A Survey of Blockchain: Techniques, Applications, and Challenges

Weichao Gao, William G. Hatcher, and Wei Yu
Department of Computer and Information Sciences
Towson University, Maryland, USA 21252, USA
Emails: {wgao3,whatch2}@students.towson.edu, wyu@towson.edu

***Abstract*—Blockchain, as a mechanism to decentralize services, security, and verifiability, offers a peer-to-peer system in which distributed nodes collaboratively affirm transaction provenance. In particular, blockchain enforces continuous storage of transaction history, secured via digital signature, and affirmed through consensus. In this study, we consider the recent surge in blockchain interest as an alternative to traditional centralized systems, and consider the emerging applications thereof. In particular, we assess the key techniques required for blockchain implementation, offering a primer to guide research practitioners. We first outline the blockchain framework in general, and then provide a detailed review of the component data and network structures. Additionally, we consider the breadth of applications to which blockchain has been applied, broadly implicating Internet of Things (IoT), Big Data, and Cloud and Edge computing paradigms, along with many other emerging applications. Finally, we assess the various challenges to blockchain implementation for widespread practical use, considering the security vulnerabilities to majority attacks, selfish mining, and privacy leakage, as well as performance limitations of blockchain platforms in terms of scalability and availability.**

***Index Terms*—Blockchain, Survey, Emergent Applications, Challenges**

I. Introduction

The unceasing growth of the Internet of Things (IoT) [1], [2], Cloud and Edge Computing [3], [4], and Big Data [5] are rapidly necessitating novel solutions to manage distributed and decentralized systems. Additionally, in the era of those areas, the enforcement of secure, trusted, and verifiable services is paramount, as the volume of network-connected user data and vulnerable devices is unprecedented and increasing. Sadly, trust is in increasingly short supply, as the frequency of data breaches at monolithic software companies continue apace, exposing massive amounts of private information. Centralization, as a key vulnerability of innumerable software architectures, establishes an asymmetric relationship between users and service providers, making individualized management of personal information difficult, while presenting a single point of failure for attackers to exploit.

Blockchain is a distributed and immutable ledger of transactions, in which each transaction is inexorably linked to the prior one. As the primary purpose of the blockchain, operation in untrusted decentralized environments can be secured by both the record of transactions, and decentralized consensus on the validity of the transaction record. In addition, transactions implement operational code, enabling software services between untrusted users. Since first used in cryptocurrencies [6], interest has been increasing as both industry and academics evaluate the applications and operation of the underlying blockchain technologies. Particularly, blockchain has been envisioned as a viable solution to the many needs of emergent applications, including Internet of Things (IoT), Big Data, Cloud and Edge Computing, Identity Management, and many others. Simultaneously, significant work is ongoing in industry to evaluate the efficacy of blockchain for various business applications, and the frameworks themselves are evolving within this atmosphere to realize the potential future needs.

Despite the potential that blockchain raises, it is clearly balanced in favor of securing user privacy, and leaves unresolved many issues regarding platform utilization from the perspective of a service provider, as well as the intrinsic computational overhead of consensus and scalability, which remains a critical challenge for wide adoption. In addition, despite the potential for blockchains to revolutionize distributed and decentralized architectures, in practice there have been some troubling results [7], [8], [9], [10], which need resolution. Just like any software system, vulnerabilities in the encoded implementation or an underlying operating system may create the potential for malicious subversion of users or the entire system. What's more, certain theoretical aspects of the system itself may afford malicious use. From this perspective, it is imperative that a thorough evaluation be conducted to fully consider the implications of the technology.

In this paper, we evaluate the adequacy of current and emerging blockchain technologies in addressing these issues. Particularly, we investigate the underlying concepts of blockchain and relevant techniques, highlight its critical features, and assess the landscape of current platforms and research available. Of practical interest, we investigate blockchain from the perspectives of emergent applications such as IoT, Big Data, and Cloud and Edge computing, as the necessary paradigms that must be served to fully integrate modern computing services, as well as outline the concerns of blockchain for widespread use in terms security and performance.

To be specific, the key contributions of this paper are summarized below: (i) We provide an overview of blockchain technologies, detail a high-level framework from which to assess blockchain, introduce techniques of the data and network layers of the framework, and highlight critical features

978-1-5386-5156-8/18/$31.00 ©2018 IEEE

enabled by blockchain technology. (ii) We provide a thorough assessment of the various areas, in which blockchain has been applied, or in which research is ongoing to apply blockchain for numerous emerging applications, including IoT, big data, cloud and edge computing, identity management, cryptocurrency, economics and markets, business solutions, smart contracts and automation, traceability in supply chains, medical informatics, communication and networking, and others. (iii) We assess two primary challenges to blockchain implementation for widespread practical use: security issues (e.g., majority attacks, selfish mining, anonymity and privacy, abuse of blockchain) and performance issues (e.g., scalability and availability) of blockchain platforms.

The remainder of this paper is as follows. In Section II, we provide an overview of blockchain, outline a high-level framework, and assess the components of the framework in detail. In Section III, we present a review of the investigated applications of blockchain technologies. In Section IV, we highlight areas of concern and limitations of blockchain in practice. Finally, in Section V, we provide concluding remarks.

II. Blockchain

In this section, we first provide an overview of blockchain technologies and detail a high-level framework from which to assess blockchain in general. We then consider the detailed techniques of the data and network layers of the framework, and highlight critical features enabled by blockchain technology.

A. Overview

The concept of the blockchain emerged wholesale, and rather enigmatically, with the emergence of the Bitcoin whitepaper in 2008 [6]. While not unique in the world of open-source software, it is notable that, since the first implementation of Bitcoin around 2009 [11], blockchain, proof-of-work, and the relevant concepts have been continually validated in real-world practice. We do not imply that these technologies are wholly secure or unassailable, but simply that they have been functioning in practice and demonstrate resilience and the intended functionality.

The recent and significant interest in blockchain can be directly attributed to the massive user-base of cryptocurrencies, originating with Bitcoin and many others, and the diversification of blockchain applications by developers already looking to apply decentralized consensus to other tasks. At the end of 2017, cryptocurrencies reached their highest valuation to date [12], and in 2018, we are seeing the aftermath, as regulations on previously unregulated financial technologies and markets are likely to be institutionalized [13].

In light of the increasing interest in blockchain technology, it is our goal to evaluate the viability of current blockchain technologies for utilization in many emerging and unresolved fields. For instance, there is a long history of cryptographically securing systems, such as auctions [14], considering the perspective of untrusted centralized systems as well as malicious adversaries. In our evaluation, it is necessary to consider the operating principles of blockchain and the related mechanisms (digital signature, pubic key cryptography, consensus algorithms, smart contracts, etc.), as well as current implementations of blockchains and their operation in practice.

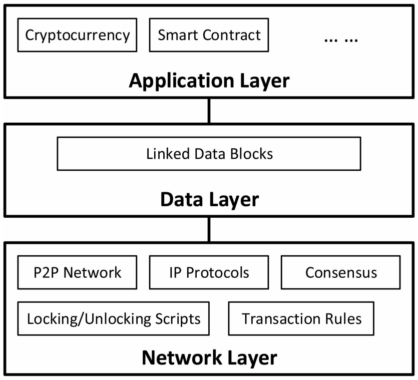

Fig. 1. Blockchain Framework

B. Blockchain Framework

In a narrow sense, blockchain can be considered as a sequence of linked data blocks, each dependent on the prior block, forming a continuous chain-like data structure. In a broader sense, however, blockchain can be considered as the underlying framework that includes a number of necessary and enabling components, such as the interaction environment and applications. More specifically, as can be seen in Fig. 1, we consider a high-level representation of the blockchain framework, subdivided into the network layer, data layer, and application layer.

In the data layer, we have the fundamental unit of the blockchain, defined by leveraging a variety of typical data structures and algorithms, including hash and hash pointer, Merkle tree, digital signature, etc. Note that the design of data structures and algorithms enable the blockchain's well-known features, such as transparency, persistence, decentralization, and more. The network layer is used to enable the interaction environments of the blockchain. These include the decentralized network based on IP protocols and the peer-to-peer (P2P) network, locking and unlocking scripts, and most importantly, the consensus mechanism used for distributed agreement on the validity of blocks. The network layer additionally enables the update and distribution of the blockchain among users. Finally, the application layer presents the various applications that can integrate blockchain to leverage its continuous ledger, consensus among distrusted nodes, smart contracts, and cryptographic components. While relatively new outside the world of cryptocurrencies, blockchain is nevertheless being applied in many areas to meet the growing demands of user privacy and security, as well as distributed and decentralized control.

Using the high-level representation outlined in Fig. 1, we now consider the data and network layers in further detail, highlighting the critical components and their variations. The application layer will be further detailed in Section III.

C. Data Layer

From a data structure viewpoint, the blockchain is a growing list of linked data records, or blocks, which are linked and secured by the application of cryptographic hashes. Each block contains a set of new data records, or transactions, as well as the hash value of the previous block. This hash is what links the current block to the previous one, and, along with a timestamp, makes the modification of records difficult, as they are dependent on the prior record and the current time. The key components and detailed structures that constitute a block are presented as follows:

Data Records (Transactions). As the primary payload in blockchain, lightweight transactions are stored as data records. These transactions are evidence of particular interactions, such as the transfer of funds or the storing of data into a database, occurring at a particular time.

Hash and Hash Pointer. A hash function is used to map the original data (message) to a collection of data of fixed size (i.e., hash value). The features of the cryptographic hash function include collision resistance, pre-image resistance, second pre-image resistance, and puzzle friendliness, Because of these features, hash functions can be applied to verify the integrity of the original message, or as hash pointers, in which the pointer contains the hash of the message that it points to. Fig. 2 shows a linked list structure that applies hash pointers. In this example, each data block contains the hash value of the previous block so that the integrity of all previous data can be verified. In blockchain, hash pointers link each data block, preventing the transaction records from being altered.

Asymmetric Cryptosystem and Digital Signatures. The asymmetric cryptosystem uses the public-secret key scheme by leveraging mathematical problems for which no efficient solution exists. In this cryptosystem, public keys are widely accessible to everyone to encrypt a message that only the key owner can decrypt. Moreover, digital signatures leverage the public-secret key scheme as well. Here, an external user can verify a message encoded with the private key by decoding it with the public key.

In the case of blockchain, the use of digital signatures ensures the provenance of the transactions from one user to the next, as each transaction is connected to the previous transactions. Recall that the basis of blockchain is a continuous history of transactions, collected into larger blocks, hence the name "block-chain". These transactions can be the execution of arbitrary code, or in the case of Bitcoin, the records of coin transfers between users. Fig. 3 illustrates the transactions with digital signatures in blockchain. A transaction in the blockchain requires the issuer to digitally sign a hash of the previous transaction and the receiver's public key. Thus, the transaction issuer can be verified and the receiver is the only one to whom the transaction belongs. In the case of a currency, the receiver is the only one who can issue the next transaction in that transaction chain [15].

Merkle Tree. Fig. 4 illustrates the structure of the Merkle tree. As the hash value in every parent in the Merkle tree depends on its child leaves (and the data blocks in the bottom), it is almost impossible to manipulate one leaf without changing others. Thus, any change to the transaction will affect the hash value all the way up to the Merkle tree root. As a result, the root can be used as an identifier. In blockchain, the transactions (data payload) are recorded using Merkle tree to maintain the integrity of the data.

Data Blocks. A block is a container data structure of fixed size. In the case of cryptocurrencies, blocks often contain many thousands of transactions, and the typical size of a block is on the order of several MB, directly affecting the number of transactions to be processed per second. A block typically consists of both a block header and a block body, as illustrated in Fig. 5. While the implementation may vary from one platform to another, or by application, the block header typically includes: *Block Version* identifying rules the blockchain must follow, *Hash of Previous Block*, *Merkle Tree Root* hash aggregating all hashes of the included transactions, *Timestamp* for traceability, *nBits* (the current hashing target), and *Nonce* used for consensus. In contrast, the block body usually includes the *Transaction Counter* and all of the *Transactions*. The number of transactions a block can have depends on the sizes of the block and each transaction.

BlockChain. Having considered transactions and blocks, the next step up is the collection of blocks to form the blockchain, an immutable ledger that provides traceability. More specifically, a block contains a hash of the prior block (effecting the chain), the collection of transactions hashed via Merkle tree, a timestamp, and a nonce [6]. Note that in the Merkle tree structure, the transactions represent leaf nodes that are each individually hashed, and each set of child hashes are combined and hashed again up the tree until the root is reached. This is used to reduce the storage size of the blockchain by discarding old transactions, and is also effective for verification of the block [16].

Once created, transactions are broadcast throughout the network to be collected and combined into valid blocks. The timestamp thus verifies the transactions existed at the time of creation of the block. The nonce is a one-time-use number that must be calculated, such that when the current block is hashed, the hash value fits some arbitrary criteria, such as beginning with a particular fixed number of zeros. This criteria can then be used to enforce the difficulty in calculating the hash of a block [17]. As the solution is difficult to find but easy to verify, it is suited for determining the correctness of the block in the blockchain [16].

D. Network Layer

We now consider the network layer of the blockchain framework, which introduces the Peer-to-Peer (P2P) network, as well as outlining consensus and its various implementations.

P2P Network. In P2P, the user both utilizes and provides the foundation of the network at the same time, though providing resources is entirely voluntary. Each peer is considered equal and is commonly referred to as a node. Despite all nodes being equal, they can take on different roles within

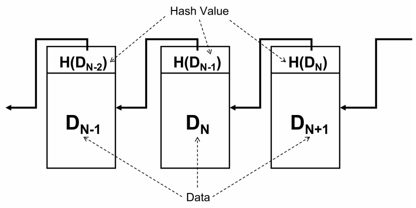

Fig. 2. Hash Pointer

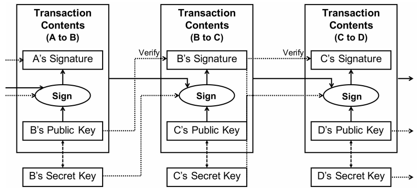

Fig. 3. Transaction with Digital Signature in Blockchain

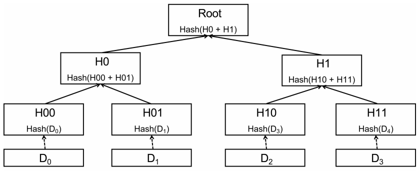

Fig. 4. Merkle Tree

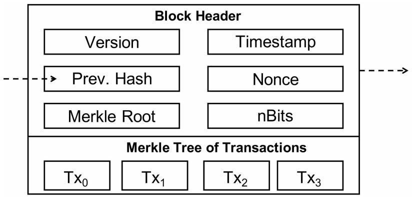

Fig. 5. The structure of data blocks

the blockchain ecosystem, such as that of a miner versus a "full node". In the case of a full node, the entire blockchain is copied to it as long as it is connected to the network. This means that the information stored on a blockchain cannot be lost or destroyed, because to do so would mean having to destroy every single full node on the network. Thus, so long as a single node with a copy of the blockchain exists, all the records will remain intact, providing the possibility to rebuild that network.

Consensus. To enable the decentralization of the blockchain, the nodes involved in conducting transactions and creating blocks must also be able to confirm the validity of blocks as they are added to the chain. In this case, *consensus* among the nodes is a necessity, as there is no trusted centralized system to make such a determination. To achieve such an agreement, various consensus mechanisms have been devised, including *Proof-of-Work (PoW)*, *Proof-of-Stake (PoS)*, *Practical Byzantine Fault Tolerance (PBFT)*, etc. [18]. These variants must achieve the same end, namely the accurate determination of which blocks in the blockchain are correct by checking the work of each block added for validity. The differences lie in who can add blocks and at what rate, and what puzzle is used to implement consensus. Consensus generally implies "mining", or the solving of some difficult problem that is easily verifiable, but not easily overcome.

In the following, we outline the primary examples of the consensus mechanism, and note some limitations.

(i) *Proof-of-Work (PoW).* The concept of Proof-of-Work utilizes a cryptographic computation, and in the general case, this is the determination of a proper nonce that results in a block hash beginning with a particular number of zeros. Only a miner that solves this problem can append a block to the chain, and others need to verify that the work is correct. In addition, different solutions may result in a fork in the blockchain, with a unique solution in each fork. Indeed, the operation of miners in the network is assumed to be Byzantine (arbitrary), and fault tolerance must be achieved. One drawback of this mechanism, however, is that by controlling a subset of miners, it is possible to confirm illegal or improper blocks. In addition, the difficulty of the problem (finding the nonce) cannot be arbitrarily small as the result will be many forks being created at high volume, potentially also resulting in "double-spending". While more efficient PoW mechanisms exist, it inherently requires significant computational expense to ensure accuracy and verifiability.

(ii) *Proof-of-Stake (PoS).* In Proof-of-Stake, the value of a miner's stake in the network (the balance of their account) is locked. As their stake changes, the difficulty of the puzzle changes with it, becoming easier as their stake increases. The result is several high-stake miners that provide efficient consensus. While this has the problem of "nothing-at-stake", in which stake-poor miners conspire to fork the blockchain, there have been several solutions to this, including a system that requires a buy-in or deposit that is withheld if the mining is erroneous [18]. The PoS mechanism has been utilized in Tendermint, Etherium's Casper, and Tezos, among others.

(iii) *Practical Byzantine Fault Tolerance (PBFT).* The PBFT mechanism, unlike PoW, is deterministic, meaning that the inclusion of a block into the blockchain is final. It operates in three phases, requiring network communication to implement [18]. First, in the *Pre-prepare* phase, the leader broadcasts to nodes the intended value to be committed to the blockchain. Next, in the *Prepare* phase, the nodes broadcast the values they intend to commit. Finally, in the *Commit* phase, more than two thirds of the node responses must agree on the value in the Prepare phase for the value to be committed. As consensus requires several rounds of communication, this mechanism in its original form scales poorly. Additional variants include varying the voting power of nodes based on some criteria.

(iv) *Trusted Hardware with Proof-of-Elapsed-Time (PoET).* Trusted hardware mechanisms for achieving consensus provide a viable alternative to reduce mining overhead and are potentially more fault tolerant. Nonetheless, their security is typically dependent on a trusted code base, and requires particular hardware, such as Intel's trusted execution environments (TEEs) [19]. All trusted hardware mechanisms utilize a key pair burned into the hardware that establishes the root of trust, and all code is measured by hashing the content with one of the keys before execution. This is used for remote attestation to certify what is being run on the device [18]. While they may be more energy efficient, the implementations are not as proven as other competing systems.

(v) *Others.* Two other consensus notable algorithms worth mentioning are *Proof-of-Authority* (PoA) and *Proof-of-Burn* (PoB) [18]. In PoA, authority is assigned to particular miners, enabling them to propose new blocks. This is further restricted by assigning time windows to each authority node in a Round-Robin scheme, such that new blocks can only be proposed inside the window. In PoB, a node destroys some currency, coin, or value it owns in order to propose new blocks for acceptance by the blockchain network. This is similar to the buy-in concept in modified PoS.

E. BlockChain Features

Derived from the components of the data and network layers outlined above, blockchain provides several key features to enable unique applications in the application layer.

Fault Tolerance. From the view of the aforementioned network layer, blockchains are inherently decentralized systems with a number of different participants. The actions taken by these participants depend on the available incentives and information. When receiving a newly broadcast transaction, each node (representing a participant) in the decentralized blockchain network has the option to either admit the transaction (adding it to its local copy of the ledger) or ignore it. Consensus can then be achieved once the majority of the nodes decide on a single state. As a result, faults that may occur in a small number of nodes are not likely to change the state of the public ledger, and will be recovered when the consensus state is updated. Under normal circumstances, blockchain is tolerant of even a single fault occurring in many nodes, so long as the total number is less than half all nodes overall.

Attack Resistance. Notice that, in centralized systems, the subversion of a datacenter (by intrusion or hacking) is fatal. In contrast, based on the decentralized P2P network, blockchain has the capability to resist hacking [20]. So long each node in the network maintains a copy of the blockchain, compromised nodes are unable to introduce fraudulent transactions or blocks into the chain. As a result, the integrity of records in the blockchain is secure. Just like fault tolerance, this remains true as long as the number of compromised nodes remains the minority. The consensus of the majority copies of the blockchain provides a reliable backup for the system, as well as for overwriting any hacked version. Another threat in the P2P network is double-spending [20]. That is, when the same coin is used to make more than one payment. When pending transactions are broadcast to the network, there may be delays that cause unconfirmed transactions to be received at different times. In blockchain, the mechanism of proof-of-Work (PoW) addresses the issue by letting nodes solve a complex mathematical problem (i.e., mining) to verify the transaction. Since only the blocks with the correct answers to the complex mathematical problem can be added to the blockchain, redoing the work to change a transaction in a block is difficult. Also, blocks are timestamped, and the earliest transaction with a coin and its owner are all that matters. Other payments with the same fund will be ignored, preventing the funds from being spent twice.

Transparency. As a public ledger, blockchain provides a high level of transparency. By the mechanism of consensus, every entry of the transaction is validated by the majority. Attempts to tamper with or delete the previous transactions will require the consensus of a majority of the system, which is highly unlikely. As a result, every original transaction can be audited.

III. Emerging Applications of Blockchain

We now provide a thorough assessment of the various areas where blockchain has been applied, or where research is ongoing to apply blockchain for emerging applications. Owing to the increasing visibility of Bitcoin and other cryptocurrencies, the diversity of platforms available for blockchain implementation, and the decentralization and verifiability that blockchains afford, research has increased dramatically, affecting a diverse spectrum of applications. These can be subdivided into the categories of Internet of Things (IoT), Big Data, Cloud and Edge Computing, Identity Management, Cryptocurrency, Economics and Markets, Business Solutions, Smart Contracts and Automation, Traceability in Supply Chains, Medical Informatics, Communication and Networking, and Others.

A. Internet of Things

The development of blockchain technologies, and their increasing profile generally, have led many to speculate about their application for IoT. As a decentralized and distributed system for ensuring credibility, this is indeed an attractive possibility. IoT and the related smart-world systems [2], [1], [21], [4], [22], which introduce massively deployed sensors, actuators, and smart electronic devices, are only increasing in volume and scope. Nonetheless, the massive deployment of devices with very limited computing capabilities for the collection and transmission of data raises significant security and privacy concerns. Thus, thorough consideration and evaluation of blockchain as applied to IoT must be carried out from all perspectives.

To this end, there have been some works toward addressing aspects of blockchain for IoT [23], [24], [25], [26]. For example, Dorri *et al.* [23] proposed a blockchain-based framework for smart homes, implementing a tiered system consisting of smart home, cloud storage, and overlay. The smart home consists of local storage, smart home miner, and IoT devices, and maintains a local private blockchain, handling these local components. Xu *et al.* [24] investigated a blockchain-based energy-aware resource management framework for cloud datacenters (DCs). The designed system eschews PoW, PoS, and other proof mechanisms, instead implementing a system in which cloud datacenters, acting as miners, sort the list of miners and eliminate λ previous miners from the list, and the first DC left in the list mines the next block.

Concerning mechanisms and implementation of blockchain holistically, Conoscenti *et al.* [25] conducted a systematic literature review of blockchain for IoT. Their assessment sought to investigate use cases and implementation differences, and the integrity, anonymity, and adaptability of blockchain.

Likewise, Polyzos and Fotiou [26] assessed the security and privacy, sustainability, and trust model challenges of IoT and considered a model in which blockchain-related tasks are offloaded to a network gateway (compatible with the Etherium platform) to overcome the computational limitations of IoT devices.

B. Big Data

Generally speaking, big data is considered data of such great volume, variety, velocity, veracity, value, etc. that traditional data storage, maintenance, and analysis services cannot be applied to handle it [5]. With the advance of computing, data mining, and machine learning [27], big data has seen considerable and widespread adoption as a framework for modern data analytics systems, and is an increasingly mature field. Mechanisms to increase the ability of big data systems to handle and assess big data, as well as generate and collect big data, are increasingly popular. Indeed, the IoT-driven smart-world systems envision the massive generation of unprecedented big data, and are already being deployed with or without thoughtful consideration [5]. Thus, in considering the applications of blockchain technology, the distribution and management of data, and the decentralization of processing and attestation, offer possible avenues for big data technology advancement.

To this end, Karafiloski and Mishev [28] considered blockchain solutions that have emerged to solve challenges in big data, including in the realms of personal data protection, digital property, and IoT. In addition, Smith [29] proposed three primary criteria for assessing the potential of blockchain-based data management: *dependability*, *security*, and *trust*, embodying a taxonomy developed from consideration and combination of various taxonomies and surveyed works. The developed criteria and sub-criteria were then applied to several blockchain managed projects or applications.

Meanwhile, in applying blockchain to particular big data use cases, Kiyomoto *et al.* [30] designed a blockchain-based distributed data trading platform that leverages Hyperledger, in which nodes act as data brokers, receivers, and verifiers. Likewise, Jung and Jang [31] developed a data management and search system that utilizes blockchain by storing the data item name, and IP address, port number, and signature of the data generator in a transaction. By storing the transactions on the blockchain, the transactions can be searched to locate the target data item by name and verify ownership.

C. Cloud and Edge Computing

Cloud computing, and the emerging edge/fog computing paradigm, offer distributed device-agnostic computing and storage services [3], [4], [32]. While cloud computing is considered a semi-centralized architecture that depends on large datacenters, edge computing implements a distributed cloud framework at the network edge, nearby the users. Acting inherently on a distributed set of co-operational hardware systems, the application of blockchain to cloud and edge computing is logical. The primary concerns for applying blockchain to the cloud and edge can be considered as security-driven, based on the ability of blockchain to provide consensus and maintain signed transactions histories. Also, the application of blockchain as a service contract management mechanism is appealing for cloud and edge computing, as it allows autonomous contract execution to users.

Broadly considering the needs of future cloud infrastructure, Sharma *et al.* [33] proposed a blockchain-based architecture for cloud computing that integrates software defined networking (SDN) and edge computing to reduce the need for trusted third party platforms and cloud computing costs. The authors outlined a blockchain-based service provisioning in the cloud, blockchain-connected SDN controllers in fog clusters, SDN-enabled base stations at the edge, and a 2-hop blockchain consensus called Proof-of-Service.

In contrast, focusing on a particular user-side application, Do and Ng [34] proposed BlockDS, an authorized keyword search system for distributed blockchain-based cloud storage. Their system introduces a private blockchain for data owners and consumers, in which access control is conducted anonymously via zero-knowledge cryptographic proof, and data is stored in a decentralized distributed hash table (DHT) maintained by proof-of-retrievability. Distinct from either, Samaniego *et al.* [35] evaluated the use of cloud and fog infrastructures to host blockchain applications for IoT, evaluating IBM's ADEPT system built on Bluemix.

D. Identity Management

Identity management can be considered from the perspectives of both human users and digital entities (devices, hardware, virtual machines, etc.). In both cases, as electronically stored identity criteria are necessary to use various services and products (email, social media, software, etc.), the security of an identity is dependent on both the underlying software systems that house identity data, as well as the communication over which identity must be verified. In the context of access control, the digital signature provides a secure means to verify a user. In considering the application of blockchain in this regard, the cryptographically secure identity can be further enhanced by decentralizing consensus of access and verification transactions.

For instance, in considering identity attestation and management systems, Yasin and Liu [36] developed a blockchain-based identity management and smart contract management system that separately rates personal, professional, and online reputations. The system is designed to secure a user's identity using blockchain while providing attestation of the user by analysis of institutional and social media data. Similarly, Yan *et al.* [37] proposed a BlockChain-based Personal Data Store (BC-PDS) on the existing OpenPDS/SafeAnswers framework to act as notary for secure storage and autonomy-based access control. Specifically, the blockchain was applied to enhance the database of OpenPDS, while an access control system was implemented to improve that of SafeAnswers based on the relationships among authorized users and data owners. Concerning identity as applied to computing devices, Zhu *et* *al.* [38] present BIFIT (Blockchain-based Identity Framework for IoT), an autonomous identity management system for IoT devices. The designed framework utilizes a global blockchain to establish user/device owner identities and create subject appliance identities, and an experimental testbed was built on the Etherium platform.

Considering identity management for access control, Zyskind *et al.* [39] developed a decentralized personal data management system for access control that relies on off-chain DHT storage to give users control of their own data. The authors also consider the use of secure multiparty computing (MPC) and assigning weights to their PoW system based on the actions taken to strengthen their consensus mechanism as future needs. Likewise, Hirotsugu and Tetsuya [40] used directed hypergraphs to study information leakage by inference in read and write access control, and proposed a dynamic access control model with blockchain-managed access logs.

E. Cryptocurrency, Economics and Markets

The first application of blockchain was as a mechanism to record the transactions of digital currencies, and this remains the largest use of the concept to date. As mentioned above, Bitcoin was the first cryptocurrency to gain widespread popularity [6]. Since then, the many variations of blockchain technologies have led to many diverse cryptocurrencies, as well as applications of blockchain in markets and economics. According to the global cryptocurrency benchmarking study [41] in 2017, there are hundreds of cryptocurrencies currently trading in various markets. While the majority of these cryptocurrencies are categorized as "altcoins" and are essentially clones of bitcoin or other coins, simply implementing different parameter values, a small portion of the new offerings have made significant innovations.

For example, Litecoin applied the first new consensus algorithm after Bitcoin's PoW, called Scrypt. It decreases the time interval of generating the blocks to 2.5 minutes, and is considered to be best applied in retail. Other cryptocurrencies that have innovated upon the mechanism of consensus include Peercoin (combining PoW and PoS), Myriad (the first currency to support 5 algorithms), and NXT (only applies PoS). Moreover, another innovation is the use of PoW, beyond *purely* securing the blockchain, to solve complex scientific problems. For example, the PoW system in Primecoin searches for chains of prime numbers, and Curecoin uses its PoW to aid research calculations in protein folding. These innovations are of particular note because they represent the potential application of mining overhead for positive global gain, rather than pure energy consumption, as well as potentially offering dual incentives in the form of mined coins and valuable mathematical data.

F. Business Solutions, Smart Contracts and Automation

Having made waves in stock and investment communities, blockchain technologies have started to spread into business applications thanks primarily to the concept of smart contracts [42]. As the blockchain ledger can store and audit transactions, the ability to execute turing-complete scripts and complex smart contracts is appealing. Furthermore, the ability to arbitrate such contracts can be considered as well, as the record of the transactions can be easily considered. One difficulty in this direction, however, is how to tie smart contracts to the external services, data, or even real-world exchange of goods that they may be intended to represent.

As a unique business application, Nath [43] proposed a blockchain-based framework for insurance intelligence sharing between agencies to combat fraud. Their work considers past attempts to share intelligence data, the insurance claims process, and the dependence of such a framework on the cooperation of multiple businesses of diverse size and competition. Likewise, leveraging smart contract automation, Zou *et al.* [44] proposed a service contract management scheme with a dispute arbitration protocol. In addition, there have been some research efforts on smart contract, including payment management [45], mining protocols [46], [47], fairness validation and correctness verification [48], and platform [49].

G. Traceability in Supply Chain

Supply chains are the necessary interconnection of businesses to bring a product to market, often involving wholly separate entities that depend on mutual honesty abide by regulations and deliver safe products and services. Nonetheless, this system is susceptible to corruption, tampering, falsification, and can be monopolistic when one organization owns the entire supply chain, opaque and asymmetric in relation to end consumers. To combat these difficulties, especially in light of various safety and quality scandals in regulated industries, the implementation of blockchain to ensure traceability and integrity of supply chain regulatory compliance has been raised.

Tian [50], for instance, considered recent food safety and quality scandals in Europe and China, and proposed a supply chain traceability system for agricultural food production based on blockchain. Further, Tian proposed an updated supply chain traceability framework based on IoT and blockchain to ensure broader food safety in general [51]. Also, applied to more generalized traceability, Lu and Xu [52] developed *originChain*, a consortium blockchain platform to provide traceability services and automate regulator compliance. On the blockchain, their platform stores only hashes of traceability certificates and small volumes of organizational and traceability data, offloading raw traceability files to a centralized MySQL database with backups possible for local business storage as well.

H. Medical Informatics

Medical services, as a highly regulated industry, are extremely interested in securing the data collected from patients, especially in the atmosphere of government oversight and mandate. Because of the very sensitive and private nature of such data, significant work has gone into developing highly resilient medical data security frameworks. As a new technology, blockchain has the potential to put the management and transmission of medical data in the hands of patients directly, such that medical history is maintained and searchable, and only authorized care providers can view and store it. Nonetheless, this poses several challenges, as the need for rapid and timely medical history data can be the difference between life and death in an emergency situation.

Taking a broad view of medical data systems, Magyar [53] considers a blockchain-based application model for securing medical data, weighing the costs and incentives of various implementations. In addition, Shae and Tsai [54] proposed a blockchain architecture for medical data sharing and storage applications that necessitates the development of blockchain-enabled management, including data sharing management, anonymous identity management, data storage management, and distributed parallel computing. While the prior works focused on high-level conceptual architectures, researchers have also implemented several frameworks as platforms have matured. For example, Azaria *et al.* [55] utilized Etherium to develop MedRec, a blockchain framework for electronic medical record (EMR) storage, authentication, and sharing. In another implementation, Xia *et al.* [56] designed MedShare, a medical record sharing system for big medical data custodians.

I. Communication and Networking

Closely related to IoT and cloud computing, the application of blockchain for communication and network management has the potential to allow secured and transactionally verified network communication, as well as identity verification. Because mining, necessary for blockchain operation and verifiability, is resource expensive, the implementation of blockchain nodes and components in the network edge provides a more resource rich medium to support transaction and block attestation. In addition, secure communication, encrypted data storage, and smart service contract implementation are further benefits that can be realized with the assistance of blockchain-based networking infrastructures.

For example, Cha *et al.* [57] proposed a privacy-aware Blockchain Connected (BC) gateway to secure IoT devices using the Etherium platform to implement smart contracts. Their system utilizes privacy policies stored as JSON objects and creates smart contracts for both IoT devices, connected by Bluetooth Low Energy (BLE), and BC gateways, which are stored on the blockchain. Also, Yin *et al.* [58] proposed HyperNet, a data-oriented hyperconnected network architecture to replace the traditional Internet structure. Their design includes private data centers (PDCs) as the primary network elements and universal data object identifiers (UDIs) for data object management, and trusted connections are established by smart contracts initiated by blockchain transactions.

J. Others

In addition to the clearly defined categories above, we further consider other emerging areas where blockchain is being applied. In these cases, the application of blockchain is only just beginning to emerge, and little consideration beyond proposed theoretical frameworks have been implemented. These areas include blockchain for managing intellectual property and copyrights, for smart government solutions, and others. For example, as applied to intellectual property, Xu *et al.* [59] proposed a scheme for digital rights management of network media using blockchain. Also, toward applying smart or automated government solutions, Hou [60] considered the practical applications and limitations of blockchain technologies for use in e-government initiatives. Particularly, blockchain provides a promising mechanism to improve the quality and integration of government services, as well as establish individualized identity and credit system.

IV. Emerging Concerns in Blockchain

Despite the voracious interest in blockchain for solving the emerging problems of IoT, Big Data, Cloud and Edge Computing, Identity Management, and many others, especially in the context of decentralization, there remain several key concerns toward wholesale adoption. In this section, we review two primary concerns, those being the security of blockchain systems, and the performance requirements and shortcomings of blockchain implementations.

A. Security Issues

The security of blockchain, just like any other system, is dependent upon the security of its underlying implementation in software and hardware, as well as the protocols and messages required for it to function. On top of this, however, the mechanism of consensus, while considered as a way to ensure fairness and trust in an untrusted system, provides a target for would-be attackers. Additionally, with all transactions being public, privacy leakage is a potential issue. Moreover, because of the immutable nature of the blockchain, any illicit blocks will persist for the lifetime of the blockchain. In the following, we outline several threats against blockchain.

Majority Attack and Selfish Mining. In blockchains, transactions are generally considered immutable after applying the mechanism of consensus and verifying a block in the chain. Nonetheless, majority attacks can be performed when controlling more than 50 % of miners in the blockchain. In this case, the entire process of writing blocks to the chain can be hijacked, and potentially erroneous blocks can be introduced. Moreover, controlling some multiple of the computing capability of all normal nodes even enables an attacker to revise the history of nearly all transactions by forking and providing a revised or falsified history [61].

In contrast to majority attacks, we also consider an attacker who owns less than 50 % of total computational power to still be quite dangerous. Particularly, a strategy called selfish mining [62] and its expansions [9] makes attacks possible. In selfish mining, the attacker (miner) puts mined blocks in a private branch instead of broadcasting them. The private branch is then revealed to the public only when it is longer than the public chain. Once revealed, the longer private chain will replace the current public chain, increasing the mining rewards to the attacker to the detriment of the miners from the original public chain. Motivated by the acquisition of greater rewards, rational miners may tend to join selfish mining pools, increasing the computing power of selfish miners and the ability to mine a longer chain.

Anonymity and Privacy. Blockchain allows its users to make transactions anonymously. Nonetheless, because the transactions are public, there may still be traceable clues that can reveal the identity and private information of users [63]. For example, transactions can be linked to IP addresses to further reveal the user's information, and third part applications tracking a user's multiple profiles, currencies, and data (e.g., trading platforms), may be hacked and subverted. To address the issues in maintaining anonymity in blockchains, several schemes were proposed [10], [64]. The examples include mixing multiple input addresses to multiple output addresses, hiding the amounts and values of coins held by the users in the transaction, etc. Nonetheless, there may be no good solution for securing trading platforms and other third-party software that manages identities and keys, as these can be considered side channels of data loss. In the implementation any blockchain application, or any cryptosystem in general, key management must be carefully considered to prevent this kind of disclosure.

Abuse of Blockchain. In contrast to the potential for privacy disclosure due to the specifics of blockchain implementation, we must also consider the abuses of blockchain in general, outside of the intended use, like other systems [65]. Particularly, the use of cryptographically secure systems provides security for both benign and criminal users alike. As such, Yin and Vatrapu [8] set out to map the Bitcoin ecosystem to provide a first estimation of the size and scope of cybercriminal and illicit activities on the blockchain. Using a dataset of 874 classified observations and some 100,000 unclassified observations provided by *Chainalysis*, the authors applied supervised machine learning using the best performing of 13 classifiers from the Scikit-Learn library. Considering approximately 31.62 % of unique addresses and 28.99 % of total coins in circulation, somewhere between 3.16 % and 5.79 % of the addresses were classified as cybercriminal entities. Also alarming is the insertion of persistent data into the actual blocks of a blockchain, having the potential to leave many users at risk of legal action. A recent investigation by Matzutt *et al.* [7] analyzed the Bitcoin blockchain to assess the threats of arbitrary blockchain content, considering a wide range of data insertion methods (Apertus, CryptoGraffiti, Satoshi Uploader, etc.) that allow for the storage of entire files.

B. Performance Issues

In the context of IoT, Big Data, Cloud and Edge Computing, and other systems, the resource requirements of blockchain technologies raise significant concerns. Specifically, the use of blockchain incurs the need for consensus, and the consensus mechanism is generally resource wasteful. This is problematic when we consider both that decentralization trades compute power and resources for latency gains, and that IoT devices are already resource constrained. In attempting to address this reality, most systems have been designed to implement the blockchain in the most resource rich platform.

Scalability. In previous sections, we have mentioned that the blockchain contains all the transactions over time, which are difficult to alter (except as highlighted above). This design provides persistent data integrity. The clear drawback of this is that, because the number of transactions is continuously growing, the size of the blockchain will increase accordingly. For example, by the end of 2017, the size of the Bitcoin blockchain reached approximately 149 Gigabytes [66]. The result of this continuous growth is not only in the increased cost of storage, but also the reduction in distribution speed of the blockchain over the network. Moreover, in order to leverage the security of the consensus mechanism, public blockchains, such as Bitcoin, usually set a restriction on block size and the time interval of the transactions, resulting in low transaction throughput. Scalability is thus a difficult issue and must be considered in designing blockchain applications.

To address the issue of scalability, Lin *et al.* [10] surveyed a number of proposed schemes, and categorized them into two main methods: (i) storage optimization, and (ii) blockchain redesign. In the former, occupied storage is released by removing old transaction records, or by allowing lightweight nodes to exist. In the latter, data blocks are decoupled into several components, and each is responsible for a particular function or purpose, such as leader election or transaction storage, to balance the block size and security requirements. While these solutions are viable, there remains significant work to be done toward developing a scalable solution that can match existing applications. Furthermore, the application of these solutions may rely on the acceptance of a blockchain version update, which depends on the constituent nodes to agree upon.

Availability. In addition to the scalability of blockchain, the availability of a blockchain system is another potential problem. Specifically, the transaction throughput and latency remain consistent challenges, and as the volume of transactions increases, in general blockchain systems cannot cope. While theoretical analysis of a platform may provide an idea about its performance, only benchmarking and implementation can provide a real-world use analysis.

In considering the performance of blockchain systems in practice, Anh *et al.* [18] developed their BLOCKBENCH framework to analyze blockchains as data processing platforms, using both micro- and macro-benchmarking workloads. The designed framework was used to compare the Etherium, Parity, and Hyperledger blockchains against the in-memory database system H-Store, finding that the throughputs in transactions per second of Parity, Etherium, and Hyperledger were each an order of magnitude apart in order from lowest to highest, and that H-Store was one to two orders of magnitude higher than Hyperledger. In general, they also found Hyperledger to have the highest throughput, fastest execution, lowest peak memory usage, and moderate to low latency, seemingly performing the best of the three.

Likewise, Weber *et al.* [67] considered the availability limitations of Bitcoin and Etherium, and measured the time for transactions to commit. Specifically, they observed that some transactions never commit, due to the blockchain design, noting the inability for abort and retry functions. In addition, Pongnumkul *et al.* [68] conducted a performance analysis of Hyperledger Fabric (HF) and Etherium in private deployment, developing a methodology for blockchain analysis. Their results showed that, while HF consistently performed better across all metrics, including latency and throughput, neither platform can be considered competitive with current database systems in high-workload scenarios.

Considering these results, we can analyze the applicability of blockchain systems based on the target use by considering the number of transactions necessary to be served in a target time frame. In the case of IoT devices, private blockchains may be suitable, as the number of measurements for any single device will be small. Nonetheless, as we scale to larger IoT-based smart-world systems serving massively distributed devices, or big data systems that act on an unprecedented number of data items, the ability to apply blockchain becomes more difficult.

V. Final Remarks

Blockchain is a technology that continues to mature, being already widely implemented in real-world practice for better or worse. The rise of cryptocurrencies and the development of blockchain have afforded a new paradigm for decentralized security and trust in untrusted systems through the consensus mechanism. In this survey, we have considered blockchain technologies from the perspectives of data, network, and application layers, focusing on the operations or implementations of each, and discussed unique features provided by blockchain. We have reviewed relevant research across a variety of applications, and noted that the continuous and immutable record that blockchain provides allows for persistent trust and audit of transactions, and is ideally suited for the distributed nature of IoT, and Cloud and Edge computing, as well as many other fields. Finally, we have considered two particular barriers to the wider application of blockchain technologies, namely security and performance. In particular, the consequences of the consensus mechanisms are novel attack strategies, while the performance of blockchain must increase to be competitive with traditional software implementation. We hope that this survey can provide a roadmap for blockchain-based application development in choosing techniques that are appropriate for their intended application scenarios and business logics, as well as aiding researchers in considering directions for valuable future research.

References

[1] J. A. Stankovic. Research directions for the Internet of Things. *IEEE Internet of Things Journal*, 1(1):3–9, Feb 2014.

[2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao. A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5):1125–1142, Oct 2017.

[3] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu. Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 3(5):637–646, Oct 2016.

[4] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang. A survey on the edge computing for the Internet of Things. *IEEE Access*, 6:6900–6919, 2018.

[5] F. Liang, W. Yu, D. An, Q. Yang, X. Fu, and W. Zhao. A survey on big data market: Pricing, trading and protection. *IEEE Access*, 6:15132–15154, 2018.

[6] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf.

[7] Roman Matzutt, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Müllmann, Oliver Hohlfeld, and Klaus Wehrle. A quantitative analysis of the impact of arbitrary blockchain content on Bitcoin. In *Proceedings of the 22nd International Confer-ence on Financial Cryptography and Data Security (FC)*, 2018.

[8] H. Sun Yin and R. Vatrapu. A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 3690–3699, Dec 2017.

[9] K. Nayak, S. Kumar, A. Miller, and E. Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *2016 IEEE European Symposium on Security and Privacy (EuroS P)*, pages 305–320, March 2016.

[10] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. Blockchain challenges and opportunities: A survey. 12 2017.

[11] Bitcoin core integration/staging tree. https://github.com/bitcoin/bitcoin/.

[12] Cryptocurrency market capitalizations. https://coinmarketcap.com/. Accessed: 2018-04-05.

[13] Oscar Williams-Grut. Here are all the theories explaining the crypto market crash. http://www.businessinsider.com/bitcoin-cryptocurrency-market-crash-explained-causes-2018-1, jan 2018. Accessed: 2018-04-02.

[14] D. An, Q. Yang, W. Yu, D. Li, Y. Zhang, and W. Zhao. Towards truthful auction for big data trading. In *2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC)*, pages 1–7, Dec 2017.

[15] K. Christidis and M. Devetsikiotis. Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4:2292–2303, 2016.

[16] Minhaj Ahmad Khan and Khaled Salah. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395 – 411, 2018.

[17] J. Göbel, H.P. Keeler, A.E. Krzesinski, and P.G. Taylor. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Performance Evaluation*, 104:23 – 41, 2016.

[18] D. T. T. Anh, M. Zhang, B. C. Ooi, and G. Chen. Untangling Blockchain: a data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, PP(99):1–1, 2018.

[19] Alyssa Hertig. Intel is winning over blockchain critics by reimagining bitcoin's dna. https://www.coindesk.com/intel-winning-blockchain-critics-reimagining-bitcoins-dna/, dec 2016. Accessed: 2018-03-02.

[20] Jennifer J. Xu. Are blockchains immune to all malicious attacks? *Financial Innovation*, 2(1):25, Dec 2016.

[21] J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu, and W. Zhao. A real-time en-route route guidance decision scheme for transportation-based cyberphysical systems. *IEEE Transactions on Vehicular Technology*, 66(3):2551–2566, March 2017.

[22] G. Xu, W. Yu, D. Griffith, N. Golmie, and P. Moulema. Toward integrating distributed energy resources and storage devices in smart grid. *IEEE Internet of Things Journal*, 4(1):192–204, Feb 2017.

[23] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 618–623, March 2017.

[24] C. Xu, K. Wang, and M. Guo. Intelligent resource management in blockchain-based cloud datacenters. *IEEE Cloud Computing*, 4(6):50–59, November 2017.

[25] M. Conoscenti, A. Vetrò, and J. C. De Martin. Blockchain for the Internet of Things: a systematic literature review. In *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, pages 1–6, Nov 2016.

[26] G. C. Polyzos and N. Fotiou. Blockchain-assisted information distribution for the Internet of Things. In *2017 IEEE International Conference on Information Reuse and Integration (IRI)*, pages 75–78, Aug 2017.

[27] W. G. Hatcher and W. Yu. A survey of deep learning: Platforms, applications and emerging research trends. *IEEE Access*, pages 1–1, 2018.

[28] E. Karafiloski and A. Mishev. Blockchain solutions for big data challenges: A literature review. In *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*, pages 763–768, July 2017.

[29] T. D. Smith. The blockchain litmus test. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 2299–2308, Dec 2017.

[30] S. Kiyomoto, M. S. Rahman, and A. Basu. On blockchain-based anonymized dataset distribution platform. In *2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA)*, pages 85–92, June 2017.

[31] M. Y. Jung and J. W. Jang. Data management and searching system and method to provide increased security for iot platform. In *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 873–878, Oct 2017.

[32] W. Yu, Guobin Xu, Zhijiang Chen, and P. Moulema. A cloud computing based architecture for cyber security situation awareness. In *2013 IEEE Conference on Communications and Network Security (CNS)*, pages 488–492, Oct 2013.

[33] P. K. Sharma, M. Y. Chen, and J. H. Park. A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access*, 6:115–124, 2018.

[34] H. G. Do and W. K. Ng. Blockchain-based system for secure data storage with private keyword search. In *2017 IEEE World Congress on Services (SERVICES)*, pages 90–93, June 2017.

[35] M. Samaniego and R. Deters. Blockchain as a service for IoT. In *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 433–436, Dec 2016.

[36] A. Yasin and L. Liu. An online identity and smart contract management system. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, volume 2, pages 192–198, June 2016.

[37] Z. Yan, G. Gan, and K. Riad. BC-PDS: protecting privacy and self-sovereignty through BlockChains for OpenPDS. In *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, pages 138–144, April 2017.

[38] X. Zhu, Y. Badr, J. Pacheco, and S. Hariri. Autonomic identity framework for the Internet of Things. In *2017 International Conference on Cloud and Autonomic Computing (ICCAC)*, pages 69–79, Sept 2017.

[39] G. Zyskind, O. Nathan, and A. '. Pentland. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184, May 2015.

[40] K. Hirotsugu and M. Tetsuya. Access control model for the inference attacks with access histories. In *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, volume 2, pages 498–503, July 2017.

[41] Garrick Hileman and Michel Rauchs. Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance*, 2017.

[42] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 839–858, May 2016.

[43] I. Nath. Data exchange platform to fight insurance fraud on blockchain. In *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, pages 821–825, Dec 2016.

[44] J. Zou, Y. Wang, and M. A. Orgun. A dispute arbitration protocol based on a peer-to-peer service contract management scheme. In *2016 IEEE International Conference on Web Services (ICWS)*, pages 41–48, June 2016.

[45] Rami Khalil and Arthur Gervais. Revive: Rebalancing off-blockchain payment networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, pages 439–453, New York, NY, USA, 2017. ACM.

[46] Fan Zhang, Ittay Eyal, Robert Escriva, Ari Juels, and Robbert Van Renesse. REM: Resource-efficient mining for blockchains. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1427–1444, Vancouver, BC, 2017. USENIX Association.

[47] Loi Luu, Yaron Velner, Jason Teutsch, and Prateek Saxena. Smartpool: Practical decentralized pooled mining. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1409–1426, Vancouver, BC, 2017. USENIX Association.

[48] Sukrit Kalra, Seep Goel, Mohan Dhawanand, and Subodh Sharma. Zeus: Analyzing safety of smart contracts. In *Network and Distributed Systems Security (NDSS) Symposium 2018*, San Diego, CA, USA, 2018.

[49] Mustafa Al-Bassam, Alberto Sonnino, Shehar Bano, Dave Hrycyszyn, and George Danezis. Chainspace: A sharded smart contracts platform. *CoRR*, abs/1708.03778, 2017.

[50] Feng Tian. An agri-food supply chain traceability system for china based on RFID blockchain technology. In *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pages 1–6, June 2016.

[51] Feng Tian. A supply chain traceability system for food safety based on HACCP, blockchain Internet of Things. In *2017 International Conference on Service Systems and Service Management*, pages 1–6, June 2017.

[52] Q. Lu and X. Xu. Adaptable blockchain-based systems: A case study for product traceability. *IEEE Software*, 34(6):21–27, November 2017.

[53] G. Magyar. Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. In *2017 IEEE 30th Neumann Colloquium (NC)*, pages 000135–000140, Nov 2017.

[54] Z. Shae and J. J. P. Tsai. On the design of a blockchain platform for clinical trial and precision medicine. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 1972–1980, June 2017.

[55] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. MedRec: using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30, Aug 2016.

[56] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani. Medshare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 5:14757–14767, 2017.

[57] S. C. Cha, J. F. Chen, C. Su, and K. H. Yeh. A blockchain connected gateway for BLE-based devices in the Internet of Things. *IEEE Access*, PP(99):1–1, 2018.

[58] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing. Hyperconnected network: A decentralized trusted computing and networking paradigm. *IEEE Network*, 32(1):112–117, Jan 2018.

[59] R. Xu, L. Zhang, H. Zhao, and Y. Peng. Design of network media 2019s digital rights management scheme based on blockchain technology. In *2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*, pages 128–133, March 2017.

[60] H. Hou. The application of blockchain technology in e-government in china. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–4, July 2017.

[61] Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun. Bitter to better — how to make Bitcoin a better currency. In Angelos D. Keromytis, editor, *Financial Cryptography and Data Security*, pages 399–414. Springer Berlin Heidelberg, 2012.

[62] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography*, 2014.

[63] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. Deanonymisation of clients in bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 15–29, New York, NY, USA, 2014. ACM.

[64] Jan Camenisch, Manu Drijvers, and Maria Dubovitskaya. Practical uc-secure delegatable credentials with attributes and their application to blockchain. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, pages 683–699, New York, NY, USA, 2017. ACM.

[65] Z. Ling, J. Luo, K. Wu, W. Yu, and X. Fu. Torward: Discovery, blocking, and traceback of malicious traffic over tor. *IEEE Transactions on Information Forensics and Security*, 10(12):2515–2530, Dec 2015.

[66] Size of the bitcoin blockchain from 2010 to 2017. https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/. Accessed: 2018-04-20.

[67] I. Weber, V. Gramoli, A. Ponomarev, M. Staples, R. Holz, A. B. Tran, and P. Rimba. On availability for Blockchain-based systems. In *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, pages 64–73, Sept 2017.

[68] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong. Performance analysis of private blockchain platforms in varying workloads. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–6, July 2017.