Key Characteristics of Blockchain*

In summary, blockchain has 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.

Table 1 Comparisons among *public blockchain*, *consortium blockchain* and *private blockchain*

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

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 is nearly impossible to tamper. Additionally, each broadcasted block will be validated by other nodes and transactions will be checked. So any falsification will be detected easily.
- *Anonymity.* Each user can interact with the blockchain network with a generated address. Further, an user will generate many addresses to avoid identity exposure. There is no longer any central party keeping users' private information. 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 5).
- *Auditability.* Since each of the transactions on the blockchain is validated and recorded with a timestamp, users can easily verify and trace the previous records through accessing any node in the distributed network. In Bitcoin blockchain, each transaction can be traced to previous transactions iteratively. It improves the traceability and the transparency of the data stored in the blockchain.

2.4 Taxonomy of blockchain systems

Current blockchain systems can be roughly categorized into three types: public blockchain, private blockchain and consortium blockchain [24]. We compare these three types of blockchain from different perspectives. The comparison is listed in Table 1.

- *Consensus determination.* In public blockchain, each node can take part in the consensus process. And only a selected set of nodes are responsible for validating the block in consortium blockchain. As for private chain, it is fully controlled by one organization who can determine the final consensus.

- *Read permission*. Transactions in a public blockchain are visible to the public while the read permission depends on a private blockchain or a consortium blockchain. The consortium or the organization can decide whether the stored information is public or restricted.
- *Immutability*. Since transactions are stored in different nodes in the distributed network, so it is nearly impossible to tamper the public blockchain. However, if the majority of the consortium or the dominant organization wants to tamper the blockchain, the consortium blockchain or private blockchain can be reversed or tampered.
- *Efficiency*. It takes plenty of time to propagate transactions and blocks as there are a large number of nodes on public blockchain network. Taking network safety into consideration, restrictions on public blockchain will be much more strict. As a result, transaction throughput is limited and the latency is high. With fewer validators, consortium blockchain and private blockchain can be more efficient.
- *Centralized*. The main difference among the three types of blockchains is that public blockchain is decentralized, consortium blockchain is partially centralized and private blockchain is fully centralized as it is controlled by a single group.
- *Consensus process*. Everyone in the world can join the consensus process of the public blockchain. Different from public blockchain, both consortium blockchain and private blockchain are permissioned. One node needs to be certificated to join the consensus process in consortium or private blockchain.

Since public blockchain is open to the world, it can attract many users. Communities are also very active. Many public blockchains emerge day by day. As for consortium blockchain, it can be applied to many business applications. Currently Hyperledger [7] is developing business consortium blockchain frameworks. Ethereum also has provided tools for building consortium blockchains [3]. As for private blockchain, there are still many companies implementing it for efficiency and auditability.

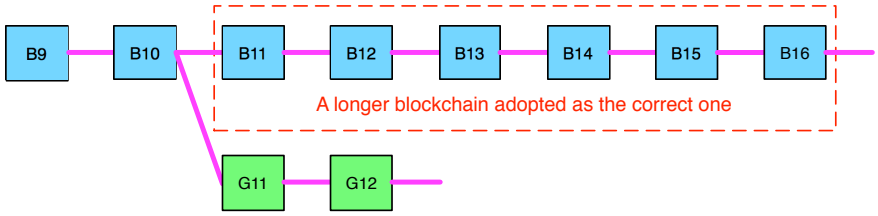
3 Consensus Algorithms

In blockchain, how to reach consensus among the untrustworthy nodes is a transformation of the Byzantine Generals (BG) Problem [49]. In BG problem, a group of generals who command a portion of Byzantine army circle the city. The attack would fail if only part of the generals attack the city. Generals need to communicate to reach an agreement on whether attack or not. However, there might be traitors in generals. Traitor can send different decisions to different generals. This is an trustless environment. How to reach a consensus in such an environment is a challenge. It is also a challenge for blockchain as the blockchain network is distributed. In blockchain, there is no central node that ensures ledgers on distributed nodes are all the same. Nodes need not trust other nodes. Thus, some protocols are needed to ensure that ledgers in different nodes are consistent. We next present several common approaches to reach consensus in blockchain.

3.1 Approaches to consensus

PoW (Proof of work) is a consensus strategy used in Bitcoin network [60]. POW requires a complicated computational process in the authentication. In POW, each node of the network

Figure 4 An scenario of blockchain branches (the longer branch will be admitted as the main chain while the shorter one will be deserted)



is calculating a hash value of the constantly changing block header. 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 will 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 that calculate the hashes are called *miners* and the POW procedure is called *mining*. 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 [60].

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 4. 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 4 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, after a certain number of new blocks are appended to the blockchain, it is nearly impossible to reverse the blockchain to tamper the transactions. In Bitcoin blockchain, 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 4). Block interval depends on different parameter setting. Bitcoin block is generated about every 10 minutes while Ethereum block is generated about every 17 seconds.

Miners have to do a lot of computer calculations in PoW, yet these works waste too much resources. To mitigate the loss, some PoW protocols in which works can have some side-applications have been designed. For example, Primecoin [44] searches for special prime number chains which can be used for mathematical research. Instead of burning electricity for mining the POW block, proof of burn [67] asks miners to send their coins to addresses where they can not be redeemed. By burning coins, miners get chances for mining blocks and they don't need powerful hardwares as POW.

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 will be less likely to attack the network. Since the selection based on account balance is quite unfair because

the single richest person is bound to be dominant in the network. As a result, many solutions are proposed with the combination of the stake size to decide which one to forge the next block. In particular, Blackcoin [81] uses randomization to predict the next generator. It uses a formula that looks for the lowest hash value in combination with the size of the stake. Peercoin [45] favors coin age based selection. In Peercoin, older and larger sets of coins have a greater probability of mining the next block. Compared with PoW, PoS saves more energy and is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequence. Many blockchains adopt PoW at the beginning and transform to PoS gradually. For instance, Ethereum is planing to move from Ethash (a kind of PoW)[84] to Casper (a kind of PoS) [85]. To combine the benefits of POW and POS, proof of activity [17] is proposed. In proof of activity, a mined block needs to be signed by N miners to be valid. In that way, if some owner of 50% of all coins exists, he cannot control creation of new blocks on his own. Sometimes stake can be other things, for example, in proof of capacity [22], miners have to allocate large hard drive space to mine the block.

PBFT (Practical byzantine fault tolerance) is a replication algorithm to tolerate byzantine faults [56]. Hyperledger Fabric [7] utilizes the PBFT as its consensus algorithm since PBFT can handle up to 1/3 malicious byzantine replicas. A new block is determined in a round. In each round, a *primary* will be selected according to some rules. And it is responsible for ordering the transaction. The whole process can be divided into three phase: *pre-prepared*, *prepared* and *commit*. In each phase, a node will enter next phase if it has received votes from over 2/3 of all nodes. So PBFT requires that every node is known to the network . Like PBFT, Stellar Consensus Protocol (SCP) [52] is also a Byzantine agreement protocol. There is no hashing procedure in PBFT. In PBFT, each node has to query other nodes while SCP gives participants the right to choose which set of other participants to believe. Based on PBFT, Antshares [8] has implemented their dBFT (delegated byzantine fault tolerance). In dBFT, some professional nodes are voted to record the transactions instead of all nodes.

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 can be confirmed quickly, making the transactions confirmed quickly. Meanwhile, the parameters of the network such as block size and block intervals can be tuned. Additionally, users do not to need worry about the dishonest delegates because the delegates can be voted out easily. DPOS has already been implemented, and is the backbone of Bitshares [2].

Ripple [74] is a consensus algorithm that utilizes collectively-trusted subnetworks within the larger network. In the network, nodes are divided into two types: *server* for participating consensus process and *client* for only transferring funds. In contrast to that PBFT nodes have to ask every node in the network, each Ripple server has an Unique Node List (UNL) to query. UNL is important to the server. When determining whether to put a transaction into the ledger, the server will query the nodes in UNL. If the received agreements have reached 80%, the transaction will be packed into the ledger. For a node, the ledger will remain correct as long as the percentage of faulty nodes in UNL is less than 20%.

Tendermint [48] is a byzantine consensus algorithm. A new block is determined in a round. A proposer will be selected to broadcast an unconfirmed block in this round. So all nodes need to be known for proposer selection. It can be divided into three steps: 1)

Prevote step. Validators choose whether to broadcast a prevote for the proposed block. 2) *Precommit step*. If the node has received more than 2/3 of prevotes on the proposed block, it broadcasts a precommit for that block. If the node has received over 2/3 of precommits, it enters the commit step. 3) *Commit step*. The node validates the block and broadcasts a commit for that block. if the node has received 2/3 of the commits, it accepts the block. The process is quite similar to PBFT, but Tendermint nodes have to lock their coins to become validators. Once a validator is found to be dishonest, it will be punished.

3.2 Consensus algorithms comparison

Table 2 Typical Consensus Algorithms Comparison

Property	**PoW**	**PoS**	**PBFT**	**DPOS**	**Ripple**	**Tendermint**
Node identity management	open	open	permissioned	open	open	permissioned
Energy saving	no	partial	yes	partial	yes	yes
Tolerated power of adversary	$< 25\%$ computing power	$< 51\%$ stake	$< 33.3\%$ faulty replicas	$< 51\%$ validators	$< 20\%$ faulty nodes in UNL	$< 33.3\%$ byzantine voting power
Example	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares	Ripple	Tendermint

Different consensus algorithms have different advantages and disadvantages. Table 2 gives a comparison between different consensus algorithms and we use the properties given by [82].

- *Node identity management*. PBFT needs to know the identity of each miner in order to select a primary in every round while Tendermint needs to know the validators in order to select a proposer in each round. For PoW, PoS, DPOS and Ripple, nodes can join the network freely.
- *Energy saving*. In PoW, miners hash the block header continuously to reach the target value. As a result, the amount of electricity required to process has reached an immense scale. As for PoS and DPOS, miners still have to hash the block header to search the target value but the work has been largely reduced as the search space is designed to be limited. As for PBFT, Ripple and Tendermint, there is no mining in consensus process. So it saves energy greatly.
- *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 [33] in PoW systems can help miners to gain more revenue by only 25% of the hashing power. PBFT and Tendermint is designed to handle up to 1/3 faulty nodes. Ripple is proved to maintain correctness if the faulty nodes in an UNL is less than 20%.
- *Example*. Bitcoin is based on PoW while Peercoin is a new peer-to-peer PoS cryptocurrency. Further, Hyperledger Fabric utilizes PBFT to reach consensus.

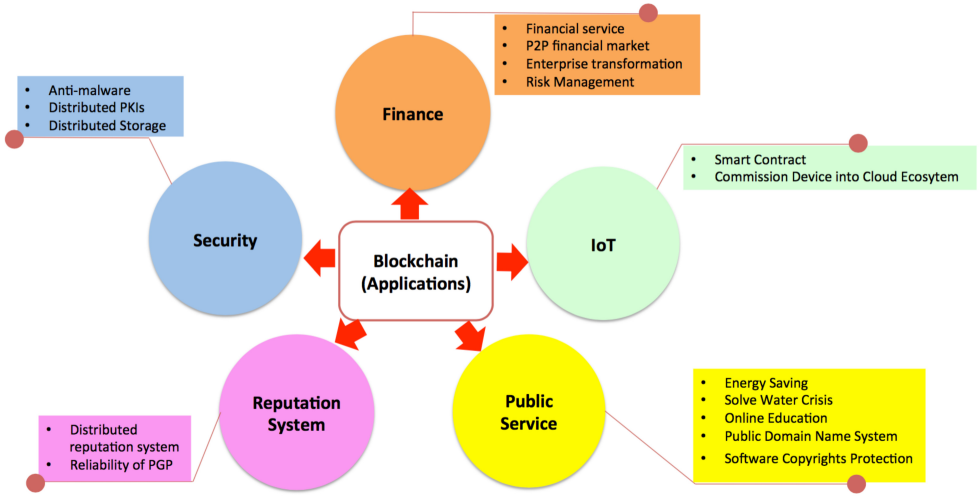
Bitshares, a smart contract platform, adopts DPOS as their consensus algorithm. Ripple implements the Ripple protocol while Tendermint devises the Tendermint protocol.

PBFT and Tendermint are permissioned protocols. Node identities are expected to be known to the whole network, so they might be used in commercial mode rather than public. PoW and PoS are suitable for public blockchain. Consortium or private blockchain might has preference for PBFT, Tendermint, DPOS and Ripple.

3.3 Advances on consensus algorithms

A good consensus algorithm means efficiency, safty and convenience. Current common consensus algorithms still have many shortages. New consensus algorithms are devised aiming to solve some specific problems of blockchain. The main idea of PeerCensus [28] is to decouple block creation and transaction confirmation so that the consensus speed can be significantly increased. Besides, Kraft [47] proposed a new consensus method to ensure that a block is generated in a relatively stable speed. It is known that high blocks generation rate compromise Bitcoin's security. So the Greedy Heaviest-Observed Sub-Tree (GHOST) chain selection rule [77] is proposed to solve this problem. Instead of the longest branch scheme, GHOST weights the branches and miners can choose the better one to follow. Chepurnoy et al. [26] proposed a new consensus algorithm for peer-to-peer blockchain systems where anyone who provides non-interactive proofs of retrievability for the past state snapshots is agreed to generate the block. In such a protocol, miners only have to store old block headers instead of full blocks.

Figure 5 Representative application domains of blockchain.



4 Applications of blockchain

There is a diverse of applications of blockchain technology. In this section, we summarize several typical applications of blockchain. We roughly categorize the applications of

blockchain into finance in Section 4.1, IoT in Section 4.2, public and social services in Section 4.3, reputation system in Section 4.4 and security and privacy in Section 4.5. Figure 5 illustrates 5 representative application domains of blockchain.

4.1 Finance

- *Financial Services*. The emergency of blockchain systems such as Bitcoin [60] and [7] has brought a huge impact on traditional financial and business services. Peters et al. [68] discussed that blockchain has the potential to disrupt the world of banking. Blockchain technology can be applied into many areas including clearing and settlement of financial assets etc. Besides, Morini et al. [58] showed that there are real business cases like collateralization of financial derivatives that can leverage blockchain to reduce costs and risks. Blockchain has also caught tremendous attention in the eyes of large software companies: Microsoft Azure [10] and IBM [9] are beginning to offer Blockchain-as-a-Service.

- *Enterprise Transformation*. 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 [41], Jaag and Bach explored opportunities of arising blockchain technology for POs and claimed that each PO can 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 can be prevailed quickly with their dense retail network. In addition, it is also shown in [41] that blockchain technology offers business opportunities for POs in identity services, device management and supply chain management.

- *P2P Financial Market*. Blockchain can also help build P2P financial market in a secure and reliable way. Noyes explored ways of combining peer-to-peer mechanisms and multiparty computation protocols to create a P2P financial MPC (Multiparty Computation) market [64]. Blockchain-based MPC market allows offloading computational tasks onto a network of anonymous peer-processors.

- *Risk Management*. Risk management framework plays a significant role in financial technology (FinTech) and now it can be combined with blockchain to perform better. Pilkington [70] 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 [54] that a new system combined with blockchain can reduce custody risk and achieve the same level of transactional safety. Besides, blockchain-based smart contract enables the decentralized autonomous organizations (DAO) to engage in business-work collaborations. A highly dependable DAO-GaaS conflict model [62] was proposed to safeguard business-semantics induced consistency rules.

4.2 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 [14, 57]. The typical killer applications of IoT include the logistic management with Radio-Frequency Identification (RFID) technology [4], smart homes [31], e-health [37], smart grids [34], Maritime Industry [83], etc.

Blockchain technologies can potentially improve the IoT sector.

- *E-business*. Zhang et al. [86] propose a new IoT E-business model and realize the transaction of smart property based on blockchain and smart contract. In this model, distributed autonomous Corporations (DAC) is adopted as a decentralized transaction entity. People trade with DACs to obtain coins and exchange sensor data without any third party.

- *Safety and Privacy*. Safety and privacy preservation is another important concern with IoT industry. Blockchain can also help in improving privacy in IoT applications. In particular, Hardjono et al. [38] proposed a privacy-preserving method for commissioning an IoT device into a cloud ecosystem. More specifically, a new architecture was proposed in [38] to help device to prove its manufacturing provenance without the authentication of third party and it is allowed to register anonymously. Besides, in [40], IBM unveiled its proof of concept for Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT), which is a system using blockchain technologies to build a distributed network of devices. In ADEPT, appliances in the home will be able to identify operational problems and retrieve software updates on their own.

4.3 Public and Social Services

Blockchain can also be widely used in public and social services.

- *Land Registration*. One of typical blockchain applications in public services is the land registration [65], 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.

- *Energy Saving*. Besides, blockchains can be used in green energy. Gogerty and Zitoli proposed the solarcoin [36] 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 can be granted by the solarcoin foundation as long as you have generated the solar energy.

- *Education*. 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 [30], blockchain learning was proposed. In blockchain learning, blocks can be packed and placed into blockchain by teachers and the learning achievements can be thought as coins.

- *Free-Speech Right*. Moreover, blockchain can be used to secure Internet infrastructure such as DNS and identities. For example, Namecoin [6] is an experimental open-source technology that improves decentralization, security, censorship resistance, privacy, and speed of DNS and identities [6]. It protects free-speech rights online by making the web more resistant to censorship.

Blockchains can also be used to other public services such as marriage registration, patent management and income taxation systems [13]. 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.

4.4 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 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. Blockchain can potentially solve this problem.

- *Academics*. Reputation is important to academics. Sharples et al. [75] proposed a blockchain-based distributed system for educational record and reputation. At the beginning, each institution and intellectual worker will be given an initial award of educational reputation currency. An institution can award a staff by transferring some reputation records to the staff. Since transactions are stored on blockchain, all the reputation change can be detected easily.

- *Web Community*. The ability to assess the reputation of a member in a web community is very important. Carboni [25] 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. Dennis et al. [29] 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 transaction happens with no suspicion. Since transactions are stored on blockchain, reputation records are nearly impossible to tamper.

4.5 Security and Privacy

- *Security Enhancement*. We have seen the proliferation of various mobile devices and various mobile services, which are also exhibiting their vulnerability to malicious nodes. 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 [63] 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 [63] that BitAV can improve the scanning speed and enhance the fault reliability (i.e., less susceptible to targeted denial-of-service attacks). 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 [15], blockchain can be used to construct a privacy-aware PKI while simultaneously improving the reliability of conventional PKIs.

- *Privacy Protection*. 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 [80]. 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 [88], 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 [5].

5 Challenges & Recent Advances

As an emerging technology, blockchain is facing multiple challenges and problems. We summarize three typical challenges: scalability in section 5.1, privacy leakage in section 5.2 and selfish mining in section 5.3.

5.1 Scalability

With the amount of transactions increasing day by day, the blockchain becomes heavy. Currently Bitcoin blockchain has exceed 100 GB storage. All transactions have to be stored for validating the transaction. 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, which cannot fulfill the requirement of processing millions of transactions in real-time fashion. Meanwhile, as the capacity of blocks is very small, many small transactions might be delayed since miners prefer those transactions with high transaction fee. However, large block size will slow down the propagation speed and lead to blockchain branches. So scalability problem is quite tough.

There are a number of efforts proposed to address the scalability problem of blockchain, which can be categorized into two types:

- *Storage optimization of blockchain*. To solve the bulky blockchain problem, a novel cryptocurrency scheme was proposed in [21]. In the new scheme, old transaction records are removed by the network and a database named account tree is used to

hold the balance of all non-empty addresses. In this way, nodes don't need to store all transactions to check wether a transaction is valid or not. Besides lightweight client can also help fix this problem. A novel schem named VerSum [39] was proposed to provide another way allowing lightweight clients to exist. VerSum allows lightweight clients to outsource expensive computations over large inputs. It ensures that the computation result is correct through comparing results from multiple servers.

- *Redesigning blockchain*. In [32], 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. Miners are competing to become a leader. The leader will be responsible for microblock generation until a new leader appears. Bitcoin-NG also extended the heaviest (longest) chain strategy where only key blocks count and microblocks carry no weight. In this way, blockchain is redesigned and the tradeoff between block size and network security has been addressed.

5.2 Privacy Leakage

Blockchain is believed to be very safe as users only make transactions with generated addresses rather than real identity. Users also can generate many addresses in case of information leakage. However, it is shown in [53], [46] that blockchain cannot guarantee the *transactional privacy* since the values of all transactions and balances for each public key are publicly visible. Besides, the recent study [16] has shown that a user's Bitcoin transactions can be linked to reveal user's information. Moreover, Biryukov et al. [19] presented an method to link user pseudonyms to IP addresses even when users are behind Network Address Translation (NAT) or firewalls. In [19], each client can be uniquely identified by a set of nodes it connects to. However, this set can be learned and used to find the origin of a transaction. Multiple methods have been proposed to improve anonymity of blockchain, which can be roughly categorized into two types:

- *Mixing* [59]. In blockchain, users addresses are pseudonymous. But it is still possible to link addresses to user real identity as many users make transactions with the same address frequently. Mixing service is a kind of service which provides anonymity by transferring funds from multiple input addresses to multiple output addresses. For example, user Alice with address A wants to send some funds to Bob with address B. If Alice directly makes a transaction with input address A and output address B, the relationship between Alice and Bob might be revealed. So Alice can send funds to a trusted intermediary Carol. Then Carol transfer funds to Bob with multiple inputs c1, c2, c3, etc., and multiple output d1, d2, B, d3, etc. Bob's address B is also contained in the output addresses. So it becomes harder to reveal relationship between Alice and Bob. However, the intermediary can be dishonest and reveal Alice and Bob's private information on purpose. It is also possible that Carol transfers Alice's funds to her own address instead of Bob's address. Mixcoin [20] provides a simple method to avoid dishonest behaviours. The intermediary encrypts users' requirements including funds amount and transfer date with its private key. Then if the intermediary did not transfer the money, anybody can verify that the intermediary cheated. However, theft is detected but still not prevented. Coinjoin [51] depends on a central mixing server to shuffle output addresses to prevent theft. And inspired by Coinjoin, CoinShuffle [71] uses decryption mixnets for address shuffling.

- *Anonymous*. In Zerocoin [55], zero-knowledge proof is used. Miners do not have to validate a transaction with digital signature but to validate coins belong to a list of valid coins. Payment's origin are unlinked from transactions to prevent transaction graph analyses. But it still reveals payments' destination and amounts. Zerocash [73] was proposed to address this problem. In Zerocash, zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs) is leveraged. Transaction amounts and the values of coins held by users are hidden.

5.3 Selfish Mining

Blockchain is susceptible to attacks of colluding selfish miners. Generally it is convinced that nodes with over 51% computing power can reverse the blockchain and reverse the happened transaction. However, recent research shows that even nodes with less 51% power are still dangerous. In particular, Eyal and Sirer [33] showed that the network is vulnerable even if only a small portion of the hashing power is used to cheat. In selfish mining strategy, selfish miners keep their mined blocks without broadcasting and the private branch will be revealed to the public only if some requirements are satisfied. As the private branch is longer than the current public chain, it will be admitted by all miners. Before the private blockchain publication, honest miners are wasting their resources on an useless branch while selfish miners are mining their private chain without competitors. So selfish miners tend to get more revenue. Rational miners will be attracted to join the selfish pool and the selfish can exceed 51% power quickly.

Based on selfish mining, many other attacks have been proposed to show that blockchain is not so secure. In stubborn mining [61], miners can amplify its gain by non-trivially composing mining attacks with network-level eclipse attacks. The trail-stubbornness is one of the stubborn strategy that miners still mine the blocks even if the private chain is left behind. Yet in some cases, it can result in 13% gains in comparison with a non-trail-stubborn counterpart. [72] shows that there are selfish mining strategies that earn more money and are profitable for smaller miners compared with simple selfish mining. But the gains are relatively small. Furthermore, it shows that attackers with less than 25% of the computational resources can still gain from selfish mining. To help fix the selfish mining problem, Heilman [18] presented an novel approach for honest miners to choose which branch to follow. With random beacons and timestamps, honest miners will select more fresh blocks. However, [18] is vulnerable to forgeable timestamps. ZeroBlock [76] builds on the simple scheme: Each block must be generated and accepted by the network within a maximum time interval. Within ZeroBlock, selfish miners cannot achieve more than its expected reward.

6 Possible future directions

Blockchain has shown its potential in industry and academia. We discuss possible future directions with respect to five areas: *blockchain testing*, *stop the tendency to centralization*, *big data analytics*, *smart contract* and *artificial intelligence*.

6.1 Blockchain testing

Recently different kinds of blockchains appear and over 700 cryptocurrencies are listed in [12] up to now. However, some developers might falsify their blockchain performance to

attract investors driven by the huge profit. Besides, when users want to combine blockchain into business, they have to know which blockchain fits their requirements. So blockchain testing mechanism needs to be in place to test different blockchains.

Blockchain testing can be separated into two phases: *standardization phase* and *testing phase*. In standardization phase, all criteria have to be made and agreed. When a blockchain is born, it can be tested with the agreed criteria to valid if the blockchain works fine as developers claim. As for testing phase, blockchain testing needs to be performed with different criteria. For example, an user who is in charge of online retail business cares about the throughput of the blockchain, so the examination needs to test the average time from a user sending a transaction to the transaction being packed into the blockchain, capacity for a blockchain block and etc.

6.2 Stop the tendency to centralization

Blockchain is designed as a decentralized system. However, there is a trend that miners are centralized in the mining pool. Up to now, the top 5 mining pools together owns larger than 51% of the total hash power in the Bitcoin network [1]. Apart from that, selfish mining strategy [33] showed that pools with over 25% of total computing power can get more revenue than fair share. Rational miners will be attracted into the selfish pool and finally the pool can easily exceed 51% of the total power. As the blockchain is not intended to serve a few organizations, some methods should be proposed to solve this problem.

6.3 Big data analytics

Blockchain can be well combined with big data. Here we roughly categorized the combination into two types: *data management* and *data analytics*. As for data management, blockchain can be used to store important data as it is distributed and secure. Blockchain can also ensure the data is original. For example, if blockchain is used to store patients health information, the information can not be tampered and it is hard to steal those private information. When it comes to data analytics, transactions on blockchain can be used for big data analytics. For example, user trading patterns might be extracted. Users can predict their potential partners' trading behaviors with the analysis.

6.4 Smart contract

A smart contract is a computerized transaction protocol that executes the terms of a contract [78]. It has been proposed for long time and now this concept can be implemented with blockchain. In blockchain, smart contract is a code fragment that can be executed by miners automatically. Nowadays, more and more smart contract develop platforms are emerging and smart contract can achieve more and more functionalities. Blockchain can be used in many areas, such as IoT [27] and banking services [68].

We categorize smart contract researches into two types: *development* and *evaluation*. Development can be smart contract development or smart contract platform development. Now many smart contracts are deployed on Ethereum [84] blockchain. As for platform development, many smart contract develop platforms like Ethereum [84] and Hawk [46] are emerging. Evaluation means code analysis and performance evaluation. Bugs in smart contract can bring disastrous damages. For instance, owing to the *recursive call bug*, over 60 million dollars are stolen from a smart contract- theDAO [42]. So smart contract attack analysis are very important. On the other hand, smart contract performance is also of vital

importance to smart contract. With blockchain technology developing quickly, more and more smart contract based applications will be put into use. Companies need to take the application performance into consideration.

6.5 Artificial Intelligence

Recent developments in blockchain technology are creating new opportunities for Artificial Intelligence (AI) applications [66]. AI technologies can help solve many blockchain challenges. For instance, there is always an oracle who is responsible for determining whether the contract condition is satisfied. Generally this oracle is a trusted third party. AI technique may help build an intelligent oracle. It is not controlled by any party, it just learns from the outside and train itself. In that way, there will be no argues in smart contract and smart contract can become smarter. On the other hand, AI is penetrating into our lives now. Blockchain and smart contract can help to restrict misbehaviors done by AI products. For instance, laws written in smart contract can help to restrict misbehaviors done by driverless cars.

7 Conclusion

Blockchain is highly appraised and endorsed for its decentralized infrastructure and peer-to-peer nature. However, many researches about the blockchain are shielded by Bitcoin. But blockchain can be applied to a variety of fields far beyond Bitcoin. Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability. In this paper, we present a comprehensive survey on blockchain. We first give an overview of blockchain technologies including blockchain architecture and key characteristics of blockchain. We then discuss the typical consensus algorithms used in blockchain. We analyze and compare these protocols in different respects. We also investigate typical blockchain applications. Furthermore, we list some challenges and problems that will hinder blockchain development and summarize some existing approaches for solving these problems. Some possible future directions are also discussed. Nowadays smart contract is developing fast, many smart contract applications are proposed. However, as there are still many defects and limits in smart contract languages, many innovative applications are hard to implement currently. We plan to take a in-depth investigation on smart contract in the 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 (61672545), the Pearl River S&T Nova Program of Guangzhou (201710010046). 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

[1] The biggest mining pools, https://bitcoinworldwide.com/mining/pools/

[2] Bitshares - your share in the decentralized exchange, https://bitshares.org/

[3] Consortium chain development, https://github.com/ethereum/wiki/wiki/Consortium-Chain-Development

[4] ISO/IEC 18000 (2013), http://en.wikipedia.org/wiki/ISO/IEC_18000

[5] Ethos (2014), http://viral.media.mit.edu/projects/ethos/

[6] Namecoin (2014), https://www.namecoin.org/

[7] Hyperledger project (2015), https://www.hyperledger.org/

[8] Antshares digital assets for everyone (2016), https://www.antshares.org

[9] Ibm blockchain (2016), http://www.ibm.com/blockchain/

[10] Microsoft azure: Blockchain as a service (2016), https://azure.microsoft.com/en-us/solutions/blockchain/

[11] State of blockchain q1 2016: Blockchain funding overtakes bitcoin (2016), http://www.coindesk.com/state-of-blockchain-q1-2016/

[12] Crypto-currency market capitalizations (2017), https://coinmarketcap.com

[13] Akins, B.W., Chapman, J.L., Gordon, J.M.: A whole new world: Income tax considerations of the bitcoin economy (2013), https://ssrn.com/abstract=2394738

[14] Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer Networks 54(15), 2787 – 2805 (2010)

[15] Axon, L.: Privacy-awareness in blockchain-based PKI. Cdt technical paper series (2015)

[16] Barcelo, J.: User privacy in the public bitcoin blockchain (2014)

[17] Bentov, I., Lee, C., Mizrahi, A., Rosenfeld, M.: Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. ACM SIGMETRICS Performance Evaluation Review 42(3), 34–37 (2014)

[18] Billah, S.: One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner (2015)

[19] Biryukov, A., Khovratovich, D., Pustogarov, I.: Deanonymisation of clients in bitcoin p2p network. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 15–29. New York, NY, USA (2014)

[20] Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A., Felten, E.W.: Mixcoin: Anonymity for bitcoin with accountable mixes. In: Proceedings of International Conference on Financial Cryptography and Data Security. pp. 486–504. Berlin, Heidelberg (2014)

[21] Bruce, J.: The mini-blockchain scheme (July 2014), http://cryptonite.info/files/mbc-scheme-rev3.pdf

[22] burstcoin: burstcoin (2014), https://bitcointalk.org/index.php?topic=731923.0

[23] Buterin, V.: A next-generation smart contract and decentralized application platform. white paper (2014)

[24] Buterin, V.: On public and private blockchains (2015), https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[25] Carboni, D.: Feedback based reputation on top of the bitcoin blockchain. arXiv preprint arXiv:1502.01504 (2015)

[26] Chepurnoy, A., Larangeira, M., Ojiganov, A.: A prunable blockchain consensus protocol based on non-interactive proofs of past states retrievability. arXiv preprint arXiv:1603.07926 (2016)

[27] Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access 4, 2292–2303 (2016)

[28] Decker, C., Seidel, J., Wattenhofer, R.: Bitcoin meets strong consistency. In: Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN). p. 13. ACM, Singapore, Singapore (2016)

[29] Dennis, R., Owen, G.: 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). pp. 131–138. IEEE (2015)

[30] Devine, P.: Blockchain learning: can crypto-currency methods be appropriated to enhance online learning? In: ALT Online Winter Conference (2015)

[31] Dixon, C., Mahajan, R., Agarwal, S., Brush, A., Saroiu, B.L.S., Bahl, P.: An operating system for the home. In: NSDI. USENIX (April 2012)

[32] Eyal, I., Gencer, A.E., Sirer, E.G., Van Renesse, R.: Bitcoin-ng: A scalable blockchain protocol. In: Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16). pp. 45–59. Santa Clara, CA, USA (2016)

[33] Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. In: Proceedings of International Conference on Financial Cryptography and Data Security. pp. 436–454. Berlin, Heidelberg (2014)

[34] Fan, Z., Kulkarni, P., Gormus, S., Efthymiou, C., Kalogridis, G., Sooriyabandara, M., Zhu, Z., Lambotharan, S., Chin, W.H.: Smart grid communications: overview of research challenges, solutions, and standardization activities. IEEE Communications Surveys and Tutorials 15(1), 21–38 (2013)

[35] Foroglou, G., Tsilidou, A.L.: Further applications of the blockchain (2015)

[36] Gogerty, N., Zitoli, J.: Deko: An electricity-backed currency proposal. Social Science Research Network (2011)

[37] Habib, K., Torjusen, A., Leister, W.: 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) (2015)

[38] Hardjono, T., Smith, N.: Cloud-based commissioning of constrained devices using permissioned blockchains. In: Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security. pp. 29–36. ACM (2016)

[39] van den Hooff, J., Kaashoek, M.F., Zeldovich, N.: Versum: Verifiable computations over large public logs. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 1304–1316. New York, NY, USA (2014)

[40] IBM: IBM ADEPT Practictioner Perspective - Pre Publication Draft (2015)

[41] Jaag, C., Bach, C., et al.: Blockchain technology and cryptocurrencies: Opportunities for postal financial services. Tech. rep. (2016)

[42] Jentzsch, C.: The history of the dao and lessons learned (2016), https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5

[43] Johnson, D., Menezes, A., Vanstone, S.: The elliptic curve digital signature algorithm (ecdsa). International Journal of Information Security 1(1), 36–63 (2001)

[44] King, S.: Primecoin: Cryptocurrency with prime number proof-of-work. July 7th (2013)

[45] King, S., Nadal, S.: Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. Self-Published Paper, August 19 (2012)

[46] Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: Proceedings of IEEE Symposium on Security and Privacy (SP). pp. 839–858. San Jose, CA, USA (2016)

[47] Kraft, D.: Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking and Applications 9(2), 397–413 (2016)

[48] Kwon, J.: Tendermint: Consensus without mining. URL http://tendermint.com/docs/tendermint {_} v04. pdf (2014)

[49] Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS) 4(3), 382–401 (1982)

[50] Lee Kuo Chuen, D. (ed.): Handbook of Digital Currency. Elsevier, 1 edn. (2015), http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170

[51] Maxwell, G.: Coinjoin: Bitcoin privacy for the real world. In: Post on Bitcoin Forum (2013)

[52] Mazieres, D.: The stellar consensus protocol: A federated model for internet-level consensus. Stellar Development Foundation (2015)

[53] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: Characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet Measurement Conference (IMC'13). New York, NY, USA (2013)

[54] Micheler, E., von der Heyde, L.: Holding, clearing and settling securities through blockchain technology creating an efficient system by empowering asset owners. Social Science Research Network (2016)

[55] Miers, I., Garman, C., Green, M., Rubin, A.D.: Zerocoin: Anonymous distributed e-cash from bitcoin. In: Proceedings of IEEE Symposium Security and Privacy (SP). pp. 397–411. Berkeley, CA, USA (2013)

[56] Miguel, C., Barbara, L.: Practical byzantine fault tolerance. In: Proceedings of the Third Symposium on Operating Systems Design and Implementation. vol. 99, pp. 173–186. New Orleans, USA (1999)

[57] Miorandi, D., Sicari, S., Pellegrini, F.D., Chlamtac, I.: Internet of things: Vision, applications and research challenges. Ad Hoc Networks 10(7), 1497 – 1516 (2012)

[58] Morini, M.: From'blockchain hype'to a real business case for financial markets. Social Science Research Network (2016)

[59] Möser, M.: Anonymity of bitcoin transactions: An analysis of mixing services. In: Proceedings of Münster Bitcoin Conference. pp. 17–18. Münster, Germany (2013)

[60] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008), https://bitcoin.org/bitcoin.pdf

[61] Nayak, K., Kumar, S., Miller, A., Shi, E.: Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In: Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 305–320. Saarbrucken, Germany (2016)

[62] Norta, A., Othman, A.B., Taveter, K.: 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. pp. 244–257. ACM (2015)

[63] Noyes, C.: Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning. arXiv preprint arXiv:1601.01405 (2016)

[64] Noyes, C.: Efficient blockchain-driven multiparty computation markets at scale. Tech. rep. (2016), https://www.overleaf.com/articles/blockchain-multiparty-computation-markets-at-scale/mwjgmsyybxvw/viewer.pdf

[65] NRI: Survey on blockchain technologies and related services. Tech. rep. (2015)

[66] Omohundro, S.: Cryptocurrencies, smart contracts, and artificial intelligence. AI Matters 1(2), 19–21 (Dec 2014), http://doi.acm.org/10.1145/2685328.2685334

[67] P4Titan: Slimcoin a peer-to-peer crypto-currency with proof-of-burn (2014)

[68] Peters, G.W., Panayi, E.: Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. Social Science Research Network (2015)

[69] Peters, G.W., Panayi, E., Chapelle, A.: Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective (2015), http://dx.doi.org/10.2139/ssrn.2646618

[70] Pilkington, M.: Does the fintech industry need a new risk management philosophy? a blockchain typology for digital currencies and e-money services in luxembourg. Social Science Research Network (2016)

[71] Ruffing, T., Moreno-Sanchez, P., Kate, A.: Coinshuffle: Practical decentralized coin mixing for bitcoin. In: Proceedings of European Symposium on Research in Computer Security. pp. 345–364. Cham (2014)

[72] Sapirshtein, A., Sompolinsky, Y., Zohar, A.: Optimal selfish mining strategies in bitcoin. arXiv preprint arXiv:1507.06183 (2015)

[73] Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from bitcoin. In: Proceedings of 2014 IEEE Symposium on Security and Privacy (SP). pp. 459–474. San Jose, CA, USA (2014)

[74] Schwartz, D., Youngs, N., Britto, A.: The ripple protocol consensus algorithm. Ripple Labs Inc White Paper 5 (2014)

[75] Sharples, M., Domingue, J.: 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). pp. 490–496. Lyon, France (2015)

[76] Solat, S., Potop-Butucaru, M.: ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin. Technical report, Sorbonne Universites, UPMC University of Paris 6 (May 2016), https://hal.archives-ouvertes.fr/hal-01310088

[77] Sompolinsky, Y., Zohar, A.: Accelerating bitcoin's transaction processing. fast money grows on trees, not chains. IACR Cryptology ePrint Archive 2013(881) (2013)

[78] Szabo, N.: The idea of smart contracts (1997)

[79] Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys Tutorials 18(3), 2084–2123 (2016)

[80] Vagata, P., Wilfong, K.: Scaling the Facebook data warehouse to 300 PB. Tech. rep. (2014), https://code.facebook.com/posts/229861827208629/scaling-the-facebook-data-warehouse-to-300-pb/

[81] Vasin, P.: Blackcoin¡¯s proof-of-stake protocol v2 (2014), https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[82] Vukolić, M.: The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In: International Workshop on Open Problems in Network Security. pp. 112–125. Zurich, Switzerland (2015), "http://dx.doi.org/10.1007/978-3-319-39028-4_9"

[83] Wang, H., Osen, O., Li, G., Li, W., Dai, H.N., Zeng, W.: Big data and industrial internet of things for the maritime industry in northwestern norway. In: IEEE Region 10 Conference (TENCON) (2015)

[84] Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper (2014)

[85] Zamfir, V.: Introducing casper ¡°the friendly ghost¡±. Ethereum Blog URL: https://blog. ethereum. org/2015/08/01/introducing-casper-friendly-ghost (2015)

[86] Zhang, Y., Wen, J.: An iot electric business model based on the protocol of bitcoin. In: Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN). pp. 184–191. Paris, France (2015)

[87] Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: Architecture, consensus, and future trends. In: Proceedings of the 2017 IEEE BigData Congress. pp. 557–564. Honolulu, Hawaii, USA (2017)

[88] Zyskind, G., Nathan, O., et al.: Decentralizing privacy: Using blockchain to protect personal data. In: Security and Privacy Workshops (SPW), 2015 IEEE. pp. 180–184. IEEE (2015)