

Received August 29, 2019, accepted October 3, 2019, date of publication October 11, 2019, date of current version October 24, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2946983

SoK of Used Cryptography in Blockchain

MAYANK RAIKWAR^{ID}, DANILO GLIGOROSKI^{ID}, AND KATINA KRALEVSKA^{ID}

Department of Information Security and Communication Technologies, Norwegian University of Science and Technology (NTNU), 7491 Trondheim, Norway

Corresponding author: Mayank Raikwar (mayank.raikwar@ntnu.no)

This work was supported by the NTNU Research Project under Grant 81771158.

ABSTRACT The underlying fundamentals of blockchain are cryptography and cryptographic concepts that provide reliable and secure decentralized solutions. Although many recent papers study the use-cases of blockchain in different industrial areas, such as finance, health care, legal relations, IoT, information security, and consensus building systems, only few studies scrutinize the cryptographic concepts used in blockchain. To the best of our knowledge, there is no Systematization of Knowledge (SoK) that gives a complete picture of the existing cryptographic concepts which have been deployed or have the potential to be deployed in blockchain. In this paper, we thoroughly review and systematize all cryptographic concepts which are already used in blockchain. Additionally, we give a list of cryptographic concepts which have not yet been applied but have big potentials to improve the current blockchain solutions. We also include possible instantiations of these cryptographic concepts in the blockchain domain. Last but not least, we explicitly postulate 21 challenging problems that cryptographers interested in blockchain can work on.

INDEX TERMS Blockchain, cryptography, hash function, proof-of-work, consensus, signature, encryption, zero-knowledge proofs, access control, accumulator.

I. INTRODUCTION

Blockchain, a distributed ledger managed by a peer-to-peer network collectively adhering to some consensus protocol, is arguably considered as a new and disruptive technology. Both academia and industry are profoundly affected by new solutions to some old problems which are based on this new technology. The success of the blockchain concept is ultimately connected with the financial success of Bitcoin [1] that was developed just one decade ago, and the subsequent avalanche of more than 2140 other crypto-currencies that all together built a financial market worth around \$285 billion (as of 16 June 2019) [2].

We can trace the origins of the ideas to use cryptography for secure and private transactions for paying access to databases, paying for services such as online games, transferring money over the Internet, Internet shopping and other commercial activities back in 1990's with David Chaum's eCash system [3]. One of the negative aspects of eCash was that it was a centralized system, controlled by a trusted third party. Another hurdle for a broader acceptance of eCash was the fact that it was covered by a long list of patented algorithms – something that is considered as a big obstacle to acceptance among the crypto community.

In parallel, in 1990's we saw the development of several cryptographic ideas not directly connected but somehow still related to the ideas of using cryptography in financial transactions. We mention some of them such as the proposal on how to combat junk email [4] by Dwork and Naor that was published in 1992, and which used computationally expensive functions. Then in 1996, there was a proposal for time-lock cryptographic puzzles [5] by Rivest, Shamir, and Wagner by using RSA based CPU expensive computations. At the end of 90's and early 2000's several patent free cryptographic concepts were proposed, implemented and released as open source projects by an online movement and a community of cryptographers and programmers known as "Cypherpunks" [6]. Those cryptographic concepts and implementations include Adam Back's "hash-cash" proposal for a currency based on the hardness of finding partial hash collisions [7], Wei Dai's "b-money" [8] and Nick Szabo's¹ "Bitgold" proposal [9]. These concepts have been the basis of the Satoshi Nakamoto's decentralized cryptocurrency, nowadays known as Bitcoin [1], [10]. As a recognition of their pioneering activities in the decentralized cryptocurrencies, Ethereum [11] – the second most popular

The associate editor coordinating the review of this manuscript and approving it for publication was Yunlong Cai^{ID}.

¹Nick Szabo was also part of the eCash development team in late 90's.

cryptocurrency – named the three of its denominations as “Wei”, “Szabo” and “Finney” [12].²

The underlying core technology in Bitcoin is blockchain. Blockchain is a distributed ledger maintaining a continuously growing list of data records that are confirmed by all of the participating nodes. The data is recorded in this public ledger in a form of blocks of valid transactions, and this public ledger is shared and available to all nodes.

Blockchain is envisioned as a promising and powerful technology but it still encounters many research challenges. Some of the main challenges are constant improvement of its security and privacy, key management, scalability, analysis of new attacks, smart contract management, and incremental introduction of new cryptographic features in existing blockchains. These challenges arise due to the network structure and the underlying consensus mechanisms and cryptographic schemes used within the blockchains. To overcome these challenges and to find enhanced solutions, many of the cryptographic concepts such as signature schemes, zero-knowledge proofs, and commitment protocols are scrutinized and applied. As cryptography is a vast research field, there is always a scope to find new cryptographic schemes in order to improve the solutions in blockchain.

The majority of the ongoing research in Blockchain focuses on finding and identifying improvements to the current processes and routines, mostly in industries that rely on intermediaries, including banking, finance, real estate, insurance, legal system procedures, and healthcare. The study on business innovation through blockchain [14] presents some blockchain enabled business applications and their instantiations. These blockchain enabled applications still need a proper way for selecting the cryptographic technique employed in their respective solution in order to meet the business requirements. Not only these blockchain applications but also the research community will benefit from an overview in a form of systematization of the current state of knowledge of all available cryptographic concepts which have been applied or can be applied in existing and future blockchain solutions. To the best of our knowledge, this is the first systematization of knowledge that gives a complete picture of the existing cryptographic concepts related to blockchain. We have tried to depict most of the cryptographic concepts in the blockchain domain. Although there are various works about specific cryptographic concepts used in blockchain, there are only few works which merge all these atomic works and present them in a single paper. Most of the review and survey works such as [15], [16] discuss security, privacy, consensus or other challenges in blockchain. A recent work of Wang et al. [17] gives a comprehensive analysis of cryptographic primitives in blockchain. Their analysis presents the functionality and the usage of these primitives in blockchain. However, the analysis is based only on exist-

ing cryptocurrencies and it lacks many of the cryptographic protocols which are used in blockchain.

A. OUR CONTRIBUTION

In this study, we classify cryptographic concepts based on their use in blockchain.³ We have divided them into two categories: 1. Concepts which are well used in blockchain, and 2. Concepts which are promising but not yet implemented in blockchain. This categorization does not have a clear boundary. We classify some cryptographic concepts as promising ones, and that requires further research and scrutiny in order to be deployed in blockchain. As a result, the following points are the main contributions of our Systematization of Knowledge (SoK) paper:

- We provide a description of cryptographic concepts which have been applied in the blockchain field. We also include instantiation of these concepts in blockchain.
- We provide a list of cryptographic concepts which are rarely used or have not been used in blockchain but they have the potential to be applied in this field. These concepts open many possible research directions and they can be examined in different blockchain applications.
- We identified 21 research challenges that we formulate as *Research Problem*. Some of them are rephrased research challenges already published in the literature and some of them are newly formulated research problems.

In this study, we do not claim that we have exhausted all of the cryptographic concepts which are employed in blockchain, but we have tried to cover the concepts which we felt are propitious for the blockchain domain. We also describe each cryptographic concept along with its associated properties and its instantiation in the blockchain field. Additionally, in order to give one unified presentation about blockchain, we give a brief explanation about:

- Enabling concepts of blockchain such as hash function, consensus protocol, network architecture.
- Layered architecture of blockchain and emphasis on some of the major challenges associated with blockchain.

B. ORGANIZATION OF THE PAPER

The rest of the paper is organized as follows. Section II presents the research methodology. Section III explains the main pillars of blockchain such as hash functions, consensus mechanisms, network infrastructure and types of blockchain. Section IV gives an overview of some critical challenges faced by existing blockchains. Section V reviews already used cryptographic concepts in blockchain and presents the basic idea of each cryptographic concept with available instantiation in blockchain. Section VI presents cryptographic concepts which have not been employed or implemented in blockchain yet, but look very promising for

²Hal Finney was a cypherpunk and the receiver of the first Bitcoin transaction of 10 Bitcoins from the anonymous Satoshi Nakamoto [13].

³A continuously updated version of cryptographic concepts is available on this github repository <http://bit.do/fchb5>

blockchain. Finally, Section VII concludes this SoK and gives possible future work directions.

II. RESEARCH METHODOLOGY

To perform a systematization of knowledge of the existing cryptographic concepts related to blockchain, we established and followed a methodology that we explain in this Section. Since the invention of Bitcoin, there has been a growing interest in blockchain from both academia and industry. The number of publications in the blockchain field has been rapidly increasing in recent years. Not all of these publications are research works; some of these works discuss different use-cases of blockchain. Therefore, to review these many papers in the blockchain field, we pursued a research methodology which defines the inclusion criteria, a search strategy to search for respective publications and a data collection mechanism to accumulate the relevant publications. The collected data is later processed based on inclusion and exclusion criteria. The publications which meet the inclusion criteria go through one final step of quality assessment. Once a publication passes the quality assessment, it is included in our systematization.

We use keyword search to make the first selection of potentially relevant scientific publications. For the keyword search, we typed keywords such as *<cryptographic concept name> <in blockchain>* or *<use of> <cryptographic concept name> <in blockchain>*. We use Google Scholar as our primary source to search for the relevant literature, but as Google Scholar does not exhaust all of the available literature, we also searched in databases such as: 1) IACR eprint archive, 2) IEEE Xplore, 3) ACM Digital Library, 4) ScienceDirect, and 5) Springer Link.

The inclusion criteria for this study is based on the following questions:

- Is the elaborated cryptographic concept useful in blockchain? The usefulness of the cryptographic concept is measured as whether we achieve some essential properties in blockchain by using the concept or whether the cryptographic concept can be beneficial for some use-case compared to an already implemented concept.
- Which properties can be achieved by using the cryptographic concept in blockchain?
- Is there any instantiation of the cryptographic concept in a blockchain study or application? If not, is there any potential?

The criteria for excluding a paper is:

- Informal literature discussing some cryptographic concepts in blockchain.
- Literature which claims on using a cryptographic concept but it does not give any guarantees about the feasibility and prospects of a potential implementation.

The quality of the papers that meet the inclusion criteria is assessed. For quality assessment, we apply the following questions:

- Is the cryptographic concept implemented in blockchain? If not, is it possible to implement it and will it be more efficient than the existing solution?
- Is there any security analysis or does the implemented concept rely on another underlying platform?
- Are the fundamental concept and its related properties adequately described?

III. SUPPORTING AND ENABLING CONCEPTS OF BLOCKCHAIN

As previously mentioned, blockchain is a way to encapsulate transactions in the form of blocks where blocks are linked through the cryptographic hash, hence forming a chain of blocks. Figure 1 shows the basic blockchain structure. Each block in the blockchain contains a block header and a representation of the transaction. For instance, in Figure 1, each block consists of its hash, the hash of the previous block, a timestamp and some other block fields (e.g., version, nonce). This depends from the block design. Merkle root hash represents the set of transactions in the Merkle tree, and this representation of transactions varies according to the design of the blockchain implementation. Figure 2 depicts the Bitcoin blockchain data structure showing in details the block format.

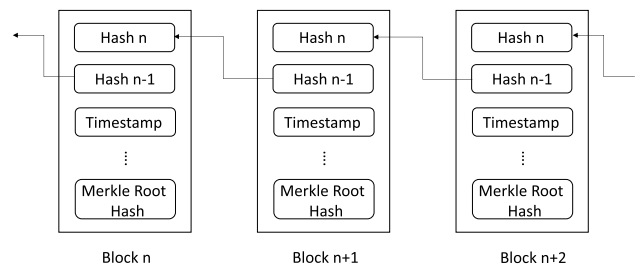


FIGURE 1. Basic blockchain structure.

Blockchain relies on different constituents which serve different purposes. In this Section, we give an overview of the main underlying concepts used to build a blockchain. A detailed technical explanation of all these concepts is out of the scope of this paper, but we have tried to cover the essentials of their functionality.

A. CRYPTOGRAPHIC HASH FUNCTION

A hash function H is a function which takes an input of an arbitrary size and maps it to a fixed size output. Cryptographic hash functions have some additional properties such as: **a) collision resistance** - it is hard to find two inputs a and b such that $H(a) = H(b)$; **b) preimage resistance** - for a given output y it is hard to find an input a such that $H(a) = y$; and **c) second preimage resistance** - for a given input a and output $y = H(a)$ it is hard to find a second input b such that $H(b) = y$. Readers interested in an extensive cover of the field of cryptographic hash functions are referred to [18].

Cryptographic hash functions in blockchain are used for various purposes such as:

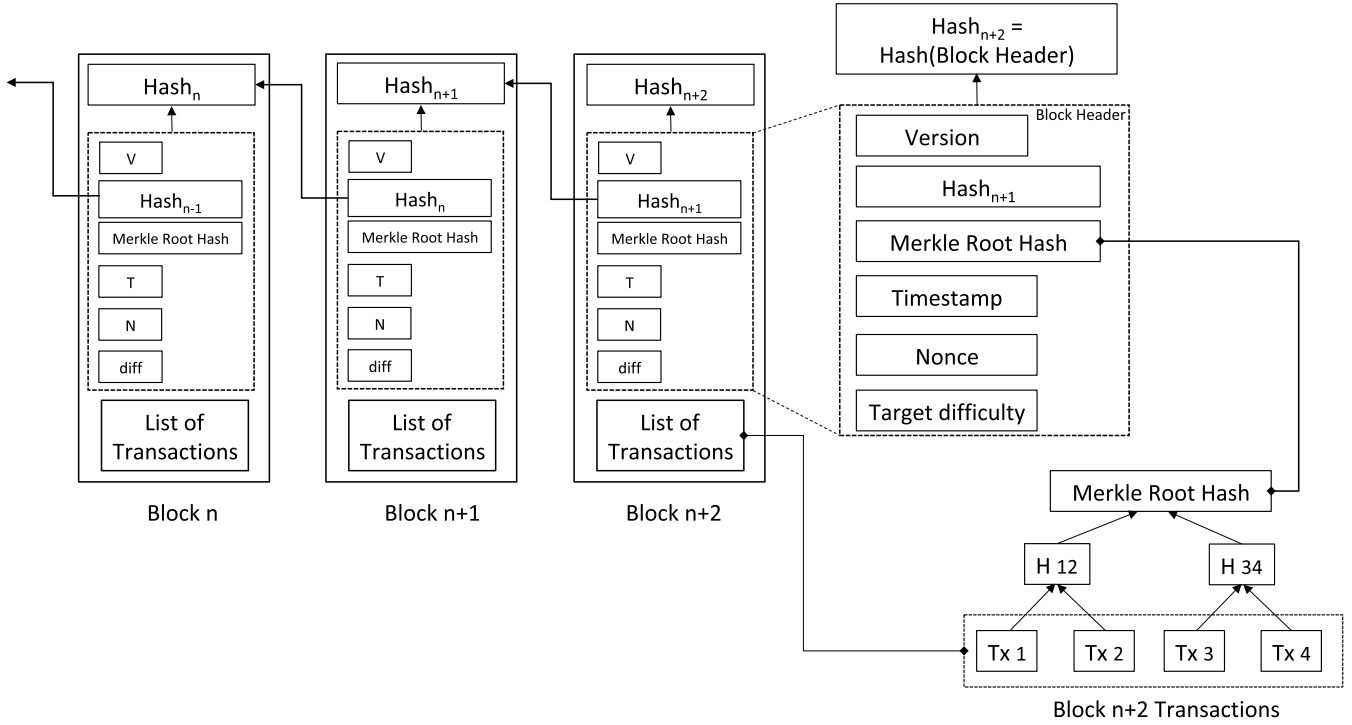


FIGURE 2. Blockchain data structure with block format.

- 1) solving cryptographic puzzles (the Proof of Work (PoW) in Bitcoin [1]);
- 2) address generation (for public and private keys);
- 3) shortening the size of the public addresses;
- 4) message digests in signatures.

The most popular cryptographic hash functions used in blockchains are SHA-2 [19] (especially the variant SHA256 - a variant that produces outputs of 256 bits), and some of the well analyzed hash functions from the NIST SHA-3 competition and standardization that went to the later stages of that process (final 5 proposals or some of the 14 proposals from the second phase [20]). Some of the existing blockchain designs such as IOTA constructed their own “homebrewed” cryptographic hash function called Curl-P, that was received very critically and negatively by the crypto community [21], [22].

A typical way how cryptographic hash functions are used in blockchain designs is in a form of a mode of operation, i.e., a combination of several invocations of a same or different hash functions. For example, in Bitcoin [1], SHA256 is used twice and that construction is called SHA256d, i.e.,

$$\text{SHA256d}(\text{message}) = \text{SHA256}(\text{SHA256}(\text{message})). \quad (1)$$

Mining is a process of creating a new block of transactions through solving a cryptographic puzzle, and the participant who solves the puzzle first is called a *miner of the block*. If we look at the Bitcoin PoW puzzle, we can see that a miner has to find a *Nonce* (similar to Hashcash protocol [7] that we discuss in the next subsection) to create the next block in the

blockchain. The puzzle looks like this:

$$\text{SHA256d}(\text{Ver} || \text{HashPrevBlock} || \dots || \text{Nonce}) \leq T \quad (2)$$

where T is 256-bit target value.

Looking into the fraction of SHA256d outputs that are less than the target value T for different values of T in Table 1 helps us to understand why mining is hard in PoW. Namely, the probability of finding a nonce that will cause the whole block to have a hash that is less than the target value is

$$\Pr[\text{SHA256d}(\text{Block}) \leq T] \approx \frac{T}{2^{256}}. \quad (3)$$

TABLE 1. Fraction of SHA256d outputs with respective target value.

Target Value T	Fraction of SHA256d outputs $\leq T$
$0 \times 7 \underbrace{t_1 t_2 t_3 t_4 \dots t_{62} t_{63}}_{63 \text{ times}}$	$\frac{1}{2}$
$0 \times 0 \underbrace{t_1 t_2 t_3 t_4 \dots t_{62} t_{63}}_{63 \text{ times}}$	$\frac{1}{16}$
$0 \times \underbrace{00 \dots 00}_{16 \text{ times}} \underbrace{t_1 t_2 t_3 t_4 \dots t_{47} t_{48}}_{48 \text{ times}}$	$\frac{1}{2^{64}}$

We next discuss the research and innovative activities in the area of cryptographic hash functions that were either remotely or directly connected and inspired by the trends in blockchain.

Several years after the launch of the Bitcoin and its source code being published as an open source on Github, blockchain designers started to clone and fork its basic

code, and started to introduce different variants and innovations. One of the earliest forks from 2011 that is still popular nowadays is Litecoin [23]. The basic idea by the Litecoin design was to use a different hash function for its proof of work puzzles. The motivation came from the fact that even in 2011 there were trends to build specialized application-specific integrated circuit (ASIC) hardware implementations of SHA256d that will mine the blocks several orders of magnitude faster than ordinary CPUs and GPUs. Instead of SHA256d, Litecoin uses *Script* [24] - a memory-intensive compilation of use of the HMAC [25] construction instantiated with SHA256 and use of the stream cipher Salsa20/8 [26]. The idea was that the use of *Script* will be impractical to implement it in ASIC, thus, giving chances of individual owners of regular computers and GPUs to become a significant mining community. While with no doubts we can say that Litecoin is a very successful alternative cryptocurrency, we can for sure claim that its initial goal to be ASIC resistant blockchain design was not successful. Nowadays, you can find commercial products for Litecoin hardware mining.⁴

Actually, we can say that the 10 years of history of blockchain, in general, and cryptocurrencies, in particular, is a history of failed attempts to construct a sustainable blockchain that will prevent the appearance of profitable ASIC miners that can mine the blocks with hash computing rates that are several orders of magnitude higher than the ordinary users of CPUs and GPUs. In that short history, we can mention Ethash used in Ethereum [11] for which there are now commercially available ASIC miners by at least two companies. In 2013, QuarkCoin [27] introduced the idea of using a chain of six hash functions (five SHA-3 finalists BLAKE, Grøstl, JH, Keccak and Skein [28]) and the second round hash function Blue Midnight Wish [29]. One of the motivations behind the QuarkCoin PoW function was to be more ASIC resistant than SHA256d. The cascading idea of QuarkCoin was later extended to a cascade of eleven hash functions in Darkcoin (later renamed DASH [30]). Needless to say, nowadays there are commercially available ASIC miners for X11 as well.

The frictions between ASIC miners and the cryptocurrency community seem to remain to the present days, and are somewhat evolving and inspiring novel proposals in blockchain protocols. The latest is the Programmatic Proof-of-Work (ProgPoW) initiative for Ethereum blockchain ecosystem that aims to make ASIC mining less efficient and to give some advantages to graphics processing units (GPU) mining [31].

B. CONSENSUS MECHANISMS

Consensus is the key component of blockchain to synchronize or update the ledger by reaching an agreement among the

⁴One such a product that can compute 580 billion Script hashes per second, is offered by the company Bitmain and is called “Antminer L3++”. As of the time of writing this article, this product was advertised at <https://shop.bitmain.com/> for a price of \$213.00 and for a 10 days delivery (2 June 2019).

participants. In order to maintain the ledger in a decentralized way, many consensus mechanisms have been proposed. The first introduction of the use of a consensus mechanism in blockchain is implicitly given by Bitcoin. Bitcoin uses Proof of Work (PoW) mechanism as consensus where the idea came from *Hashcash Protocol* [7]. The objective of Hashcash was to prevent spam in public databases. The *Hashcash Protocol* is as follows. Suppose an email client wants to send an email to an email server. In the beginning, the client and the server both agree on a cryptographic hash function H which maps an input string to an n length output string. Then, the email server sends a challenge string c to the client. Now the client has to find a string x such that $H(c||x)$ starts with k zeros. Since H has pseudorandom outputs, the probability of success in a single trial is

$$\frac{2^{n-k}}{2^n} = \frac{1}{2^k}.$$

Here x corresponding to c is considered as PoW and the process of finding that x is called mining. PoW is difficult to generate but easy to verify.

Many literature studies on consensus mechanisms, for instance, the survey by Wang et al. [16] and “SoK: Consensus in the age of blockchains” [32], have been carried out in the past few years. Since consensus mechanisms have already been thoroughly studied in the literature, in this paper, we present the basic idea about how consensus mechanisms work and their classification.

In a consensus protocol, depending on the network architecture and blockchain type, some or all of the participants take part and maintain the ledger by adding a block consisting of transactions to their ledger. However, the creation of a new block to be added to the ledger is performed by a participant who is known as a leader of the consensus protocol in that particular execution. This leader is elected by different mechanisms of leader election process, and some of these mechanisms are given in Table 2.

TABLE 2. Leader election in consensus protocols.

Leader Election Criteria	Reference Protocols
PoW Puzzle Competition	Bitcoin-NG [33], Casper [34], Proof of Stake velocity [35]
Verifiable Random Function	Tendermint [36], Algorand [37], Secure Proof of Stake [38]
Trusted Random Function	Proof of luck [39], Proof of elapsed time [40]
Modified Preimage Search	Snow White [41]
Sub-network of Masternodes / Validator nodes	Darkcoin and DASH [42], Libra [43]

After the leader is elected and the new block is created in order to achieve consensus or agreement on this block, two types of voting mechanisms are followed: *explicit* and *implicit*. In explicit voting, multiple rounds of voting occur and then based on the votes, consensus is reached. However, in implicit voting, the new block created by the leader is accepted by others who implicitly vote for the new block

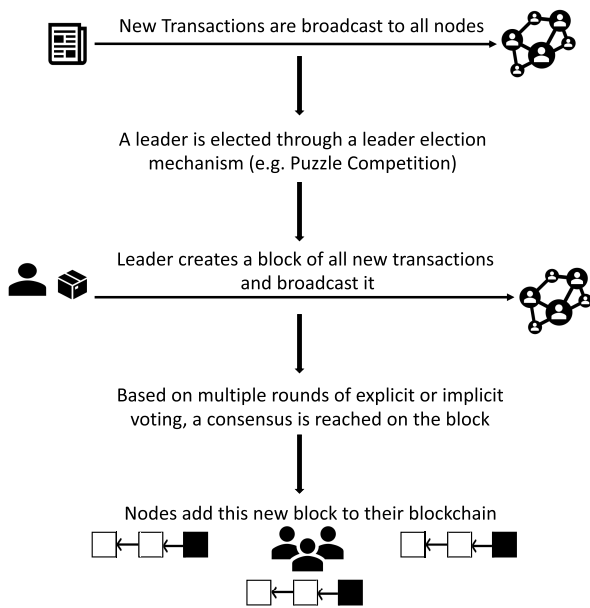


FIGURE 3. Blockchain consensus scenario.

and add it to their ledgers. A leader election through PoW puzzle competition (e.g., PoW puzzle 2 in Bitcoin) followed by an implicit voting to reach an agreement is also called “Nakamoto Consensus”.

Consensus mechanisms also determine the performance of the blockchain network in terms of consensus finality, throughput, scalability, and robustness against various attacks. In some manner, consensus orchestrates the state of the programs executed in the blockchain network nodes by providing a runtime environment to collectively verify the same program and hence reach to a finality. There is no exact classification of consensus mechanisms, but in general they can be classified as consensus protocols with proof of concept and consensus protocols with byzantine fault-tolerant replication. These consensus protocols can be chosen based on the blockchain network and type. Most of the proof of concept consensus protocols are used in permissionless blockchains. There are many proof of concept schemes which have been proposed and implemented, e.g., Proof of Work (PoW) [44], Proof of Stake (PoS) [45], Equihash [46], having Masternodes in Dash [42], etc. As described in Section III-A, in PoW puzzle based consensus protocols, miners try to solve the cryptographic puzzle by mining and these miners are also responsible for verification of the transactions, and an incentive (*reward*) is given to the first miner who solves the puzzle.

In case of a permissionless network, as there is no authentication and no proper synchronization, the underlying consensus algorithm should be able to handle the synchronization problem, scale well and mitigate different attacks in order to maintain canonical blockchain state in P2P network. To solve this synchronization issue, most of the blockchains use “Longest chain rule” to have a consistent canonical state of blockchain in this P2P blockchain network. On the

contrary, in the permissioned blockchain, as there are restrictions and privileges associated with the peers, there is a strict control on the synchronization among the peers. Byzantine fault-tolerant protocols are usually adopted in permissioned blockchains to provide consensus properties such as validity, agreement, and termination. Practical Byzantine Fault Tolerant (PBFT) [47], Proof of Elapsed Time [40], Ripple consensus [48] are some of the consensus protocols used in permissioned blockchains. Recently, Facebook launched its own global cryptocurrency Libra [43] which works as a permissioned blockchain and provides users to do transactions with nearly zero fee. Libra blockchain comes with a new programming language Move and a new consensus protocol called LibraBFT.

1) MINING, POOL MINING AND INCENTIVE MECHANISMS

In Proof of Work based blockchains, the addition of new transactions in the blockchain is performed by the mining process. In the Bitcoin mining process, a puzzle is solved by computing many hashes repeatedly (Equation 2) by putting different values for the nonce to satisfy the condition. When a miner successfully solves the puzzle first among all of the miners, it gets a monetary incentive for solving the puzzle. Because of this incentive process, all consensus nodes or miners follow the rules of the blockchain state transition during the puzzle competition. Mining is a resource-intensive process where the main resources are computational power and memory. Mining can be performed either by a solo miner or by a group of miners, called a mining pool, who collectively try to solve the puzzle. Mining pools may operate on different mining techniques and incentive mechanisms. These incentive mechanisms can vary based on the used mining technique or the decision of the pool operator. Reference [16] gives a brief idea about the mining strategy management in blockchain networks, while reference [49] provides a strategic study of mining through stochastic games. Different incentive mechanisms are proposed and tested in blockchains. Reference [50] analyzes Bitcoin pooled mining reward systems, and a reward system based on information propagation in blockchain network is presented in [51].

C. NETWORK INFRASTRUCTURE

Blockchain is maintained by a peer-to-peer (P2P) network. P2P network is an overlay network which is built on the top of the Internet. This P2P blockchain network can be modeled as structured, unstructured or hybrid based on several parameters such as the consensus mechanism and the type of blockchain. Regardless of the representation of the network, a blockchain network should quickly disseminate the newly generated block so that the global view of the blockchain remains consistent. Consequently, a synchronization protocol is needed, but a routing protocol might or might not be needed. A traditional P2P network uses a routing protocol to route the information through multihop; however, in many blockchains (e.g., Bitcoin), routing is not required because

a peer can get information through at most one hop, so no routing table is maintained.

Almost all cryptocurrencies and blockchains such as Bitcoin [1], Ethereum [11], Litecoin [23] use unstructured P2P network where the idea is to have equal privileges for all of the nodes and to create an egalitarian network. A P2P network can follow flat or hierarchical organization for building a random graph among the peers. This graph is not fully connected, but in order to receive all of the communication and to maintain the ledger, each peer maintains a list of peer addresses. Thus, if any peer propagates a message in the network, eventually all peers receive it through their available connections. In an unstructured network, techniques like flooding and random walk are used to make new connections with the peers. In the unstructured network, peers can leave and join at any time. This can be exploited by an adversary that can join and see the messages floating in the network and can further do source spoofing, reordering or injecting of messages.

Blockchain can also use structured P2P network where nodes are organized in a specific topology and thus finding any resource/information becomes easier. In this structured P2P network, an identifier is assigned to each node to route the messages in a more accessible way. Each node also maintains a routing table. A structured P2P network maintains a distributed hash table (DHT) where (key, value) pairs are stored corresponding to the peers which help in the resource discovery. Ethereum has started the adoption of structured P2P network by using Kademlia protocol [60]. However, most of the blockchain networks are unstructured, and moreover, if the blockchain is public where no restriction to join or leave the network is enforced, then many possible attacks can happen. Thus, the security of blockchain depends heavily on the network architecture. A propagation delay or a synchronization problem in a P2P network can affect the consensus protocol of blockchain, leading to a non-consistent global view in blockchain. In addition to these problems, an adversary can cause several attacks in a P2P network, where few of the main attacks are as following:

- Netsplit (Eclipse) attack: An adversary monopolizes all of the connections of a node and splits that node from the entire network. Further, the node cannot participate in consensus or validation protocol and this causes inconsistency in the network [61].
- Routing attack: A set of participants are isolated from the blockchain network by the adversary and thus the block propagation is delayed in the network [62].
- Distributed Denial-Of-Service (DDOS) attack: An adversary exhausts the network resources and targets honest nodes so that honest nodes do not get the services or information which they are supposed to receive [63], [64].

D. TYPES OF BLOCKCHAIN

Blockchains can be classified depending on the implementation design, administration rules, data availability, and access

privileges. From an academic point of view, they have been classified as “public” and “private”. While from the administrative point of view, they are described as “permissioned” and “permissionless”. Nevertheless, these terms are used interchangeably in most of the blockchain studies and applications in industries, which is not the correct way to use these terms. Even though the classification of blockchains is not very clearly specified in the literature, we can still classify blockchains by coupling public, private, permissioned and permissionless.

- 1) *Permissionless Public*: In this type of blockchain, anyone can join or leave the network at any time and participate in consensus as well to maintain the ledger. Everyone also has read and write access to the blockchain. Thus, it provides minimum trust among the participants, but it still achieves maximum transparency. Most of the cryptocurrencies and blockchain platforms are permissionless public, e.g., Bitcoin [1], Zerocash [52] and Monero [53].
- 2) *Permissioned Public*: This type of blockchain allows everyone to read the blockchain state and data, but in order to write the data and take part in consensus, there are permissions/privileges associated with the participants provided by the network administrator which in a certain way makes the system not fully decentralized. In this type of blockchain once a participant has some privileges, based on that it can become a validator as well. Examples for permissioned public blockchain are Ripple [54], EOS [55] and the newest Libra [43].
- 3) *Permissionless Private*: This type of a blockchain allows organizations to collaborate without the need of sharing information publicly. Being permissionless, allows anyone to join or leave the blockchain at any time, which is also acknowledged by other nodes as well. The smart contracts on these networks also define who is allowed to read the contract and the related data, not only just who is allowed to perform the actions. Some permissionless private blockchains use Federated byzantine agreement as a consensus protocol. LTO [56] network is an example of a permissionless private blockchain which creates “live contract” on the network.
- 4) *Permissioned Private*: These blockchains are mostly used in organizations where data/information is stored in the blockchain with permissioned access control by members of the organization. The membership in the network is provided by the network administrator or some membership authority. Read and write access to the data is also provided by the network administrator. Hyperledger fabric [57], Monax [58], Multichain [59] are examples of permissioned private blockchains.

Table 3 proffers a clear picture of the classification of blockchains with associated advantages, challenges and application domains. However, in general, permissionless public blockchains are commonly referred to as public blockchains and permissioned private blockchains are

TABLE 3. Blockchain classification.

Blockchain Type	Application Domain	Anonymity	Scalability	Challenges	References
Permissionless Public	Decentralized P2P Networks	High	Low	Privacy, Scalability	Bitcoin [1], Zerocash [52], Monero [53]
Permissioned Public	Decentralized Organizations	High	Moderate	Privacy, Centralization	Ripple [54], EOS [55]
Permissionless Private	Intra-Organization Networks	Moderate	Moderate	Consensus, Scalability	LTO [56]
Permissioned Private	Organizational restricted ledgers	Low	High	Consensus, Centralization	Hyperledger fabric [57], Monax [58], Multichain [59]

TABLE 4. Layered architecture of blockchain.

	Confidentiality	Integrity	Availability	Data Privacy	Anonymity
Smart Contract	Encryption	MAC	–	Data Privacy Preserving Computation	Identity Privacy Preserving Computation
Transaction	–	Signature Scheme	Access Structure of Transactions	Zero-Knowledge Proofs, Mixing Techniques	Zero-Knowledge Proofs
Consensus	–		Consensus	Access Control	Blind or Ring Signature
Network	Encryption	MAC	Protocols e.g. Gossip	–	IP Anonymity e.g. TOR
Database			Access Control	Access Control	–

referred to as fully private blockchains. A combination of permissioned public and permissionless private makes “consortium blockchain” which is also called a federated blockchain. A consortium blockchain is neither completely public nor completely private, and it makes blockchain as partially decentralized. In consortium blockchain, the consensus is reached by a selected group of participants. Nowadays most of the organizations have embraced consortium blockchains for their blockchain enabled solutions.

IV. CHALLENGES IN BLOCKCHAIN

Blockchain as an emerging technology comes with many challenges. In order to solve these challenges, various solutions have been proposed and implemented in the blockchain. The proliferation of cryptocurrencies across multiple payment systems brings many risks in social, economic and technical terms. Blockchain encounters many challenges due to network architecture, underlying consensus protocol and applied cryptographic primitives. Some of these major challenges are security and privacy associated with blockchain, scalability of blockchain, and resource consumption (computational power, memory, network bandwidth). An insightful analysis on the research perspectives and challenges for bitcoin and other cryptocurrencies [65] has been presented in the past and gives a nice overview of scalability, security, privacy and consensus of cryptocurrencies.

We can summarize our discussion in Section III-B, in a form of generic research problems and research challenges in the area of blockchain consensus mechanisms as follows. Construct a new blockchain consensus mechanism that is better than the existing ones from the following perspectives:

- 1) Less energy consumption;
- 2) More efficient consensus achievements;
- 3) Better security than the existing consensus mechanisms.

However, further in the paper when we identify a more concrete and focused research challenge, we formulate it in a form of a Research Problem. For example, from the discussion given in the III-A we can formulate the following: **Research Problem 1:** Construct sustainable blockchain systems that have one of the following properties:

- 1) They are provably resistant to give mining advantages to ASIC miners as opposite to GPU and CPU miners;
- 2) They are provably resistant to give mining advantages to ASIC and GPU miners as opposite to CPU miners.

If we observe the blockchain as a layered architecture, we can identify the challenges that occur in each layer. Table 4 shows blockchain as a stack of five layers. These five layers serve the following purposes:

- **Smart contract layer** processes contract data and send the result data to the transaction layer.
- **Transaction layer** creates the transactions and sends those to consensus layer.
- **Consensus layer** runs the consensus algorithm and adds the transactions to the block.
- **Network layer** deals with all P2P communication among blockchain nodes.
- **Database layer** stores the blockchain data in a respective database used by respective blockchain platform.

Table 4 gives a glimpse of blockchain layered architecture and also mentions some of the cryptographic techniques to achieve properties like security and privacy. In Table 4, the first column defines the layers of blockchain, and the

first row illustrates the properties which can be accomplished in the different layer using different cryptographic techniques. Thus to understand, each cell corresponds to the deployed cryptographic method to attain the property in the corresponding column in the respective blockchain layer (corresponding row). For example, encryption can be used to achieve confidentiality in smart contract layer, Message Authentication Code (MAC) can be used to achieve integrity in the network layer of blockchain. Table 4 names few of the techniques used in the blockchain but there are more available cryptographic techniques which can be employed in blockchain. “–” in Table 4 represents that the corresponding property for the corresponding layer does not make much sense. Some of the significant challenges of blockchain are as follows.

A. SECURITY AND PRIVACY

For any blockchain, a key evaluation parameter is how well the security and privacy conditions meet the requirement of the blockchain. Analyzing the security and privacy issues of blockchain is a broad research area, and some studies have been conducted in this area. Here we do not cover those details, instead we only define these terms. Security is defined as three components: confidentiality, integrity, and availability. In a generic context, (i) confidentiality is a set of rules that limits access to information, (ii) integrity is the assurance that the information is trustworthy and accurate, and (iii) availability is a guarantee of reliable access to the information by authorized people. However, in case of blockchain, the term *Information* used in the above context can have multiple meanings such as data in the database, smart contract data or transactions. Privacy can be defined as data privacy and user privacy (anonymity). Table 4 includes some cryptographic mechanisms for achieving security and privacy of information subjected to different blockchain layers.

In the light of recent increased number of incidents with the security of the different layers of blockchain platforms and the theft of millions of dollars worth cryptocurrencies, we formulate the following research problem.

Research Problem 2: Construct a penetration testing tool irrespective of the blockchain platform to test the security and privacy requirements for each layer of any blockchain platform.

B. SCALABILITY ISSUES

The size⁵ of blockchain is continuously growing, and scalability is becoming a big problem in the blockchain domain. Scalability depends on the underlying consensus, network synchronization and architecture. To scale the blockchain, the computational power and the bandwidth capabilities should be high for each node in the blockchain, which is

practically infeasible. Most of the current blockchains grant limited scalability.

One proposal how to address the scalability problems of the blockchain ledger is so called: “SPV, Simplified Payment Verification” [66]. It verifies if particular transactions are valid but without downloading the entire ledger. This method is used by some wallet and lightweight Bitcoin clients, and its security was first analyzed in [67]. Another proposal to achieve high scalability is to use erasure codes in blockchain by encoding validated blocks into small number of coded blocks. A recent work [68] proposes the use of fountain codes (a class of erasure codes) to reduce the storage cost of blockchain by the order of magnitude and hence achieving high scalability. Applying other types of erasure codes for distributed storage, such as regenerating codes [69], [70], locally repairable codes [71], [72] or a combination of both types of codes [73], [74], may reduce even further the storage and communication costs.

Another issue in connection with the scalability is the issue of the interoperability. Namely, it is a fact that the number of different public ledgers is increasing rapidly. While some sort of a rudimentary interoperability has been implemented in cryptocurrencies exchange platforms [75], the risks and insecurities with these platforms are vast and well documented [76].

Research Problem 3: Construct a new blockchain mechanism that periodically prunes its distributed ledger (reduces its size), producing a fresh but equivalent ledger, while provably keeping correct state of all assets that are subject of the ledger transactions.

Research Problem 4: Construct secure protocols for blockchain interoperability.

A recent reference [77] strongly supports our research problem 3 since it admits that Ethereum blockchain is almost full now and hence the scalability is a big bottleneck.

C. FORKING

A blockchain fork is essentially caused when two miners find a block at almost the same time due to a software update or versioning. In a blockchain network, each device or computer is considered as “a full node” which runs software to keep the blockchain secure by verifying the ledger. The software is updated to adjust some parameters and to install new features in the blockchain. This updated software may not be compatible with the old software. Consequently, the old nodes which have not updated their software and the new nodes which have performed a software update can cause a fork in the blockchain when they create new blocks. There are two types of forks: one which is not compatible with previous software version, called a hard fork, and another one which is compatible with the previous version (backward-compatible), called a soft fork. A hard fork happens when there is a significant change in the software such as change of block parameters or change of consensus mechanism. In the case of Ethereum, a hard fork will occur when it will migrate from Proof of Work to Proof of Stake. One example of a soft

⁵<https://bitinfocharts.com> gives most of the statistics (including size) of popular cryptocurrencies.

fork is Segregated Witness (SegWit) which was implemented in Bitcoin by changing the transaction format. Recently, privacy coin Beam [78] (an implementation of Mimblewimble privacy protocol) conducted its first hard fork away from ASICS. Figure 4 depicts a blockchain forking scenario where the correct chain can be any of these two forked chains depending on the case of the hard or soft fork.

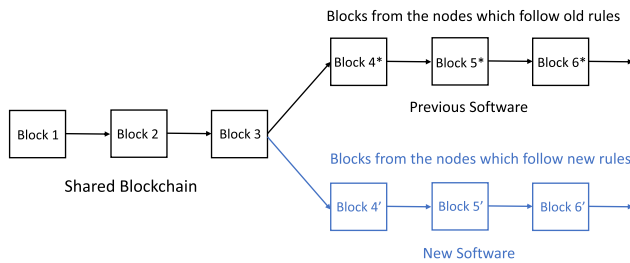


FIGURE 4. Blockchain forking.

Research Problem 5: Construct Forking-free consensus mechanism for permissionless public blockchain.

D. THROUGHPUT

It is a measure of the number of blocks appended in blockchain per second which effectively means the number of transactions processed per second. Throughput depends on many factors such as underlying consensus algorithm, number of nodes participating in consensus, network structure, node behavior, block parameters and the complexity of the contract (in case of smart contract supported blockchains). The complexity of a smart contract depends on whether the programming language of the blockchain is turing-complete or not. However, regarding turing-completeness of blockchains [79], there is always a division between the blockchain community. Considering these primary factors, attaining high throughput is a bit hard in blockchain. However, for value-asset blockchains to achieve high throughput, the size of the transaction can be reduced by excluding some information from the transaction and the throughput can be increased by increasing the block size and the bandwidth of the network till a certain level.

The number of transactions per second was recognized as a serious problem in Bitcoin network. While in the peak holiday period Visa and MasterCard can handle up to 50,000 transactions per second worldwide, the Bitcoin network can handle just 7 transactions. One proposal how to address this scalability issue is the “The Bitcoin Lightning Network” [80]. It is a network that handles instantly the Bitcoin transactions off the main ledger. It establishes a network of micropayment channels that addresses the malleability by using Bitcoin multi-signatures 2-of-2. Special nodes are needed for these micropayment networks and as of June 2019, there were around 4,500 nodes. The first financial transaction via the Lightning network was reported in January 2018. Litecoin decided to follow the Bitcoin Lightning network, and as of March 2019 there were more

than 1000 registered nodes that handle the micropayments for that alternative cryptocurrency. Many other solutions were proposed to solve the scalability issue, similar to the Lightning off-chain computation and off-chain state channels, such as Sharding [81], Plasma [82], Liquid [83] and the recent Channel Factories [84].

As the Lightning network has gained popularity, new research challenges emerge as explained in [85], and here we rephrase one of their research challenges.

Research Problem 6: [85]: Develop scalable protocols that will perform multi-hop payment-channel and path-based transactions with strong privacy guarantees even against an adversary that has network-level control.

Addressing Problem 6, many works have been done in the past but all those works are mostly compatible with Bitcoin or Ethereum blockchain. Recent works [86], [87] on multi-hop payment channel provide value privacy and security but only for Bitcoin-compatible blockchains. Instead of supporting only payments like Lightning network, there are off-chain state channels, like Celer Network [88], which support general state updates while providing significant improvement in terms of cost and finality.

Research Problem 7: Develop fully functional state channel with strong security and privacy guarantee.

E. ENERGY CONSUMPTION

The mining process of blockchain (e.g., bitcoin mining) consumes a lot of energy. Most of the PoW puzzle based consensus protocols waste a huge amount of energy.⁶ Many alternative consensus algorithms are introduced which use less energy than Bitcoin’s PoW such as PoS [45], Equihash [46], and PBFT [47]. Energy is also consumed during communication over the network. Some cryptographic mechanisms also consume high energy so the selection of a proper cryptographic mechanism should be based not only on the memory requirement and the computational load but also on the amount of energy consumption. The use of blockchain should be energy efficient and to fulfill that 1) PoS-like consensus should be used and 2) proper energy management techniques should be utilized, for example in the case of Internet-of-Things (IoT).

F. INFRASTRUCTURE DEPENDENCIES

The blockchain infrastructure is built with several elements of network protocols, cryptographic concepts, and mining hardware. All these elements depend on each other in some sense. If we look into the layered architecture of blockchain in Table 4, each layer is dependent on its upper and lower layers for some input/output. Thus, there are many infrastructure dependencies in blockchain. For instance, the data from the smart contract layer is an input to the transaction layer that outputs actual transactions; the data from the consensus layer

⁶<https://digiconomist.net/bitcoin-energy-consumption> depicts Bitcoin energy consumption index charts in TWh per year. It also shows the energy consumption per country.

results in an input to the network layer through a communication protocol; and the data from the network layer data is sent to the database through database storage management. These dependencies must be taken into account while building a comprehensive blockchain framework for any use case; otherwise, some of the blockchain functionalities will not be fulfilled.

From the blockchain infrastructure perspective, we have to mention here one evolving and enabling technology that will be very important in the next decade: 5G. 5G will connect hundreds of billions of IoT devices, but that vast number of devices can be governed securely only by strong decentralized mechanisms offered by the blockchain technologies [89], [90]. We formulate this debate as the following. **Research Problem 8:** Construct efficient, scalable, inexpensive and sustainable blockchain systems capable to handle and securely manage up to billions of IoT devices connected via the 5G network infrastructure.

V. OVERVIEW OF USED CRYPTOGRAPHIC CONCEPTS IN BLOCKCHAIN

From the cryptographic point of view, many of the cryptographic techniques have already been exhibited and heavily employed in various blockchain platforms and blockchain use-cases [17]. As the spectrum of the cryptographic concepts is vast, there is always a scope to dig out some of the existing cryptographic schemes and use them in blockchain services.

In Table 5 we give a comprehensive summary of all cryptographic concepts that we will cover in this and in the next Section. It serves as a handy overview and quick reference table for our systematization of the cryptographic knowledge used in blockchain.

Following are some of the cryptographic concepts which have already been well analyzed and implemented in blockchain.

A. SIGNATURE SCHEME

A standard digital signature is a mathematical scheme based on public-key cryptography that aims to produce short codes called signatures of digital messages by the use of a private key, and where those signatures are verifiable by the use of the corresponding public key. In this context, digital signatures guard against tampering and forgeries in digital messages.

A signature scheme is used in blockchain to sign the transaction, hence, authenticating the intended sender and providing transaction integrity as well as non-repudiation of the sender. Many of the signature schemes are widely accepted to employ integrity and anonymity in blockchain. The digital signature is one of the most important cryptographic primitives that makes blockchain to be publicly verifiable and with achievable consensus. Signature schemes are used in almost every blockchain. Figure 5 represents a general example about how a blockchain user (signer) creates a digitally signed transaction or block using his private key. Moreover, figure 6 shows how other blockchain nodes (verifier) verify whether the signature on the transaction or block is

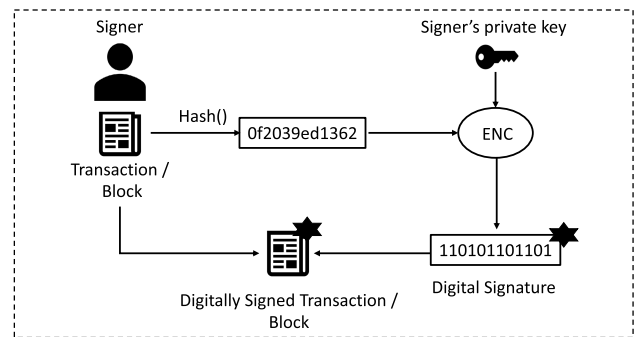


FIGURE 5. Signing process of blockchain transaction/block.

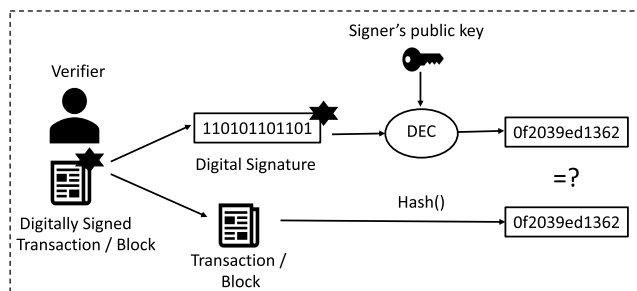


FIGURE 6. Verification of digitally signed transaction/block.

valid or not using the signer's public key. Blockchain applies different signature schemes to provide additional features like privacy, anonymity, and unlinkability. Signature scheme can also be applied to generate constant size signature using signature aggregation. Schnorr Signatures are a form of signature aggregation and it has been used in Bitcoin instead of P2SH [125] for scalability [126]. Some of the signature schemes applied in blockchain are:

- 1) **Multi-Signature:** In a multi-signature scheme, a group of users signs a single message. In a blockchain network, when a transaction requires a signature from a group of participants, it might be advantageous to use a multi-signature scheme. Blockchain platforms such as Openchain [127] and MultiChain [59] support M -of- N multi-signature scheme which reduces the risk of theft by tolerating compromise of up to $M-1$ cryptographic keys. Boneh et al. also designed compact multi-signatures for smaller blockchains [128].
- 2) **Blind Signature:** In this scheme [129], signatures are employed in privacy-related protocols where the signer and the message authors (transaction in case of blockchain) are different parties. Blind signatures are used to provide unlinkability and anonymity of the transaction. In a blockchain setup, a blind signature might be helpful to provide anonymity and unlinkability where the transacting party and the signing party are different. Blind signatures have been used in BlindCoin [130] distributed mixing network to provide the unlinkability of transactions. Blind signatures are

TABLE 5. Summary of Cryptographic Concepts in Blockchain.

Cryptographic Concept	Properties	Instantiation (Reference)
Access Control	Data privacy	Hyperledger Fabric [57], FairAccess [91], [92]
Accumulator	Provides Membership Proofs, Anonymity	Batching Techniques for Accumulators in Blockchain [93]
Aggregate Signature	Fast Signature Verification	Tested in Bitcoin [94]
Commitment Scheme	Non-Repudiation	Used in Bulltproof [95] and in Monero [53], [96]
Decentralised Authorization	Data Privacy	BlendCAC [97], WAVE [98]
Encryption Scheme	Confidentiality and Anonymity	Kadena [99], Hyperledger Fabric [57], Tendermint [36]
Identity Based Encryption	No Public Key Distribution Infrastructure	BAVP [100], BLIC [101]
Incremental Cryptography	Efficiency Improvement	Kadena [99]
Lightweight Cryptography	Fast, less Memory/Energy Consumption	LSB [102], EVCE [103]
Obfuscation	Privacy	Tested in Bitcoin [104]
Oblivious RAM	Confidentiality and Integrity	Solidus [105], EVORAM [106]
Oblivious Transfer	Data Privacy	Searchchain [107], [108]
Post-Quantum Cryptography	Quantum Resistant	Post-Quantum Blockchain [109], [110], [111]
Private Information Retrieval	Data Privacy	Private Blockchain Queries from PIR [85]
Proof of Retrievability	Cloud Data Recovery	Permacoin [112], Retricoin [113], Storj [114]
Secret Sharing	Data privacy	SHARVOT [115], Wanchain [116]
Secure Multiparty Computation	Privacy of Peers and Smart Contract	Enigma [117], Hawk [118], Wanchain [116]
Signature Scheme	Integrity and Authentication	In Every Blockchain e.g. Multichain [59], CryptoNote [119]
Verifiable Delay Function	Less Parallelism, Fast Verification	Chia Network [120]
Verifiable Random Function	Verifiable Pseudorandom Output	Algorand [37], Ouroboros Praos [121], Dfinity [122]
White-Box Cryptography	Data Privacy	Runtime Self-Protection in Blockchain Ledger [123]
Zero-Knowledge Proof	User and Data privacy	Zerocoin [124], Zerocash [52]

also tested in Bitcoin to provide the anonymity for the Bitcoin on-chain and off-chain transactions [131].

- 3) Ring Signature: This scheme [132] uses a protocol where a signature is created on a message by any member of a group on behalf of the group while preserving the identity of the individual signer of the signature. Ring signatures are used to achieve anonymity of the signing party in the blockchain network. CryptoNote [119] technology uses a ring signature scheme to create untraceable payments in the cryptocurrencies. A trustless tumbling platform [133] also uses ring signature for anonymity.
- 4) Threshold Signature: This signature scheme is a (t, n) threshold signature where n parties receive a share of the secret key to create the signature and t out of n parties create a signature over any message. As the parties directly construct the signature from the shares, the key is never revealed in the entire scheme. Threshold signature can be helpful to provide anonymity in the blockchain network. Coin-Party [134] uses a threshold signature scheme for multi-party mixing of Bitcoins. A recent work about coin mixer, ShareLock [135], uses threshold ECDSA (Elliptic Curve Digital Signature Algorithm [136]) to provide privacy-enhancing solution for cryptocurrencies. However threshold ECDSA signatures are complex due to the intricacies of the signing algorithm. Other signature schemes, such as EdDSA (Edwards-curve Digital Signature Algorithm [137]) using the Edwards25519 curve, are efficient threshold signatures. Libra [43] blockchain applies this EdDSA during new account address generation.

While digital signatures produced with the keys used in Public Key Infrastructure (PKI) are well legally regulated and can be used in different types of legal disputes, it is a big challenge how to achieve similar regulations with all types of digital signatures used in the existing blockchain solutions. Additionally, in the physical world if an asset is stolen (for example an expensive car, or an expensive watch), it can be traced back to its legal owner.

Research Problem 9: Develop security protocols that merge the existing standardized and legalized PKI systems with some of the developed blockchain systems.

Research Problem 10: Design an anti-theft blockchain system, i.e., a system that guarantees a return of stolen assets back to their legitimate owners.

Regarding Research Problem 10, recently the Vault proposal was re-launched. Its purpose is to shield the bitcoin wallet from theft without the need for hard forking [138]. However, for other blockchain systems, no such proposal or solution exists.

B. ZERO-KNOWLEDGE PROOFS

In Zero-knowledge proofs [139], two parties, a prover and a verifier, participate. First, the prover asserts some statement and proves its validity to the verifier without revealing any other information except the statement. Thus, a zero-knowledge proof proves the statement as ‘transfer of an asset is valid’ without revealing anything about the asset. Zero-knowledge protocols are extremely useful cryptographic protocols for achieving secrecy in the applications. They can be used to provide the confidentiality of an asset (transaction data) in the blockchain while keeping the asset in the blockchain. Some of the public blockchains

use zero-knowledge proofs such as Zerocoin [124] or Zerocash [52] for untraceable and unlinkable transactions. Zerocoin is a decentralized mix and extension to Bitcoin for providing anonymity and unlinkability of transactions by applying zero-knowledge proofs. In Zerocoin protocol, a user who has Bitcoins can generate an equal value of Zerocoins without the need of any third party mixing set. A user can spend his/her Bitcoin by 1) producing a secure commitment (i.e., Zerocoin), 2) recording it in the blockchain, and 3) broadcasting a transaction and a zero-knowledge proof for the respective Zerocoin. Hence, other users can validate the Zerocoin recorded in the blockchain and verify the transaction along with the proof. Here zero-knowledge proof protects the linking of Zerocoin to a user, yet Zerocoin is a costly protocol due to its high complexity and large proof size.

To reduce the complexity and the proof size, a variant of zero-knowledge proof known as Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) [140] is used by Zerocash protocol. zk-SNARK hides the information about the amount and the receiver address in a transaction. The main idea of zk-SNARK is any computational condition can be represented by an arithmetic circuit, which takes some data as input and gives *true* or *false* in response. zk-SNARK reduces the proof size and the computational effort compared to the basic zero-knowledge proofs. An enterprise-focused version of Ethereum, Quorum blockchain platform [141] also uses zk-SNARK for transaction privacy and anonymity. Figure 7 illustrates an interactive protocol of zero-knowledge where the prover has a statement, and he/she wants to prove that the statement is correct without revealing any information related to the statement. In the interactive protocol, the verifier asks many questions related to the statement and the prover answers these questions in such a way where the prover proves the statement and does not reveal any necessary information.

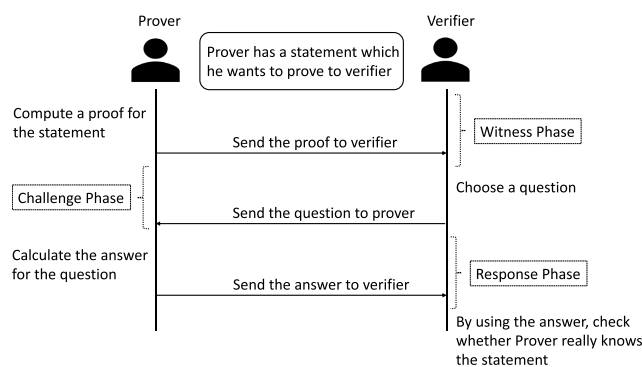


FIGURE 7. An interactive zero-knowledge protocol.

C. ACCESS CONTROL

It is a selective restriction on information or resource based on some policy or criteria. These mechanisms [142] can be enforced to put a restriction or access in the blockchain.

The access can be a read/write access or an access to participate in a blockchain protocol. There are many different access control mechanisms such as role-based, attribute-based, organizational-based access control which can be used in blockchain. Recent incidents show security breaches and data theft from certain blockchain platforms, which can be tackled and prevented by access control. The privacy of data can be ensured in blockchains by using access control [91], [92]. Nowadays, access control techniques are profoundly used in blockchain based medical applications [143] or blockchains for the insurance industry where the data is sensitive information that must be accessible to only trusted and authorized parties. There are different types of access control mechanisms which can be utilized in blockchain applications.

- 1) **Role-based Access Control (RBAC)**: RBAC is an approach for restricting the system view to the users of the system according to their roles in the system. Thus, it can be applied in a blockchain framework where access is provided according to the user roles. RBAC is used in a blockchain based solution for healthcare [144]. A simple example depicted in Figure 8 describes the role-based access control in a private healthcare blockchain. Based on the role, each entity in the blockchain system has its own access rights. A Patient can ask for his personal medical data, however only the Doctor associated with the patient can enter or modify the patient's health record in the blockchain. A Research Company on the other hand can ask for patients' data for any disease for research purpose.
- 2) **Attribute-based Access Control (ABAC)**: In ABAC, the access control rules are based on the attribute structure. These attributes can be user specific, environment-specific or object specific. For example, in a blockchain setup for the insurance industry, 'department' could be an attribute through which the access of the blockchain data is restricted, which means the claims handling department would have a different

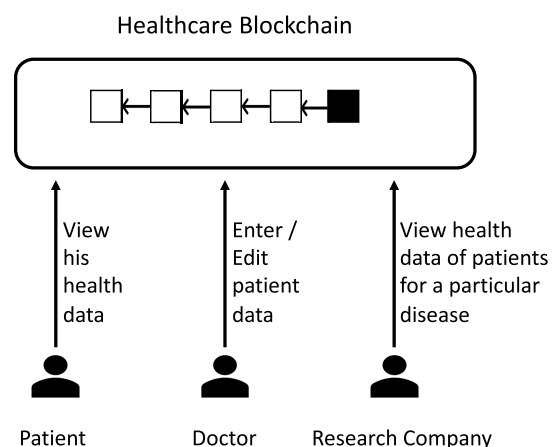


FIGURE 8. Role-based access control in healthcare blockchain.

view of the blockchain compared to the audit department. ABAC can be used in a fair access blockchain model [91] by keeping attributes in policy.

- 3) **Organization-based Access Control (OrBAC):** OrBAC is one of the richest access control models. OrBAC consists of three entities (subject, action, object) which define that some subject has the permission to realize some action on some object. OrBAC has already been used in blockchain for IoT in a fair access blockchain model [91] and in dynamic access control model on blockchain [145].

Other access control mechanisms such as context-based access control and capability-based access control (proposed in blockchain solutions for autonomous vehicles, smart cities, IoT [146]) can also be useful for different blockchain solutions.

D. ENCRYPTION SCHEME

It is a process of encoding a piece of information by which only authorized parties can access it. It can be used to achieve confidentiality of blockchain data by encrypting it. There are many encryption schemes which can be used in blockchain. Symmetric-key Encryption is used in Hyperledger fabric for confidentiality of smart contract [57] and Blockchain for Smart Home [147]. Although searching and computation over an encrypted data is a big challenge, there are many existing techniques which can be used for that purpose. Some of these techniques such as searchable encryption for searching on encrypted data in the cloud is already used in permissioned blockchain [148], and for computation over encrypted data, fully homomorphic encryption and functional encryption can also be utilized in blockchain. Monero cryptocurrency [53] uses (half) additive homomorphic encryption together with range proof techniques, yet supporting only value transactions.

In order to assure simultaneously confidentiality and authenticity of data, an authenticated encryption can be used in blockchain. In authenticated encryption, two peers establish a connection, they both share their public keys and compute the shared secret which is used as the symmetric key for the authenticated encryption algorithm. The recently finished cryptographic competition CAESAR [149] has identified a portfolio of six ciphers for authenticated encryption. So far, as of this writing (June 2019), none of those ciphers has been deployed in some blockchain system.

Broadcast encryption can be used in blockchain to provide the anonymity of blockchain receiver nodes. [150] gives a proposal to use for Availability and Accountability for IoT by blockchain. It has as every user in the group receives the encrypted message, although only users with the correct permission or key can decrypt it.

E. SECURE MULTI-PARTY COMPUTATION (SMPC)

Secure Multi-party Computation enables parties to act together in a way that no single party has an access to all of the data, and hence no one can leak any secret information.

The main idea of SMPC scheme is to jointly compute a function by parties over their inputs without disclosing their inputs. For example, a group of people can compute the average salary of the group without disclosing their actual individual salaries. The blockchain platform Enigma [117] leverages the concept of SMPC to achieve strong privacy. In Enigma platform, a blockchain network is combined with SMPC network, where the blockchain network contains the hashes and SMPC network contains the data corresponding to those hashes which split is among different nodes. For each node, the view over SMPC network differs as everyone has a different piece of information. Specifically, each node contains a random piece of data, and no single party ever has access to the entire data.

A blockchain model Hawk [118] for privacy-preserving smart contracts also specifies the use of SMPC to minimize the trust in the generation of common reference string in SNARK proof used in the model. SMPC can also be exercised for private data storage in a decentralized system, such as Keep [151]. Keep provides a privacy-focused storage solution for Ethereum. In this system, network nodes collaborate to provide secure decentralized data containers, called keeps, which can be accessed from smart contracts on Ethereum.

An application of SMPC can also be seen in the Wanchain [116] Cross-Chain network. Figure 9 reflects the SMPC idea in cross-chain transfer model. In Wanchain network, if user A wants to send an asset (say ETH) from one blockchain (say Ethereum blockchain) to user B on Wanchain blockchain, then at first the asset value is locked in an account on its original chain using smart contract. This locked account holds control of the funds. The equivalent token WETH is sent to another user B of the Wanchain network. When user B wants to convert its WETH to ETH, the locked amount is released from the locked account and sent to user B, and the equivalent portion of WETH is burned. These locking and unlocking of asset value (ETH) happen using SMPC. Wanchain has a concept of Storeman nodes

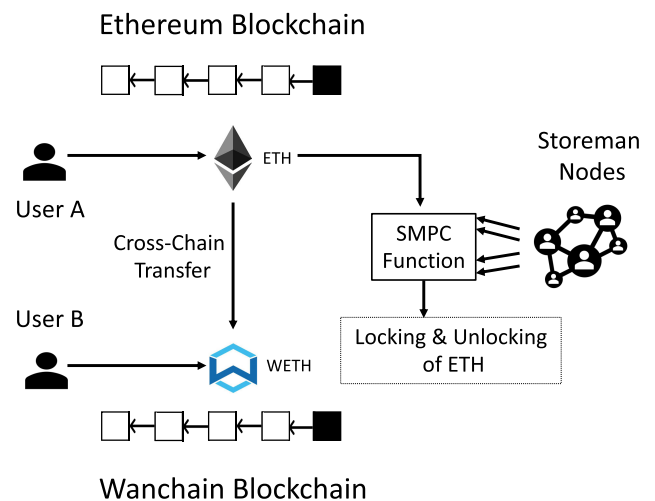


FIGURE 9. Cross-Chain transfer mechanism of blockchain using SMPC.

which work together and perform locking and unlocking of account. These Storeman nodes jointly work together to create public and private key pair of the related locked account. This shared account private key is scattered among the Storeman nodes as pieces of the key. To unlock the account, M out of N ($M \leq N$) Storeman nodes contribute their shares of the private key to generate the signature using MPC jointly.

F. SECRET SHARING

In this concept, a secret is divided into multiple parts among the participants, and it is reconstructed by using a minimum number of parts. These parts are called shares and they are unique for each participant. Secret sharing is used to secure sensitive information. Secret sharing scheme is advantageous in SMPC for distributing the shares among parties. Shamir's secret sharing [152] is already being used to distribute transaction data, without a significant loss in data integrity in blockchain [153]. Decentralized Autonomous Organizations (DAO) can take advantage of secret sharing by distributing the shares of information among the system nodes rather than storing full information in each node. Secret sharing in DAO can be practiced in consensus where each participating node stores a set of shares of the system state rather than storing full system state. These shares are points on polynomials which make up part of the state.

Secret sharing schemes are also used in different off-chain and on-chain bitcoin wallets to safeguard the private keys of the crypto holders. For example, suppose an organization wants to store its bitcoin with a single master private key. In that case, secret sharing scheme helps to store the same key among multiple people. A simple example of this scenario will be sharing a bitcoin wallet key among three people by distributing the shares of the key. These individual shares do not convey any information about the actual key. However, any 2 of 3 people can reconstruct the key using their shares as presented in Figure 10. Secret sharing schemes can also benefit blockchain by storing secret information in a decentralized way so that unauthorized parties cannot access it. Secret sharing is used in blockchain for different purposes such as secret share-based fair and secure voting protocol (SHARVOT) [115] and new cryptocurrency based on mini blockchain [154].

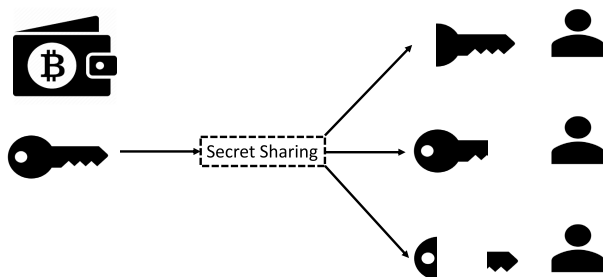


FIGURE 10. Secret-Sharing-Scheme 2-of-3 for a cryptocurrency wallet private key.

G. COMMITMENT SCHEME

A commitment scheme is a digital analog of a sealed envelop. It is a two-phase game between two parties where the phases are commit and open. Commit phase involves hiding and binding of a secret by the first party and send it to the second party; while open is to prove that the first party did not cheat the second party in the commit phase. Therefore, a commitment scheme satisfies the aforementioned two security properties: *hiding* and *binding*. Hiding ensures that the receiver cannot see the message before the open phase, while binding ensures that the sender cannot change the message after the commit phase. The following example shows a binding commitment:

- 1) Pick a secret value s to commit from 0 to $p - 1$ where p is a large prime number;
- 2) Calculate the value $c = g^s \mod p$;
- 3) Publish the value c as a commitment.

In the above example, the binding property follows as it is infeasible for the sender to find any other value y which gives the same c . Here finding the value s from known c , p and g is a computationally hard problem of discrete logarithm but any party can verify the commitment value c if s is provided. There are many commitment schemes such as Pedersen commitment [155] and elliptic curve Pedersen commitment. Zerocoin [124] uses Pedersen commitment to bind a serial number s to Zerocoin z . The commitment c is given as follows:

$$c = g^s h^z \mod p.$$

Here g , h , and p are known to everyone, and the user chooses s , z and computes and publishes the commitment c . These s , z cannot be computed from c even if one is provided. As a consequence, in Zerocoin when the serial number s is published, the user can prove his/her ownership by providing z . Pedersen commitment has also been used to build blockchain-oriented range proof system, Bulletproof [95] and its elliptic curve version is also successfully implemented in Monero [53], [96]. A switch commitment scheme is designed for confidential transactions in blockchain [156].

H. ACCUMULATOR

An accumulator is a one-way function which gives a membership proof without revealing individual identity in the underlying set. This can be used in blockchain to build other cryptographic primitives such as commitment, ring signatures, and zero-knowledge proofs. Merkle tree, used in many cryptocurrencies, fits under a more comprehensive class of cryptographic accumulators which is space and time efficient data structure to test for set membership. Figure 11 shows how blockchain transactions are represented in the Merkle tree, and the Merkle root is stored in the block structure of the blockchain. Non-Merkle accumulators are classified as RSA accumulators and elliptic curve accumulators.

In Zerocoin [124], an accumulator A is computed by the network overall coin commitments (c_1, c_2, \dots, c_n) along

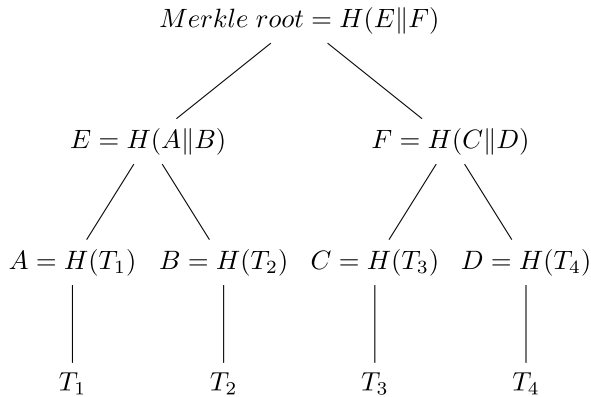


FIGURE 11. Merkle tree of blockchain transactions.

with the appropriate membership witnesses for each item in the set. The witness w is computed by the accumulation coins with the exception of one. In this way, during Zerocoin spend transaction, a user proves the knowledge of one coin by using that witness. This witness w and accumulator A are publicly verifiable without any trusted third party. Accumulator A in Zerocoin is defined as:

$$A = u^{c_1 c_2 c_3 \dots c_n} \mod N,$$

where the integers A , u and N are known to everyone. The coin c is a Pedersen commitment of a coin serial number s and the random number z . Zerocoin uses Random Number Generator (RNG) to generate different s and z to find c using Pedersen commitment until c is prime. The witness w of a coin c is defined as the accumulation of all coins with the exception of c :

$$w = u^{c_1 c_2 c_3 \dots c_n} \mod N.$$

Accumulators can also be employed for range proofs in blockchain. Accumulators are used in [93] to design a stateless blockchain where in order to participate in consensus, the node only needs a constant amount of storage.

I. OBLIVIOUS TRANSFER (OT)

Oblivious Transfer is a two-party protocol between a sender S and a receiver R . The general type of oblivious transfer is k -out-of- n oblivious transfer $\binom{n}{k}$ -OT, where $k < n$, in which S holds n messages and R retrieves simultaneously k of them without letting S know about which k out of n messages R received. Oblivious transfer is introduced by Rabin [157] in which a sender sends a message to a receiver with probability $\frac{1}{2}$. The protocol is called as $\frac{1}{2}$ -OT, and it is as following:

- 1) Sender S chooses two large primes p, q and computes $N = pq$ and then the sender generates RSA public key (e, N) such that e is relatively prime to $(p-1)(q-1)$.
- 2) S computes cipher text c over message M as $c = E_{(e,N)}(M) = M^e \mod N$ and sends e, N, c to receiver R .
- 3) R chooses a random $x \in \mathbb{Z}_{N^*}$ and sends $a = x^2 \mod N$ to S .

- 4) S computes four square roots of $a \mod N$ and chooses one of the roots y at random and sends it to R .
- 5) R checks whether $y^2 \equiv a \mod N$ and if $y \not\equiv \pm x \mod N$, then R will be able to factor N and, hence, be able to decrypt c to recover M .

$\frac{1}{2}$ -OT is complete for secure multi-party computation. Oblivious transfer has been realized in secure multiparty computation to create private and verifiable smart contracts on blockchain [158]. Oblivious transfer can also be utilized for exchange of secrets, private information retrieval, and building protocols for signing contracts. There has been loads of work done in oblivious transfer, and some of these works have been applied in blockchains such as Searchchain [107] and APDB [108] (for automated penalization of data breaches using crypto-augmented smart contracts).

J. OBLIVIOUS RAM (ORAM)

Oblivious RAM is a cryptographic protocol through which a client can safely store his/her data in an untrusted server. The client performs read and write operations remotely. ORAM hides the memory access pattern from the server as well as from outside entities accessing to that part of the data. Therefore, if a client performs two operations of equal length, then the polynomial-bounded adversarial server cannot distinguish between these operations. ORAM bestows freshness, confidentiality of data and integrity so it can be used in various blockchain use-cases and applications. Solidus [105], a protocol for confidential transactions on public blockchain, uses oblivious RAM. Solidus framework operates on a modest number of banks where each bank maintains a large number of user accounts. Solidus introduces a new primitive called Publicly Verifiable Oblivious RAM Machine (PVORM). Most of the previous usage of Oblivious RAM is performed by a single client to outsource storage. In Solidus, ORAM is used to store user account balances and uses PVORM to verify the valid transaction set of a bank. Oblivious RAM is also used in the client-server ORAM protocol [106], Externally Verifiable Oblivious RAM, where Ethereum's automated crypto-currency contracts adjudicate the disputes occurred due to the malicious server by penalizing the server.

K. PROOF OF RETRIEVABILITY (POR)

With the advent of cloud computing, a client might outsource his/her data to the cloud, but still, the client needs a guarantee that the old data has not been modified or deleted. This can be achieved by using proof of retrievability [159] which is an interactive mechanism between a client (verifier) and a server (prover) where the server provides a compact proof to the client that his/her data is intact and he/she can recover the data at any point of time. In this direction, to verify the proof, the client should be equipped with devices having some computational power and network access. This requirement hinders the large-scale adoption of POR by cloud users. To solve this issue, outsource proof of

retrievability (OPOR) [160] is introduced where external auditors verify the POR with the cloud provider on behalf of the clients. OPOR protocol specification uses Bitcoin functionalities for the building blocks.

Permacoin [112] uses proof of retrievability. The primary goal of Permacoin is the distributed storage of archival data. As in Bitcoin's mining mechanism, the client continuously invests his/her computational power, and in addition to the computational power, his/her storage is invested. As a consequence, Permacoin requires storage overhead and high bandwidth consumption. To solve these issues, *Retricoin* [113] is proposed to repurpose the mining work in order to ensure the retrievability of a large file at any point of time. Retricoin also proposes a new algorithm for miners to mine collectively. Storj [114] also uses POR to prove the existence of a fresh copy of a shard on the storer side. As a result, POR can be employed in many cryptocurrencies and blockchain applications.

L. POST-QUANTUM CRYPTOGRAPHY

Recent advances in quantum computing pose a severe threat to classical cryptography, as most of the widely used cryptography is based on the hardness of some problem which can be efficiently solved using quantum computers. Thus, research in the Post-Quantum cryptography [161] has taken a massive leap. The security impact of breaking public key cryptography by quantum computers would be tremendous. Elliptic curve cryptography (ECC), which is an approach to public key cryptography, is mostly used in blockchain applications. Using a variant of Shor's algorithm [162], a quantum computer can easily forge an elliptic curve signature that underpins the security of each transaction in blockchain and so breaking of ECC will affect blockchain in terms of broken keys, hence, digital signatures.

Research in this field is in the rise to create Post-Quantum resistant digital signatures (BPQS) [163] which is a hash-based signature and uses one-time signature (OTS) schemes as a building block. OTS does not depend on any number-theoretic hard problem, and it requires only a secure cryptographic hash function, hence, it is not vulnerable to Shor's algorithm. BPQS has advantages like shorter signatures, faster key generations, and customizable property. Post-Quantum cryptography is also used to design Post-Quantum blockchain [109] using one-time signature chains or to create secure crypto-currency based on Post-Quantum blockchain [110].

For the quantum proof solutions, research is now focused on Lattice-based cryptography [164], multivariate cryptography [165], hash-based cryptography [161], and code-based cryptography [166]. Most of the developed primitives within these areas offer either signatures or public keys that are orders of magnitude bigger than the currently used ones, and that is really a hard research challenge that we formulate as:

Research Problem 11: Construct a new blockchain mechanism that has comparably efficient public key addresses and comparably small digital signatures as the currently

used ones, but that is based on Post-Quantum cryptographic schemes.

M. LIGHTWEIGHT CRYPTOGRAPHY

Conventional cryptographic methods such as RSA and SHA256, work well on systems having reasonable memory and processing power, but these methods are not suitable for devices constrained with memory, physical size, and battery. Conventional cryptographic methods are challenging to implement in resource-constrained devices due to implementation size, large key size, throughput, speed, and energy consumption. Nevertheless, to solve these issues, lightweight cryptography has evolved. Lightweight cryptography targets sensor networks, embedded systems and other variety of resource-constrained devices such as IoT end nodes and RFID tags. Lightweight cryptography is simpler and faster than conventional cryptography but less secure (suffers from many attacks). In IoT, embedded devices having sensors are interconnected through a public or private network. As these are resource-constrained devices, lightweight cryptography solves the issues of communication, memory, and power consumption, but still lacks security. To provide better security, blockchain can be used in conjunction with the sensor network.

Reference [167] reinforces our point to use lightweight cryptography and blockchain for IoT devices to improve security (confidentiality and integrity of IoT device data). A lightweight scalable blockchain (LSB) [102] is also introduced to improve IoT security and privacy. LSB uses a lightweight hash function and lightweight consensus algorithm in order to achieve scalability, security, and privacy. Blockchain is also used to cater security in electric vehicles, cloud and edge computing [103] which use lightweight cryptographic primitives like lightweight symmetric key encryption.

N. VERIFIABLE RANDOM FUNCTION (VRF)

This cryptographic primitive [168] is a pseudorandom function which gives a public verifiable proof of its output based on public input and private key. In short, it maps inputs to verifiable pseudorandom outputs. VRFs can be used to provide deterministic precommitments which can be revealed later using proofs. VRFs are resistant to pre-image attacks unlike traditional digital signature. VRF is a triple of the following algorithms:

- $KeyGen(r) \rightarrow (VK, SK)$. Key generation algorithm generates verification key VK and secret key SK on random input r .
- $Eval(SK, M) \rightarrow (O, \pi)$. Evaluation algorithm takes secret key SK and message M as input and produces pseudorandom output string O and proof π .
- $Verify(VK, M, O, \pi) \rightarrow 0/1$. Verification algorithm takes input as verification key VK , message M , output string O , and proof π . It outputs 1 if and only if it verifies that O is

the output produced by the evaluation algorithm on input secret key SK and message M , otherwise it outputs 0.

In context of blockchain, many Proof of Stake blockchains use VRF to perform secret cryptographic sortition such that electing leader and committee as part of underlying consensus protocol. Proof of Stake blockchain protocols given in [169] use VRF to elect block proposers and voting committee members. Algorand [37] and Witnet network protocol [170] also employ VRF to conduct secret cryptographic sortition. Ouroboros Praos [121] uses VRF on current timestamp and nonce to determine whether a participant is eligible to issue a block. Dfinity [122] network is a decentralized cloud computing resource which uses VRF to generate stream of outputs over time. Thus, the usage of verifiable random function brings many advantages to be exploited in blockchain and opportunities for more research.

O. OBFUSCATION

Obfuscation is a way of transforming a program P into a “Black-box” equivalent of the program $Q = O(P)$ so that P and Q give the same output when the given inputs are same. It should be hard to find out the internal logic or structure of the program once it is obfuscated. Obfuscation aims to make reverse engineering difficult by making the program unintelligible while preserving its functionality. Finding a perfect black-box obfuscation is mathematically impossible. Along these lines, a weaker solution is to find an “Indistinguishability Obfuscation” so that one cannot determine whether the generated output is from the original program or the obfuscated program. A very simplified example for understanding the Indistinguishability Obfuscation, is the following: There are two equivalent programs $P = x * (y + z)$ and $P' = x * y + x * z$. They are obfuscated such that we have $O(P)$ and $O'(P')$. We say that the obfuscated programs O and O' are indistinguishable if on a received output o one cannot determine which of the programs O, O' gave that output.

Obfuscation can be applied for witness encryption, functional encryption, and restricted use of software. It can be applied in blockchain to turn smart contract into a black-box. An obfuscated smart contract can also possess a secret key to decrypt an encrypted input to the smart contract. As a result, publicly running contracts can possess secret data inside it by obfuscating the smart contract. Figure 12 depicts an obfuscated smart contract which stores the private key corresponding to a public key which is used to encrypt the transaction data. It is hard to get the corresponding private key because of the obfuscated smart contract.

One of the very first successful attempts to offer a very limited variant of obfuscation in Bitcoin was the standardization of the “Pay to script hash (P2SH) transactions” [125]. The amounts of Bitcoins in P2SH transactions are sent to a script hash instead of a public key hash. We say that it was a limited variant of obfuscation because in order to spend Bitcoins received via P2SH, the recipient must provide a script that matches the script hash. Still, the successful acceptance of the P2SH transactions without causing a hard fork in Bitcoin

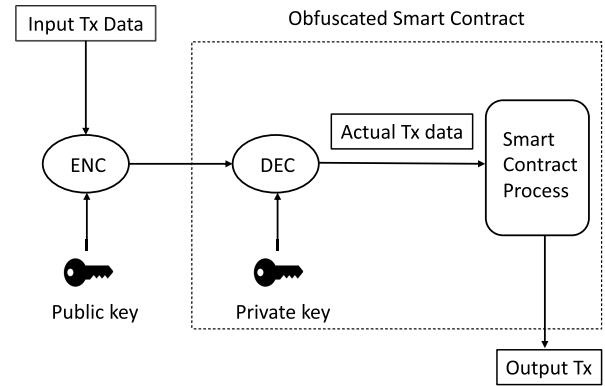


FIGURE 12. An example of smart contract obfuscation.

showed that there is an interest in obfuscation in Blockchain, and that subject is a viable research area.

Research on obfuscation in Bitcoin [104] has been conducted and can be compiled for other cryptocurrencies and blockchain applications. Obfuscation is also used in blockchain for power grid consumption [171] where noise is added to the user’s electricity consumption data through obfuscation, and the electricity consumption data is divided into random and non-random obfuscated data.

As noted in [172] the definition and characteristics of some languages determine how easy is to obfuscate programs written in those languages. For example C, C++, Java and Perl are languages that offer easier program obfuscation. What about scripting languages used in Blockchain? We reformulate this question as a research problem:

Research Problem 12: Study the easiness/hardness of obfuscating programs written in the scripting languages used in the current blockchain systems. Study the feasibility of applying some of the developed obfuscation techniques in C, C++, Java and Perl for the blockchain scripting languages.

VI. PROMISING BUT YET NOT EMPLOYED CRYPTOGRAPHIC PRIMITIVES IN BLOCKCHAIN

This Section construes some cryptographic concepts which are promising candidates to be utilized in blockchain. These cryptographic concepts are not yet well-studied and fully applied in blockchain but constitute of some excellent properties which overlap with some desired properties of blockchain. Therefore, some use cases and blockchain services can benefit from these concepts. The included concepts in this Section have either not at all been studied for use in blockchain or have been studied but not implemented yet. We include references which show some initial ideas how to use these concepts in blockchain, but these references do not give any details about concrete implementation.

A. AGGREGATE SIGNATURE

An aggregate signature allows creating a single compact signature from k signatures on k distinct messages from k distinct signers. It provides faster verification as well

as reduction in storage and bandwidth. As in blockchain, the requirement of storage and computation is high; aggregate signatures can be used for reduction in storage and computation. Aggregate signatures are the non-trivial generalization of multi-signatures (where all users sign the same message). There are two primary mechanisms of signature aggregation: general and sequential aggregation. In order to describe these mechanisms, assume a set of k users having public-private key pair (PK_i, SK_i) and user i wants to sign message M_i .

- 1) In general signature aggregation scheme, each user i (from the group of k users) creates signature σ_i on his/her message M_i . Now to create aggregate signature, anyone can run public aggregation algorithm to take all k signatures $\sigma_1, \sigma_2, \dots, \sigma_k$ and compress them into a single signature σ .
- 2) In sequential signature aggregation scheme, user 1 signs M_1 to obtain σ_1 ; user 2 then combines σ_1 and M_2 to obtain σ_2 ; and so on. The final signature σ is generated by user k which binds M_k and the signature σ_{k-1} . Sequential signature aggregation can only take place during the signing process.

Techniques for aggregating signatures are known for a variety of signature schemes such as DSA, Schnorr, pairing-based, and lattice-based. Aggregate signature schemes should restrict any adversary from creating a valid aggregate signature on his/her own. Aggregate signatures have been proposed for Bitcoin [94], and they can be applied to other cryptocurrencies and blockchain designs.

Research Problem 13: Construct an efficient new signature scheme based on aggregate signatures, that is specifically tailored for blockchain transactions.

B. IDENTITY-BASED ENCRYPTION (IBE)

Identity-Based Encryption first proposed as idea in [173] and later realized as complete cryptographic primitive in [174], allows the encrypting party to use any known (or supposedly known) identity of any receiving party as its public key. Upon receiving the encrypted message, the receiving party asks a trusted third party “Private Key Generator (PKG)” to generate the corresponding private key. Then the receiver decrypts the message using the private key received by PKG. Nowadays, by using identity-based encryption, public keys can be generated using the social identities (Facebook, Twitter, LinkedIn).

There are many flavors and extensions of IBE such as Hierarchical IBE [175], Attribute-based encryption [176], Decentralized attribute-based encryption [177], Functional encryption [178] to name a few.

One of the specifics of IBE is that it replaced the role of the Public-Key Infrastructure with the trusted third party PKG. The presence of a trusted third party somehow defeats the purpose to use it in permissionless blockchain, but still there is a scope to use it in the distributed ledger. Namely, it seems that IBE can be used in permissioned blockchain network. In permissioned blockchain a consortium of trusted

third parties that distribute the private keys to the users can take the role to be IBE PKG. Another variant could be a smart contract layer being responsible for the generation of public-private key pairs inside the PKG using IBE.

We identified that the use of IBE within blockchain has started in [100] as well as in supply chain management [101]. Still, there are a lot of challenges and opportunities for other blockchain applications and services.

Research Problem 14: Construct an IBE based (or IBE related) permissioned blockchain network.

C. VERIFIABLE DELAY FUNCTION (VDF)

Verifiable Delay Function (VDF) is a function $f : X \rightarrow Y$ which takes a prescribed number of sequential steps to compute; however, the output can be easily verifiable by anyone. This delay function prevents malicious miners from computing the random output, and it also provides a short proof which is used during the verification of the output along with previously generated public parameters. Boneh et al. described the concept of VDF [179] as well as illustrated the idea about how it can be applicable to blockchain. VDF can be efficiently used as a way to add a delay in decentralized applications. VDF can be used in the application of decentralized systems such as in leader election process of consensus mechanisms, constructing randomness beacons and proofs of replication.

Delay function was initially implemented in Ethereum prototype [180] where the main idea was verification of delay functions through smart contract by using a multi-round protocol. After this prototype implementation, the concept of verifiable delay function was proposed by Boneh et al. Nowadays several blockchain industries are trying to use VDF in their consensus mechanisms. Chia Network [120] which is open source blockchain is trying to use VDF in its “Proof of space and time” consensus mechanism. Ethereum is also trying to develop a pseudorandom number generator using VDF. In this way, VDF brings opportunities to dig deeper and to be applied in the blockchain domain.

Research Problem 15: [181]: Finding a post-quantum secure simple VDF for the use of blockchain.

D. PRIVATE INFORMATION RETRIEVAL (PIR)

It is a cryptographic primitive in which a client queries to a server and retrieves the corresponding response from the server without exposing query terms as well as response. It is a weaker version of 1-out-of- n oblivious transfer. It can facilitate private blockchain queries to fetch transaction data privately from blockchain. Accordingly, it can be used to find out whether a particular transaction has been appended in the blockchain or can be used to check the transactions associated with the set of public keys and find out the remaining balances. In addition, PIR can be helpful to query transaction data in simplified payment verification (SPV) clients without compromising privacy. PIR requires an adequate amount of processing, but in the future there might be efficient PIR techniques which can be implemented in blockchain. PIR has

also been applied in distributed storage [182] which can be further investigated and adopted in blockchain.

Paper [85] sets several research problems in the area of blockchain transactions privacy and private information retrieval. We rephrase some of the research challenges postulated there:

Research Problem 16: [85]: Develop protocols where non-anonymous users can publish transactions that cannot be linked to their network addresses or to their other transactions.

Research Problem 17: [85]: Develop protocols where non-anonymous users can fetch details of specific transactions without revealing which transactions they seek.

Research Problem 18: [85]: Develop efficient and scalable protocols for anonymous publishing on permissioned blockchains, by combining the asynchronous Byzantine-tolerant consensus protocols for agreeing on transactions with the process of mixing users' announcements.

E. DECENTRALIZED AUTHORIZATION

Authorization and/or hiding sensitive data and actions are essential concepts of resource sharing in open and collaborative environments such as the Internet. Furthermore, in a decentralized form of authorization, parties have full control over their resources and authority to delegate it whether entirely or in part to other parties. An authorization system should provide only as little access to the users as possible to perform their jobs.

Traditional access control is a centralized authorization server which imposes a problem of single point of failure. The centralized authorization scheme has different methods of authorization such as access control list or role-based access.

In comparison, decentralized authorization is more efficient and easier in terms of time, resource and quality. A decentralized authorization system should be well administered to give access privileges to the users. On the negative side, having in mind that the auditing is also a key component of authorization, in a decentralized manner, it is hard to efficiently implement it and to enforce it.

By using blockchain smart contract, some decentralized authorization systems have been designed, e.g., BlendCAC [97] and WAVE [98]. WAVE introduces an authorization layer for the name spaces and resources. Moreover, for the outside entities, a delegation of trust is used to obtain permission on a resource. Decentralized authorization and blockchain can be used to grow each other by combining one another in a specific way.

Research Problem 19: Construct a decentralized authorization protocol for permissioned blockchain that will provide access privileges as well as a delegation of these access to the users.

F. WHITE-BOX CRYPTOGRAPHY

White-box attack is a threat model where the attacker has full visibility of the internal data flow and can modify the data and code. White-box cryptography [183] aims to address the

challenge of implementing a cryptographic algorithm in software in such a way that cryptographic assets remain secure even when subject to white-box attacks. A white-box cryptographic implementation must resist black-box (the attacker has access to only input and output of algorithm), grey-box (side-channel), and also white-box attacks. White-box cryptography is a way to implement cryptographic algorithms like RSA and AES so that the keys remain hidden all the time even during the execution. In some white-box implementations, the key is baked into the code and further concealed to use it in a cryptographic algorithm. In blockchain, it can be used to hide the private key inside the smart contract, and that key can be unlocked when smart contract executes and further it can be used to create a signature.

White-box cryptography can be orchestrated in blockchain to establish trust and privacy of assets. As in blockchain, key and seed secrets are a single point of compromise; these are the highly vulnerable and lucrative targets when stored in memory. To safely store the key, it can be obfuscated in white-box cryptography and further used for encryption/decryption. The implementation of white-box cryptography should be strong enough to facilitate the key storage in blockchain. It has been used in runtime self-protection in a trusted blockchain-inspired ledger [123] and can be promoted in other blockchain applications and services.

G. INCREMENTAL CRYPTOGRAPHY

The idea behind incremental cryptography [184] is if there is a modification to some document M to M' , then the time to update the result upon modification of M should be "proportional" to the "amount of modification" done to M . Incremental cryptography can be used in incremental collision free-hashing or incremental digital signature. The initial idea proposed for incremental cryptography uses the example of a digital signature. The idea was to have a digital signature which is easy to update upon the modification of the underlying message. Suppose M is a message and σ is the corresponding signature. If M is changed to M' by adding/deleting any block, then the time to update the signature from σ to σ' should be "proportional" to the "amount of modification" done to get M' from M .

A proposal for construction of an incremental hash function based on SHA-3 is given in [185], and a private blockchain "Kadena" [99] proposes the use of either Merkle tree or incremental hashing for transaction verification. The concept of incremental hashing in Kadena blockchain is to update the distributed log among the blockchain nodes.

Research Problem 20: Construct a new blockchain mechanism that uses an incremental hash function for updates of the distributed ledger.

H. IDENTITY-BASED BROADCAST ENCRYPTION (IBBE)

IBBE scheme [186] can be considered as a generalization of identity-based encryption scheme (Section VI-B) where instead of having one receiver, there are multiple receivers. In broadcast encryption the users are recognized by their

identities rather than by their public keys. In a multi-receiver setting, IBBE proves as a powerful method to provide data security and privacy. In this scheme, a sender broadcasts the encrypted message to an intended set of users called privilege set. There can be many privilege sets with different cardinalities. A revocable IBEE scheme [187] shows a scenario of IBEE in which the involved players are the key authority, revoked and non-revoked users. In this setting, the decryption key is updated through the release of a key update material by the key authority. These decryption keys are updated only for the non-revoked users. In this scheme, a membership is revoked for a user if he/she is found malicious or his/her keys are compromised. This RIBBE scheme is further implemented in Charm framework [188].

As blockchain is a multi-receiver setting, IBBE can be a propitious candidate to provide transaction data security and privacy. It can also be used in a permissioned blockchain to certify blocks of membership operation logs. RIBBE scheme as being very efficient in terms of computational complexity and communication can work efficiently as well in the case of blockchain.

Research Problem 21: Develop protocols to certify the blocks of membership operation logs in permissioned blockchain setting.

I. OTHER TECHNIQUES

- 1) *Message Authentication Code (MAC)*: It is a short piece of information (known as a tag) to authenticate a message which states that the message comes from the stated sender and it has not been changed. It can be used in blockchain to provide integrity of smart contracts or network data. A blockchain-based system for secure mutual authentication (BSeIn) [189] uses MAC for the authentication.
- 2) *Non-Interactive Witness Indistinguishability (NIWI)*: These are proof systems which are weaker variants of Non-Interactive zero-knowledge (NIZK) proofs. Witness Indistinguishable property states that the verifier cannot distinguish which witness is used to prove the statement by the prover, considering the case of existence of many witnesses. NIWI has been used to construct NIZK over POS based blockchain protocol [190] as well as recently, a new construction of publicly verifiable NIWI proofs from blockchain [191] is also proposed. Hence NIWI proofs bring a new direction to be exploit within the blockchain domain.
- 3) *Position-based Cryptography*: In this cryptographic protocol [192], the identity or the credentials of a party are derived from his/her geographical location. These credentials can be further used for position-based secure communication and position-based authentication. Position-based cryptography has not been applied in blockchain yet, but it looks promising.
- 4) *Elliptic Curve Diffie-Hellman Merkle (ECDHM) addresses*: These addresses [193] can be used to exchange messages privately in the blockchain. It can

be used in blockchain for secure communication among parties. ECDHM address is shared between the sender and the receiver as secret shares, and they use this shared secret to derive anonymous transacting addresses of each other. This address may only be exposed once they have the share to construct these addresses. In this way, it can be used for the privacy of transaction data.

- 5) *Verifiable Secret Shuffle*: It is a variant of a zero-knowledge proofs (an honest-verifier zeroknowledge) proposed in [194]. An initial application of verifiable shuffles has been proposed as a mixing service for Ethereum [195].

VII. CONCLUSION

The goal of this work was to offer a systematic study of available cryptographic concepts and to identify different research directions and problems. Based on these reviewed concepts and associated properties, we hope that the paper will help cryptographers interested in blockchain to choose a challenging research problem and for practitioners to choose a suitable concept for their particular use case.

Current transitions to blockchain enabled solutions by different industries give rise to more research on this technology. Academic and industrial research is focused on making blockchain cost efficient in terms of computational power, memory requirements and security. Many existing cryptographic concepts have been embraced for blockchain use. This paper systematizes the current state-of-the-art knowledge of existing cryptographic concepts used in the blockchain. It also gives a brief description of the used cryptographic concept and points to the available blockchain models that are using that concept. The paper also identifies some concepts which have not yet been used in blockchain but can be beneficial if applied in the blockchain. Apart from existing cryptographic concepts, the paper also presents the basic building blocks of blockchain and how these building blocks are dependent on each other.

Table 5 summarizes all of the cryptographic concepts (used or with potentials to be used in blockchain) presented in this work.

REFERENCES

- [1] S. Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: <http://bitcoin.org/bitcoin.pdf>
- [2] CoinMarketCap. (May 2019). *Total Market Capitalization*. Accessed: Jun. 16, 2019. [Online]. Available: <https://coinmarketcap.com/charts/>
- [3] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Boston, MA, USA: Springer, 1983, pp. 199–203.
- [4] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Proc. Annu. Int. Cryptol. Conf.* Springer, 1992, pp. 139–147.
- [5] R. L. Rivest, A. Shamir, and D. A. Wagner, "Time-lock puzzles and timed-release crypto," Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep. MIT/LCS/TR-684, 1996.
- [6] E. Hughes. (1993). *A Cypherpunk's Manifesto*. Accessed: Apr. 18, 2019. [Online]. Available: <https://www.activism.net/cypherpunk/manifesto.html>

- [7] A. Back, *The Hashcash Proof-of-Work Function*, document Draft-Hashcash-back-00, Internet-Draft Created, Jun. 2003.
- [8] W. Dai. (1998). *B-Money*. Accessed: Apr. 18, 2019. [Online]. Available: <http://www.weidai.com/bmoney.txt>
- [9] N. Szabo. (2005). *Bit Gold*. Accessed: Apr. 18, 2019. [Online]. Available: <https://unenumerated.blogspot.com/2005/12/bit-gold.html>
- [10] N. Satoshi. (Jul. 2010). *RE: They Want to Delete the Wikipedia Article*. Accessed: Apr. 18, 2019. [Online]. Available: <https://bitcointalk.org/index.php?topic=342.msg4508#msg4508>
- [11] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum, Yellow Paper 1e18248, 2014.
- [12] Ether Foundation. (Jan. 2016). *The Ether Denominations are Called Finney, Szabo, and Wei. What/Who are These Named After?* Accessed: Apr. 30, 2019. [Online]. Available: <https://ethereum.stackexchange.com/questions/253/>
- [13] H. Finney. (Mar. 2013). *Bitcoin and Me (Hal Finney)*. Accessed: Apr. 30, 2019. [Online]. Available: <https://bitcointalk.org/index.php?topic=155054.0>
- [14] V. Morabito, *Business Innovation Through Blockchain*. Cham, Switzerland: Springer, 2017.
- [15] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.
- [16] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," 2018, *arXiv:1805.02707*. [Online]. Available: <https://arxiv.org/abs/1805.02707>
- [17] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang, "Cryptographic primitives in blockchains," *J. Netw. Comput. Appl.*, vol. 127, pp. 43–58, Feb. 2019. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S108480451830362X>
- [18] B. Preneel, "The state of cryptographic hash functions," in *School organized by the European Educational Forum*. Berlin, Germany: Springer, 1998, pp. 158–182.
- [19] P. Gallagher and A. Director, "Secure hash standard (SHS)," *FIPS PUB*, vol. 180, p. 183, Mar. 1995.
- [20] A. Regenscheid, R. Perlner, S.-J. Chang, J. Kelsey, M. Nandi, and S. Paul, "Status report on the first round of the SHA-3 cryptographic hash algorithm competition," Inf. Technol. Lab., Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR 7620, 2009.
- [21] E. Heilman, N. Narula, G. Tanzer, J. Lovejoy, M. Colavita, M. Virza, and T. Dryja, "Cryptanalysis of curl-P and other attacks on the IOTA cryptocurrency," in *Proc. IACR Cryptol. ePrint Arch.*, 2019, p. 344.
- [22] E. Heilman, N. Narula, T. Dryja, and M. Virza, "Iota vulnerability report: Cryptanalysis of the curl hash function enabling practical signature forgery attacks on the iota cryptocurrency," Tech. Rep., 2017.
- [23] C. Lee. (2011). *Litecoin*. [Online]. Available: <https://litecoin.org>
- [24] C. Percival, "Stronger key derivation via sequential memory-hard functions," BSCCan, Ottawa, ON, Canada, Tech. Rep., 2009.
- [25] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-hashing for message authentication," Netw. Work. Group RFC, Tech. Rep., 1997.
- [26] D. J. Bernstein, "The Salsa20 family of stream ciphers," in *New Stream Cipher Designs*. Berlin, Germany: Springer, 2008, pp. 84–97.
- [27] V. Buterin, *QuarkCoin: Noble Intentions, Wrong Approach*. Nashville, TN, USA: Bitcoin Magazine, Dec. 2013. Accessed: Jun. 3, 2019.
- [28] M. S. Turan, R. A. Perlner, L. E. Bassham, W. E. Burr, D. H. Chang, S.-J. Chang, M. J. Dworkin, J. M. Kelsey, S. Paul, and R. C. Peralta, "Status report on the second round of the SHA-3 cryptographic hash algorithm competition," NIST Interagency, Gaithersburg, MD, USA, Tech. Rep. 7764, 2011.
- [29] D. Gligoroski, V. Klima, S. J. Knapskog, M. El-Hadedy, and J. Amundsen, "Cryptographic hash function blue midnight wish," in *Proc. 1st Int. Workshop Secur. Commun. Netw.*, May 2009, pp. 1–8.
- [30] E. Duffield and D. Diaz. (2018). *Dash: A Payments-Focused Cryptocurrency*. Accessed: Jun. 3, 2019. [Online]. Available: <https://github.com/dashpay/dash/wiki/Whitepaper>
- [31] Open Source Community at Github. (2018). *ProgPoW—A Programmatic Proof of Work*. Accessed: Jun. 3, 2019. [Online]. Available: <https://github.com/ifdefelse/ProgPOW>
- [32] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, "Consensus in the age of blockchains," 2017, *arXiv:1711.03936*. [Online]. Available: <https://arxiv.org/abs/1711.03936>
- [33] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. NSDI*, 2016, pp. 45–59.
- [34] V. Buterin and V. Griffith, "Casper the friendly finality gadget," 2017, *arXiv:1710.09437*. [Online]. Available: <https://arxiv.org/abs/1710.09437>
- [35] L. Ren, "Proof of stake velocity: Building the social currency of the digital age," White Paper, 2014, pp. 1–13. [Online]. Available: <http://reddcoin.com>
- [36] J. Kwon. (2014). *Tendermint: Consensus Without Mining*. [Online]. Available: <https://tendermint.com/static/docs/tendermint.pdf>
- [37] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proc. 26th Symp. Oper. Syst. Princ. (SOSP)*, New York, NY, USA, 2017, pp. 51–68. doi: 10.1145/3132747.3132757.
- [38] A. Kiayias, I. Konstantinou, A. Russell, B. David, and R. Oliynykov, "A provably secure proof-of-stake blockchain protocol," in *Proc. IACR Cryptol. ePrint Arch.*, 2016, p. 889.
- [39] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in *Proc. 1st Workshop Syst. Softw. Trusted Execution (SysTEX)*, 2016, pp. 2:1–2:6. doi: 10.1145/3007788.3007790.
- [40] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," in *Stabilization, Safety, and Security of Distributed Systems, P. Spirakis and P. Tsigas, Eds.* Cham, Switzerland: Springer, 2017, pp. 282–297.
- [41] I. Bentov, R. Pass, and E. Shi, "Snow white: Provably secure proofs of stake," in *Proc. IACR Cryptol. ePrint Arch.*, 2016, p. 919.
- [42] E. Duffield, H. Schinzel, and F. Gutierrez. (2014). Transaction Locking and Mastermode Consensus: A Mechanism for Mitigating Double Spending Attacks. CryptoPapers.info. Accessed: Jun. 3, 2019. [Online]. Available: <https://cryptopapers.info/assets/pdf/instasend.pdf>
- [43] Libra Association. (Jun. 2019). *The Libra Blockchain*. Accessed: Jun. 24, 2019. [Online]. Available: <https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf>
- [44] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Advances in Cryptology—EUROCRYPT 2015*, E. Oswald and M. Fischlin, Eds. Berlin, Germany: Springer, 2015, pp. 281–310.
- [45] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2016, pp. 142–157.
- [46] A. Biryukov and D. Khovratovich, "Equihash: Asymmetric proof-of-work based on the generalized birthday problem," *Ledger J.*, vol. 2, pp. 1–30, Apr. 2017.
- [47] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.
- [48] D. Schwartz, N. Youngs, and A. Britto, "The Ripple protocol consensus algorithm," Ripple Labs, San Francisco, CA, USA, White Paper 5, 2014.
- [49] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, "Blockchain mining games," in *Proc. ACM Conf. Econ. Comput. (EC)*, New York, NY, USA, 2016, pp. 365–382. doi: 10.1145/2940716.2940773.
- [50] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," 2011, *arXiv:1112.4980*. [Online]. Available: <https://arxiv.org/abs/1112.4980>
- [51] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar, "On bitcoin and red balloons," in *Proc. 13th ACM Conf. Electron. Commerce (EC)*, New York, NY, USA, 2012, pp. 56–73. doi: 10.1145/2229012.2229022.
- [52] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 459–474.
- [53] The Monero Project. (2014). *Monero*. [Online]. Available: <https://web.getmonero.org>
- [54] R. F. A. Britto and D. Schwartz. (2012). *Ripple*. [Online]. Available: <https://ripple.com>
- [55] EOS. IO. (2017). *EOS. IO Technical White Paper*. Accessed: Dec. 18, 2017. [Online]. Available: <https://github.com/EOSIO/Documentation>
- [56] LTO Network. (2014). *Blockchain for Decentralized Workflows*. [Online]. Available: <https://www.lto.network>
- [57] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, New York, NY, USA, 2018, pp. 30:1–30:15.
- [58] (2014). *Monax*. [Online]. Available: <https://monax.io/>

- [59] G. Greenspan. (2015). *MultiChain Private Blockchain*. [Online]. Available: <https://www.multichain.com/download/MultiChain-White-Paper.pdf>
- [60] P. Maymounkov and D. Mazières, “Kademlia: A peer-to-peer information system based on the XOR metric,” in *Peer-to-Peer Systems*, P. Druschel, F. Kaashoek, and A. Rowstron, Eds. Berlin, Germany: Springer, 2002, pp. 53–65.
- [61] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attacks on bitcoin’s peer-to-peer network,” in *Proc. 24th USENIX Secur. Symp. (USENIX Secur.)*, Washington, DC, USA, 2015, pp. 129–144. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/heilman>
- [62] M. Apostolaki, A. Zohar, and L. Vanbever, “Hijacking bitcoin: Routing attacks on cryptocurrencies,” in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 375–392.
- [63] J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, Apr. 2004. doi: [10.1145/997150.997156](https://doi.org/10.1145/997150.997156).
- [64] M. Vasek, M. Thornton, and T. Moore, “Empirical analysis of denial-of-service attacks in the bitcoin ecosystem,” in *Financial Cryptography and Data Security*, R. Böhme, M. Brenner, T. Moore, and M. Smith, Eds. Berlin, Germany: Springer, 2014, pp. 57–71.
- [65] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies,” in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 104–121.
- [66] Bitcoin. (2012). *SPV, Simplified Payment Verification*. Accessed: Jun. 8, 2019. [Online]. Available: <https://bitcoin.org/en/glossary/simplified-payment-verification>
- [67] R. Skudnov. (2012). *Bitcoin Clients*. [Online]. Available: https://www.theusefi/bitstream/handle/10024/47166/Skudnov_Rostislav.pdf
- [68] S. Kadhe, J. Chung, and K. Ramchandran, “SeF: A secure fountain architecture for slashing storage costs in blockchains,” 2019, *arXiv:1906.12140*. [Online]. Available: <https://arxiv.org/abs/1906.12140>
- [69] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, “Network coding for distributed storage systems,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4539–4551, Sep. 2010.
- [70] K. Kralevska, D. Gligoroski, R. E. Jensen, and H. Øverby, “Hashtag erasure codes: From theory to practice,” *IEEE Trans. Big Data*, vol. 4, no. 4, pp. 516–529, Dec. 2018.
- [71] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, “On the locality of codeword symbols,” *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6925–6934, Aug. 2012.
- [72] K. Kralevska, D. Gligoroski, and H. Øverby, “Balanced locally repairable codes,” in *Proc. Int. Sym. Turbo Codes Iterative Inf. Process. (ISTC)*, Sep. 2016, pp. 280–284.
- [73] G. M. Kamath, N. Prakash, V. Lalitha, and P. V. Kumar, “Codes with local regeneration and erasure correction,” *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4637–4660, Aug. 2014.
- [74] D. Gligoroski, K. Kralevska, R. E. Jensen, and P. Simonsen, “Repair duality with locally repairable and locally regenerating codes,” in *Proc. IEEE 15th Int. Conf. Dependable, Autonomous Secure Comput., 15th Int. Conf. Pervasive Intell. Comput., 3rd Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech)*, Nov. 2017, pp. 979–984.
- [75] L. H. White, “The market for cryptocurrencies,” *Cato J.*, vol. 35, no. 2, p. 383, 2015.
- [76] B. McLannahan, “Bitcoin exchange MT GOX files for bankruptcy protection,” *Financial Times*, vol. 28, Feb. 2014.
- [77] M. Huillet. (Aug. 2019). *Vitalik Buterin Talks Scalability: Ethereum Blockchain is Almost Full*. [Online]. Available: <https://cointelegraph.com/news/vitalik-buterin-talks-scalability-ethereum-blockchain-is-almost-full>
- [78] Beam Development Team. *Beam*. 2019. [Online]. Available: <https://www.beam.mw>
- [79] T. Rölfe. (Feb. 2019). *Turing Completeness and Smart Contract Security*. [Online]. Available: <https://medium.com/kadena-io/turing-completeness-and-smart-contract-security-67e4c41704c>
- [80] J. Poon and T. Dryja. (2016). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. Accessed: Jun. 8, 2019. [Online]. Available: <https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf>
- [81] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, “A secure sharding protocol for open blockchains,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2016, pp. 17–30. doi: [10.1145/2976749.2978389](https://doi.org/10.1145/2976749.2978389).
- [82] J. Poon and V. Buterin, “Plasma: Scalable autonomous smart contracts,” White Paper, 2017, pp. 1–47. [Online]. Available: <http://plasma.io>
- [83] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, and J. Timón, and P. Wuille. (2014). *Enabling Blockchain Innovations With Pegged Sidechains*. [Online]. Available: <http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains>
- [84] C. Burchert, C. Decker, and R. Wattenhofer, “Scalable funding of bitcoin micropayment channel networks,” *Roy. Soc. Open Sci.*, vol. 5, no. 8, 2018, Art. no. 180089.
- [85] R. Henry, A. Herzberg, and A. Kate, “Blockchain access privacy: Challenges and directions,” *IEEE Security Privacy*, vol. 16, no. 4, pp. 38–45, Jul./Aug. 2018.
- [86] C. Egger, P. Moreno-Sanchez, and M. Maffei, “Atomic multi-channel updates with constant collateral in bitcoin-compatible payment-channel networks,” in *Proc. Cryptol. ePrint Arch.*, 2019, pp. 1–27. [Online]. Available: <https://eprint.iacr.org/2019/583>
- [87] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei, “Anonymous multi-hop locks for blockchain scalability and interoperability,” in *Proc. NDSS*, 2019, pp. 1–30.
- [88] M. Dong, Q. Liang, X. Li, and J. Liu, “Celer network: Bring Internet scale to every blockchain,” 2018, *arXiv:1810.00037*. [Online]. Available: <https://arxiv.org/abs/1810.00037>
- [89] N. Kshetri, “5G in E-commerce activities,” *IEEE IT Prof.*, vol. 20, no. 4, pp. 73–77, Jul. 2018.
- [90] R. H. N. J. Dewey and R. Plasencia, “Blockchain and 5G-enabled Internet of Things (IoT) will redefine supply chains and trade finance,” in *Proc. Secured Lender*, Jan/Feb. 2018, pp. 43–45.
- [91] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “FairAccess: A new blockchain-based access control framework for the Internet of Things,” *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5943–5964, 2016. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1748>
- [92] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “Towards a novel privacy-preserving access control model based on blockchain technology in IoT,” in *Europe and MENA Cooperation Advances in Information and Communication Technologies*, Á. Rocha, M. Serrhini, and C. Felgueiras, Eds. Cham, Switzerland: Springer, 2017, pp. 523–533.
- [93] D. Boneh, B. Bünz, and B. Fisch, “Batching techniques for accumulators with applications to IOPs and stateless blockchains,” *Cryptol. ePrint Arch.*, Tech. Rep. 2018/1188, 2018.
- [94] Y. Zhao, “Aggregation of gamma-signatures and applications to bitcoin,” *Cryptol. ePrint Arch.*, Tech. Rep. 2018/414, 2018. [Online]. Available: <https://eprint.iacr.org/2018/414>
- [95] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, “Bulletproofs: Short proofs for confidential transactions and more,” in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 315–334. [Online]. Available: <https://ieeecomputersociety.org/10.1109/SP.2018.00020>
- [96] G. Maxwell and A. Poelstra. (2015). *Borromean Ring Signatures*. Accessed: Jun. 8, 2019. [Online]. Available: https://raw.githubusercontent.com/Blockstream/borromean_paper/master/borromean_draft_0.01_34241bb.pdf
- [97] R. Xu, Y. Chen, E. Blasch, and G. Chen, “BlendCAC: A blockchain-enabled decentralized capability-based access control for iots,” 2018, *arXiv:1804.09267*. [Online]. Available: <https://arxiv.org/abs/1804.09267>
- [98] M. P. Andersen, J. Kolb, K. Chen, G. Fierro, D. E. Culler, and R. A. Popa, “Wave: A decentralized authorization system for iot via blockchain smart contracts,” Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2017-234, Dec. 2017. [Online]. Available: <http://www2.eecs.berkeley.edu/Pubs/TechRpts/2017/EECS-2017-234.html>
- [99] W. Martino, “Kadena: The first scalable, high performance private blockchain,” Kadena, Okinawa, Japan, Tech. Rep., 2016.
- [100] S. Wei, S. Li, P. Liu, and M. Liu, “BAVP: Blockchain-based access verification protocol in LEO constellation using IBE keys,” *Secur. Commun. Netw.*, vol. 2018, pp. 1–14, May 2018.
- [101] S. Bose, M. Raikwar, D. Mukhopadhyay, A. Chattopadhyay, and K.-Y. Lam, “BLIC: A blockchain protocol for manufacturing and supply chain management of ICS,” in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber. Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul./Aug. 2018, pp. 1326–1335.
- [102] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “LSB: A lightweight scalable blockchain for IoT security and privacy,” 2017, *arXiv:1712.02969*. [Online]. Available: <https://arxiv.org/abs/1712.02969>

- [103] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, May 2018.
- [104] A. Narayanan and M. Möser, "Obfuscation in bitcoin: Techniques and politics," 2017, *arXiv:1706.05432*. [Online]. Available: <https://arxiv.org/abs/1706.05432>
- [105] E. Cecchetti, F. Zhang, Y. Ji, A. Kosba, A. Juels, and E. Shi, "Solidus: Confidential distributed ledger transactions via PVORM," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2017, pp. 701–717. doi: [10.1145/3133956.3134010](https://doi.org/10.1145/3133956.3134010).
- [106] J. Gancher, A. Groce, and A. Ledger, "Externally verifiable oblivious ram," *Proc. Privacy Enhancing Technol.*, vol. 2017, no. 2, pp. 149–171, 2017. [Online]. Available: <https://content.sciendo.com/view/journals/popets/2017/2/article-p149.xml>
- [107] P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, "Searchchain: Blockchain-based private keyword search in decentralized storage," *Future Gener. Comput. Syst.*, to be published. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0167739X17318630>
- [108] E. V. Mangipudi, K. Rao, J. Clark, and A. Kate, "Automated penalization of data breaches using crypto-augmented smart contracts," *Cryptol. ePrint Arch.*, Tech. Rep. 2018/1050, 2018. [Online]. Available: <https://eprint.iacr.org/2018/1050>
- [109] W. van der Linde, P. Schwabe, A. Hülsing, and Y. Yarom, "Post-quantum blockchain using one-time signature chains," Radboud Univ., Nijmegen, The Netherlands, Tech. Rep., 2018.
- [110] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018.
- [111] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum attacks on bitcoin, and how to protect against them," 2017, *arXiv:1710.10377*. [Online]. Available: <https://arxiv.org/abs/1710.10377>
- [112] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing bitcoin work for data preservation," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2014, pp. 475–490. [Online]. Available: <https://ieeecomputersociety.org/10.1109/SP.2014.37>
- [113] B. Sengupta, S. Bag, S. Ruj, and K. Sakurai, "Retricoin: Bitcoin based on compact proofs of retrievability," in *Proc. 17th Int. Conf. Distrib. Comput. Netw. (ICDCN)*, New York, NY, USA, 2016, pp. 14:1–14:10. doi: [10.1145/2833312.2833317](https://doi.org/10.1145/2833312.2833317).
- [114] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, "Storj a peer-to-peer cloud storage network," Storj Labs, Atlanta, GA, USA, Tech. Rep., 2014.
- [115] S. Bartolucci, P. Bernat, and D. Joseph, "SHARVOT: Secret SHARE-based VOTing on the blockchain," 2018, *arXiv:1803.04861*. [Online]. Available: <https://arxiv.org/abs/1803.04861>
- [116] (2018). *Wanchain*. [Online]. Available: <https://www.wanchain.org>
- [117] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," 2015, *arXiv:1506.03471*. [Online]. Available: <https://arxiv.org/abs/1506.03471>
- [118] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 839–858.
- [119] N. van Saberhagen. (2013). *Cryptonote*. [Online]. Available: <https://cryptonote.org/whitepaper.pdf>
- [120] B. Cohen. (2017). *Chia Network*. [Online]. Available: <https://www.chia.net>
- [121] B. David, P. Gaži, A. Kiayias, and A. Russell, "Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain," in *Advances in Cryptology—EUROCRYPT 2018*, J. B. Nielsen and V. Rijmen, Eds. Cham, Switzerland: Springer, 2018, pp. 66–98.
- [122] T. Hanke, M. Movahedi, and D. Williams, "DFINITY technology overview series, consensus system," 2018, *arXiv:1805.04548*. [Online]. Available: <https://arxiv.org/abs/1805.04548>
- [123] C. Liem, E. AbdAllah, C. Okoye, J. O'Connor, M. S. Ul Alam, and S. Janes, "Runtime self-protection in a trusted blockchain-inspired ledger," in *Proc. ESCAR Eur.*, Nov. 2017, pp. 1–10.
- [124] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 397–411.
- [125] Bitcoin. (2012). *Pay to Script Hash*. Accessed: Jun. 8, 2019. [Online]. Available: https://en.bitcoin.it/wiki/Pay_to_script_hash
- [126] C. Coverdale. (2018). *Scaling Bitcoin: Schnorr Signatures*. [Online]. Available: <https://bitointechtalk.com/scaling-bitcoin-schnorr-signatures-abe3b5c275d1>
- [127] F. Charlon. *Openchain*. [Online]. Available: <https://www.openchain.org/>
- [128] D. Boneh, M. Drijvers, and G. Neven, "Compact multi-signatures for smaller blockchains," in *Advances in Cryptology—ASIACRYPT 2018*, T. Peyrin and S. Galbraith, Eds. Cham, Switzerland: Springer, 2018, pp. 435–464.
- [129] D. Chaum, *Blind Signature System*. Boston, MA, USA: Springer, 1984, p. 153.
- [130] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for bitcoin," in *Financial Cryptography and Data Security*, M. Brenner, N. Christin, B. Johnson, and K. Rohloff, Eds. Berlin, Germany: Springer, 2015, pp. 112–126.
- [131] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions," in *Financial Cryptography and Data Security*, J. Clark, S. Meiklejohn, P. Y. Ryan, D. Wallach, M. Brenner, and K. Rohloff, Eds. Berlin, Germany: Springer, 2016, pp. 43–60.
- [132] F. Zhang and K. Kim, "Id-based blind signature and ring signature from pairings," in *Advances in Cryptology—ASIACRYPT 2002*, Y. Zheng, Ed. Berlin, Germany: Springer, 2002, pp. 533–547.
- [133] S. Meiklejohn and R. Mercer, "Möbius: Trustless tumbling for transaction privacy," *Proc. Privacy Enhancing Technol.*, vol. 2018, no. 2, pp. 105–121, 2018.
- [134] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, "CoinParty: Secure multi-party mixing of bitcoins," in *Proc. 5th ACM Conf. Data Appl. Secur. Privacy*, New York, NY, USA, 2015, pp. 75–86.
- [135] O. Shlomovits and I. A. Seres, "ShareLock: Mixing for cryptocurrencies from multiparty ECDSA," *Cryptol. ePrint Arch.*, Tech. Rep. 2019/563, 2019. [Online]. Available: <https://eprint.iacr.org/2019/563>
- [136] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001. doi: [10.1007/s102070100002](https://doi.org/10.1007/s102070100002).
- [137] S. Josefsson and I. Liusvaara, *Edwards-Curve Digital Signature Algorithm (EDDSA)*, document RFC 8032, Internet Research Task Force, Crypto Forum Research Group, 2017.
- [138] B. Dale. (Aug. 2019). *The Vault is Back: Coder Revives Plan to Shield Bitcoin Wallets From Theft*. [Online]. Available: <https://www.coindesk.com/the-vault-is-back-bitcoin-coder-to-revive-plan-to-shield-wallets-from-theft>
- [139] O. Goldreich and Y. Oren, "Definitions and properties of zero-knowledge proof systems," *J. Cryptol.*, vol. 7, no. 1, pp. 1–32, Dec. 1994. doi: [10.1007/BF00195207](https://doi.org/10.1007/BF00195207).
- [140] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von neumann architecture," in *Proc. 23rd USENIX Secur. Symp. (USENIX Secur.)*, San Diego, CA, USA, 2014, pp. 781–796. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/ben-sasson>
- [141] J. P. Morgan. (2016). *Quorum*. [Online]. Available: <https://github.com/jpmorganchase/quorum>
- [142] R. S. Sandhu and P. Samarati, "Access control: Principle and practice," *IEEE Commun. Mag.*, vol. 32, no. 9, pp. 40–48, Sep. 1994.
- [143] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.
- [144] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, Aug. 2016. doi: [10.1007/s10916-016-0574-6](https://doi.org/10.1007/s10916-016-0574-6).
- [145] A. Outchakoucht, J. P. Leroy, and H. Es-Samaali, "Dynamic access control policy based on blockchain and machine learning for the Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 7, pp. 417–424, 2017.
- [146] S. H. Hashemi, F. Faghri, and R. H. Campbell, "Decentralized user-centric access control using pubsub over blockchain," 2017, *arXiv:1710.00110*. [Online]. Available: <https://arxiv.org/abs/1710.00110>
- [147] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.
- [148] S. Tahir and M. Rajarajan, "Privacy-preserving searchable encryption framework for permissioned blockchain networks," in *Proc. IEEE Perv. iThings, GreenCom, CPSCom SmartData*, Jul./Aug. 2018, pp. 1628–1633.
- [149] D. J. Bernstein. (2014). *CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness*. [Online]. Available: <https://competitions.cr.yt/to/caesar.html>

- [150] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, "Towards better availability and accountability for IoT updates by means of a blockchain," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS PW)*, Apr. 2017, pp. 50–58.
- [151] M. Luongo and C. Pon, "The keep network: A privacy layer for public blockchains," *Keep Netw.*, Tech. Rep., 2018. [Online]. Available: <https://keep.network/whitepaper>
- [152] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979. doi: [10.1145/359168.359176](https://doi.org/10.1145/359168.359176).
- [153] R. K. Raman and L. R. Varshney, "Distributed storage meets secret sharing on the blockchain," in *Proc. Inf. Theory Appl. Workshop (ITA)*, Feb. 2018, pp. 1–6.
- [154] B. F. França, "Homomorphic mini-blockchain scheme," Tech. Rep., 2015.
- [155] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology—CRYPTO'91*, J. Feigenbaum, Ed. Berlin, Germany: Springer, 1992, pp. 129–140.
- [156] T. Ruffing and G. Malavolta, "Switch commitments: A safety switch for confidential transactions," in *Proc. Int. Conf. Financial Cryptogr. Data Secur. Cham, Switzerland: Springer*, 2017, pp. 170–181.
- [157] M. O. Rabin, "How to exchange secrets with oblivious transfer," in *Proc. IACR Cryptol. ePrint Arch.*, 2005, p. 187.
- [158] D. C. Sánchez, "Raziel: Private and verifiable smart contracts on blockchains," 2018, *arXiv:1807.09484*. [Online]. Available: <https://arxiv.org/abs/1807.09484>
- [159] A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2007, pp. 584–597. doi: [10.1145/1315245.1315317](https://doi.org/10.1145/1315245.1315317).
- [160] F. Armknecht, J.-M. Bohli, G. O. Karame, Z. Liu, and C. A. Reuter, "Out-sourced proofs of retrievability," in *Proc. 2014 ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2014, pp. 831–843. doi: [10.1145/2660267.2660310](https://doi.org/10.1145/2660267.2660310).
- [161] D. J. Bernstein, *Introduction to Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 1–14.
- [162] A. Ekert and R. Jozsa, "Quantum computation and shor's factoring algorithm," *Rev. Mod. Phys.*, vol. 68, no. 3, p. 733, 1996.
- [163] K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto, and T. Schroeter, "Blockchain-based post-quantum signatures," in *Proc. IACR Cryptol. ePrint Arch.*, 2018, p. 658.
- [164] O. Regev, "Lattice-based cryptography," in *Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer*, 2006, pp. 131–141.
- [165] J. Ding and B.-Y. Yang, "Multivariate public key cryptography," in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 193–241.
- [166] R. Overbeck and N. Sendrier, "Code-based cryptography," in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 95–145.
- [167] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0167739X17315765>
- [168] S. Micali, M. Rabin, and S. Vadhan, "Verifiable random functions," in *Proc. 40th Annu. Symp. Found. Comput. Sci.*, Oct. 1999, pp. 120–130.
- [169] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, and J. Herrera-Joancomartí, Eds. Cham, Switzerland: Springer, 2017, pp. 297–315.
- [170] A. S. de Pedro, D. Levi, and L. I. Cuende, "Witnet: A decentralized oracle network protocol," 2017, *arXiv:1711.09756*. [Online]. Available: <https://arxiv.org/abs/1711.09756>
- [171] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.
- [172] A. Binstock. (2003). *Obfuscation: Cloaking Your Code From Prying Eyes*. [Online]. Available: <https://web.archive.org/web/20080420165109/http://www.devx.com/microsoft/ISV/Article/11351>
- [173] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Adv. Cryptol.*, G. R. Blakley and D. Chaum, Eds. Berlin, Germany: Springer, 1985, pp. 47–53.
- [174] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology—CRYPTO 2001*, J. Kilian, Ed. Berlin, Germany: Springer, 2001, pp. 213–229.
- [175] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer*, 2005, pp. 440–456.
- [176] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, 2006, pp. 89–98.
- [177] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer*, 2011, pp. 568–588.
- [178] S. Agrawal, S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Functional encryption: New perspectives and lower bounds," in *Proc. Annu. Cryptol. Conf. Berlin, Germany: Springer*, 2013, pp. 500–518.
- [179] D. Boneh, J. Bonneau, B. Bünz, and B. Fisch, "Verifiable delay functions," in *Advances in Cryptology—CRYPTO 2018*, H. Shacham and A. Boldyreva, Eds. Cham, Switzerland: Springer, 2018, pp. 757–788.
- [180] B. Bünz, S. Goldfeder, and J. Bonneau, "Proofs-of-delay and randomness beacons in ethereum," in *Proc. IEEE Secur. Privacy Blockchain (IEEE S&B)*, Apr. 2017, pp. 1–11.
- [181] D. Boneh, B. Bünz, and B. Fisch, "A survey of two verifiable delay functions," in *Proc. IACR Cryptol. ePrint Arch.*, 2018, p. 712.
- [182] S. Kumar, E. Rosnes, and A. G. I. Amat, "Private information retrieval in distributed storage systems using an arbitrary linear code," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 1421–1425.
- [183] S. Chow, P. Eisen, H. Johnson, and P. C. Van Oorschot, "White-box cryptography and an AES implementation," in *Proc. Int. Workshop Sel. Areas Cryptogr. Berlin, Germany: Springer*, 2002, pp. 250–270.
- [184] M. Bellare, O. Goldreich, and S. Goldwasser, "Incremental cryptography: The case of hashing and signing," in *Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer*, 1994, pp. 216–233.
- [185] H. Mihajloska, D. Gligoroski, and S. Samardjiska, "Reviving the idea of incremental cryptography for the zettabyte era use case: Incremental hash functions based on SHA-3," in *Proc. Int. Workshop Open Problems Netw. Secur. Cham, Switzerland: Springer*, 2015, pp. 97–111.
- [186] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *Advances in Cryptology—ASIACRYPT 2007*, K. Kurosawa, Ed. Berlin, Germany: Springer, 2007, pp. 200–215.
- [187] A. Ge and P. Wei, "Identity-based broadcast encryption with efficient revocation," *Cryptol. ePrint Arch.*, Tech. Rep. 2019/038, 2019. [Online]. Available: <https://eprint.iacr.org/2019/038>
- [188] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: A framework for rapidly prototyping cryptosystems," *J. Cryptograph. Eng.*, vol. 3, no. 2, pp. 111–128, 2013. doi: [10.1007/s13389-013-0057-3](https://doi.org/10.1007/s13389-013-0057-3).
- [189] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *J. Netw. Comput. Appl.*, vol. 116, pp. 42–52, Aug. 2018. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1084804518301619>
- [190] R. Goyal and V. Goyal, "Overcoming cryptographic impossibility results using blockchains," in *Theory of Cryptography*, Y. Kalai and L. Reyzin, Eds. Cham, Switzerland: Springer, 2017, pp. 529–561.
- [191] A. Scafuro, L. Siniscalchi, and I. Visconti, "Publicly verifiable proofs from blockchains," in *Public-Key Cryptography—PKC 2019*. Cham, Switzerland: Springer, 2019, pp. 374–401.
- [192] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position based cryptography," in *Advances in Cryptology—CRYPTO 2009*, S. Halevi, Ed. Berlin, Germany: Springer, 2009, pp. 391–407.
- [193] Notes on Bitcoin Privacy Technology, Open Bitcoin Privacy Project. (2019). *ECDHM Address*. [Online]. Available: <http://wiki.openbitcoinprivacyproject.org/topics:ecdhm-address>
- [194] C. A. Neff, "A verifiable secret shuffle and its application to e-voting," in *Proc. 8th ACM Conf. Comput. Commun. Secur.*, 2001, pp. 116–125.
- [195] I. A. Seres, D. A. Nagy, C. Buckland, and P. Burcsi, "MixEth: Efficient, trustless coin mixing service for ethereum," *Cryptol. ePrint Arch.*, Tech. Rep. 2019/341, 2019. [Online]. Available: <https://eprint.iacr.org/2019/341>



MAYANK RAIKWAR was born in Uttar Pradesh, India, in 1994. He received the B.Tech. degree in computer science and engineering from Uttar Pradesh Technical University, in 2013, and the M.Tech. degree in computer science from the Indian Statistical Institute, India, in 2016. He is currently pursuing the Ph.D. degree with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU), since 2019.

In 2017, he joined the Department of Computer Science, Nanyang Technological University, Singapore, as a Research Engineer. His research interests are in cryptography, blockchain, cryptocurrencies, and security.



DANILO GLIGOROSKI was born in Skopje, Republic of Macedonia, in 1967. He received the B.S. and M.S. degrees in applied mathematics from Ss Cyril and Methodius University in Skopje, and the Ph.D. degree in computer science from Ss Cyril and Methodius University in Skopje, in 1997.

From 1997 to 2008, he was an Assistant Professor with the Faculty of Natural Sciences, Skopje University. Since 2008, he has been a Professor of information security and cryptography with the Norwegian University of Science and Technology (NTNU). He is an author of more than 180 scientific publications and more than 10 inventions. His main research interests are in application of various algebraic structures in cryptography, information security, and coding theory.



KATINA KRALEVSKA was born in Skopje, Macedonia, in 1987. She received the B.Sc. and M.Sc. degrees in telecommunications from Ss. Cyril and Methodius University-Skopje, Macedonia, in 2010 and 2012, respectively, and the Ph.D. degree from the Norwegian University of Science and Technology (NTNU), in December 2016.

In 2017, she was a Postdoctoral Researcher with the Department of Information Security and Communication Technology, NTNU. In 2018, she became an Associate Professor with the same department. Since 2019, she has been the Deputy Head of the Department of Information Security and Communication Technology. Her research interests include coding theory, blockchain, and mobile and wireless communications. She is an author of more than 25 scientific publications and more than eight inventions.

...