A survey on security and privacy issues of blockchain technology

Article · January 2018

DOI: 10.3934/mfc.2018007

3 authors, including:

Archana Joshi
Kennesaw State University
1 PUBLICATION **3** CITATIONS

SEE PROFILE

Mathematical Foundations of Computing
©American Institute of Mathematical Sciences
Volume **1**, Number **2**, May **2018**
doi:10.3934/mfc.2018007
pp. **121–147**

A SURVEY ON SECURITY AND PRIVACY ISSUES OF BLOCKCHAIN TECHNOLOGY

Archana Prashanth Joshi, Meng Han* and Yan Wang

Kennesaw State University, Marietta, GA 30060, USA

(Communicated by Zhipeng Cai)

Abstract. Blockchain is gaining traction and can be termed as one of the furthermost prevalent topics nowadays. Although critics question about its scalability, security, and sustainability, it has already transformed many individuals' lifestyle in some areas due to its inordinate influence on industries and businesses. Granting that the features of blockchain technology guarantee more reliable and expedient services, it is important to consider the security and privacy issues and challenges behind the innovative technology. The spectrum of blockchain applications range from financial, healthcare, automobile, risk management, Internet of things (IoT) to public and social services. Several studies focus on utilizing the blockchain data structure in various applications. However, a comprehensive survey on technical and applications perspective has not yet been accomplished. In this paper, we try to conduct a comprehensive survey on the blockchain technology by discussing its structure to different consensus algorithms as well as the challenges and opportunities from the prospective of security and privacy of data in blockchains. Furthermore, we delve into future trends the blockchain technology can adapt in the years to come.

Index Terms– Blockchains, Future Trends of Blockchains, Security, Privacy

1. **Introduction.** Over the past years, the internet has observed the initiation of numerous bottom-up, significant applications that resolve problems in an accommodating and distributed technique. Some of these public and non-profit systems have become well-known and widespread. One question that is ascending with surprising frequency is related to cryptocurrency bitcoin as well as the technology source behind it called Blockchain. Although the research interest attempts to separate blockchain from Bitcoin, the history of the two together is worth to be known. Bitcoin was invented in the year 2008 by Satoshi Nakamoto and the code was released as open source in 2009. Though Satoshi Nakamoto vanished from the forums, code contributions and paper in 2011, irrespective the bitcoin cryptocurrency continued to grow in value and gathered popularity in 2013, the main reason for the increase in popularity was the acceptance of the bitcoin currency by websites and investment driven startups. The bitcoin technology is constantly evolving, and its deployment is susceptible to human infirmities and conflicting standards. While the level of

2010 *Mathematics Subject Classification.* Primary: 90B10, 94A15; Secondary: 94A60.
Key words and phrases. Blockchain, security, privacy, challenge, peer-to-peer.
* Corresponding author: Meng Han.

curiosity towards bitcoin is waning, the opposite is true for blockchain, with cryptocurrency as its technology underneath. As a result, many areas such like banking, business, and government organizations are displaying a mounting interest in the blockchain technology.

Blockchain is a digitized, decentralized, and public ledger of all cryptocurrency transactions. These transactions are documented in a chronological order, helping participants to keep track of digital currency transactions without central record-keeping [17, 3, 22]. Distributed database is one of the key features of blockchain [11]. This kind of database exists in many copies across various computer systems forming a peer-to-peer network, denoting that no solitary, centralized database or server exists [18]. Instead, a blockchain database across the decentralized network of computers exists. Every computer in the network is called a node in the network and every node in the network receives a duplicate copy of blockchain that automatically gets downloaded. Transactions are digitally signed with a public key cryptography that uses two keys, which contains a public and a private key. These two keys are mathematically related to one another. Owing to the complexity of math used, it is almost impossible to guess these keys, making it tougher for the transactions to be cracked. The public key is used to sign and encrypt a message to be sent and the designated recipient can decrypt the message using their private key. To maintain the blockchain database as a "World Wide Ledger" data with respect to all new transactions is propagated to all nodes.

In this paper, we intend to survey the key challenges on the security and privacy issues with regards to the blockchain technology and its future trends. Although many papers are published with respect to the security of blockchain technology and its future trends, no research discusses the various fields that blockchain can be used and how the security and privacy issues can be challenging in those sectors [53, 49]. Every genre of application is using blockchain technology off late and has a different approach to the usage, hence different security and privacy concerns arise. In this paper we discuss various areas of usage of blockchain as well as the related security and privacy issues. Furthermore, we propose some possible solutions that can be used to achieve a more secure and private environment. We compare the research already done and explore the security and privacy challenges and solutions in a systematic and detailed manner.

The authors of [59] and [43] discusses the increase in the number of surveillance and security breaches conceding user privacy [54, 19, 55]. The paper converses about a decentralized personal data management system that guarantees user's ownership and control over his/her data. The blockchain technology is used to develop a protocol for automated access-control while not requiring a central third-party management. [23] and [9] describes the growth in research and industry with respect to Internet of things(IoT) and how the blockchain technology is used to provide security and privacy in the peer-to-peer networks with topologies such as IoT [15, 6]. In [31], the popular blockchain systems such as Ethereum, bitcoin, Monero, and the security threats for blockchain in real time scenarios was deliberates. The work of [2] focused on the vulnerabilities of blockchain cloud [56, 7, 20]. It further examines the capability of blockchain to provide assured data provenance in a cloud environment.

The authors of [24] investigate the tradeoff amid provable security and processing speed of transactions with respect to the block generation rate. This research also introduces an official property of blockchain protocols called chain growth and

argues the security of a robust transaction ledger. The work in [31] explains the unique features of blockchain technology along with its reliable and convenient services [30]. It also discusses the security issues and challenges behind the blockchain technology. In this paper, we demonstrate a thorough understanding on classifying the security and privacy issues of blockchain and provide a comprehensive reference for others who are new to this technology.

The structure of the survey is as follows. In Section 2, we define the concepts of blockchain technology and related techniques used. Section 4 deliberates on the classifications of security and privacy related issues. In Section 5, some of the future challenges and the abundance of opportunities provided with the growth of blockchain technology are explicated with respect to its security and privacy aspects. Finally, Section 6 concludes the paper.

2. **Blockchain: The concept behind it.** Blockchain technology is an amalgamation of many techniques consisting of cryptography, algorithms, economic models and mathematics. It combines peer-to-peer networking and distributed consensus algorithms to solve the synchronization issues from traditional distributed database as discussed in [13].

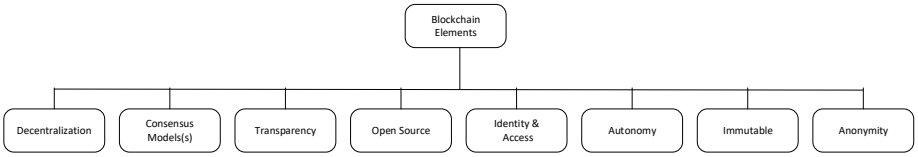

FIGURE 1. Illustration of Blockchain Elements

2.1. **Elements of blockchain technology.** There are several elements of blockchain and the eight most significant elements are discussed in this section. These elements are illustrated in Figure 1 and are explained as follows.

2.1.1. *Decentralization.* Decentralization is the dispersion of functions and controls from a central authority to all the units involved. In blockchain a centralized authority is not available. Instead, every blockchain user (miner) is provided with a copy of the transaction ledger and a new block is added by validating transaction by the miners involved. In a decentralized environment the network operates on a peer-to-peer (user-to-user) basis. The researchers in [50] use this element of blockchain as one of the major aspects in developing Ethereum digital currency.

2.1.2. *Consensus model(s).* The consensus model(s) help preserve the sanctity of data recorded on blockchain. In [42], it is reported that various consensus mechanisms and issues could result when the consensus mechanism fails including blockchain forks, consensus failures, dominance issues, validating nodes and deficient performance of the blockchain network [1]. A consensus protocol has three properties based on applicability and efficiency:

a). Safety: A consensus protocol must be safe and consistent, meaning that all nodes should produce the same output which is valid in accordance with the protocol rules.

b). Liveness: A consensus protocol promises liveness of all non-faulty nodes to yield a value.

c). Fault Tolerance: A consensus protocol provides tolerance while providing recovery to a failure node participating in consensus.

2.1.3. *Transparent.* The blockchain network routinely checks in with itself every ten minutes in order to self-audit the ecosystem of a digital value, which reconciles transactions that happen in ten-minute intervals. A collection of these transactions is referred to as a "block". Two resulting properties, transparency and inability of corruption, are generated.

2.1.4. *Open source.* A decentralized and closed-source application needs user to trust that the application is decentralized and the data cannot be accessed from a central source. Closed-source applications act as a barrier to adoption by users. The repugnance to a closed source network is noticeable when the application is intended to receive, hold, or transfer user funds. Even though it is possible to launch a closed-source decentralized application, the level of the difficulty to achieve the desired result would be catastrophic, making it obvious for the users to favor open source participants. Open sourcing a decentralized application modifies the structure of business practices who used to favor the Internet as the common denominator.

2.1.5. *Identity and access.* The identity and accessibility of a blockchain are related to three main criteria including public or permissionless, private or permissioned, and consortium. These criteira of blockchain was discussed in detail in [39]. A private blockchain restricts the users from having the authority to validate block transactions and create smart contracts. This is appropriate for the traditional businesses and governance models [16]. Public blockchains are designed to cut the middleman out in transactions while keeping the security intact. In public blockchains any user with access to internet can join the network by participating in block verifications and creating smart contracts. Consortium blockchains are partly private and allows a few predetermined selective nodes to have full control. It is a substitute for allowing any random user with an internet connection to verify transactions. The platform like private blockchain provides efficiency and privacy of transactions.

2.1.6. *Autonomy.* The main objective of blockchain technology is to switch the trust from one centralized authority to the whole network without interference. Every node in the blockchain system can transfer and update information securely. A decentralized autonomous organization (DAO), which is frequently categorized as decentralized autonomous corporation (DAC), is explained as an organization that follows a set of rules prearranged as computer programs and termed as smart contracts. The transaction record and smart contract details are maintained as blocks in blockchain.

2.1.7. *Immutability.* Immutability is something that is unchanging over a period. In the context of blockchain, immutability is relevant to data or information stored in the blocks. Once the data or information is written in a block of blockchain nobody can alter it. This is highly essentially beneficial for auditing data. On one hand, the provider of data can verify that the data is secure, efficient, and has not been tampered with or altered. On the other hand, the recipient of data is confident that data is authentic and unaltered. The immutability element of blockchain is extremely beneficial for databases used in financial transactions since the records are reserved forever and cannot be hanged unless somebody takes control of more than 51% of the nodes in the network simultaneously.

2.1.8. *Anonymity.* [38] explains the anonymity element of blockchain technology. The blockchain address of a miner is necessary for this element and no other detail is required, resulting in anonymity resolving trust issues. Anonymity of an entity inside a set of entities is not distinguishable. In a communication system, the anonymity set can be divided into two sets: the sender sets and the recipient sets.

2.2. **Working of blockchain.** Blockchain is a public ledger involving various processes and the working of blockchain includes several processes discussed as follows:

1. The node or user who wants to initiate a transaction would record and broadcasts the data to the network.
2. The node or user who receives the data verifies the authenticity of the data received in the network. Then the verified data is stored to a block.
3. All nodes or users in the network validate the transaction by executing either the proof of work algorithm or the proof of stake algorithm to the block that needs validation.
4. Consensus algorithm used by the network will store the data to the block that is added to blockchain. And all nodes in the network admit the respective block and extend the chain base on the block.

2.3. **Structure of blockchain.** Blockchain technology is expected to greatly impact approximately all industries in the near future. Financial establishments are developing in ingenious ways to start testing and investing in this technology, making it extremely significant for everyone to understand the structure as well as the working algorithm of the blockchain technology. A blockchain is a continuously growing list of records called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. The structure of blockchain data is efficient and the adjoin list of transaction blocks can be maintained in a modest database or in the form of flat files. These blocks are connected to each other, with each block referring to the previous one in the chain. The first block in the chain is called a genesis block. The blockchain is envisioned as a vertical stack and the blocks are stacked on top of one another with the genesis block being the base of the stack. [58, 33] discusses the structure of blockchain in detail. It is pointed out that all blocks are recognized by cryptographic hash values created by SHA256 algorithm and these hash values are part of the block header.

Granting that a block at any given point has one parent, it can transitorily have multiple children. Every child block in the chain refers to the same block as its parent and has the same parent hash value. Although the multiple children situation occurs mainly when a blockchain fork is encountered, as soon as the fork is resolved and the valid block is determined, the blocks in the fork would be orphaned and not pursued in the future. The identity of child blocks depends on the parent block identity and varies accordingly. Then the hash value of the parent block changes. As a result, the preceding block hash pointer of the child block is changed. This process continues until reaching each of the grandchild blocks. The cascade effects make sure that once a block has many generation, it cannot be meddled without compelling recalculations of all the consecutive blocks.

The structure of the blockchain is illustrated in Figure 2 and described as follows.

- Data. The data stored in the blockchain depends on the service and the application. It could be used in a peer-to-peer file system such as IPFS, in distributed databases such as apache Cassandra, in cloud file storage such as

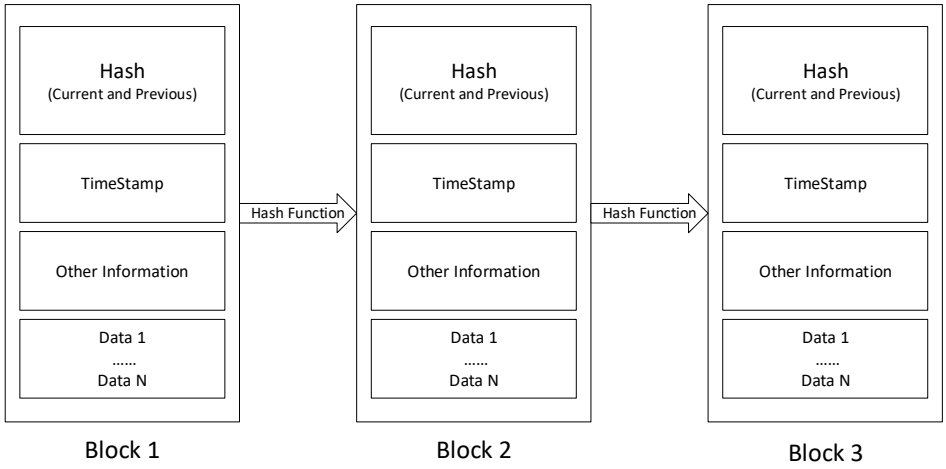

FIGURE 2. Blockchain Structure

storj, and Ethereum swarm, sia etc. The data stored can be used in various applications like recording the transaction details, banking, contracting and IoT.

- Hash. A hash function is the one that takes an input of any length and generates the output with unique fixed length. If a single value in the input is modified, the output is extremely different. Hash functions are used ubiquitously in the blockchain technology. Each block containing data is hashed and the changes could be big or small. For instance, a user named Alex tries to change the data stored in a block. Then the modified block will have a completely different hash value, assuring that every node or miner in the network would have knowledge of the modification made by updating the ledger copy of all users. This can increase the trustworthiness of data stored in blockchains. In a hash tree or Merkle tree every node is represented as a leaf and is labelled with a block. This Merkle tree permits the user to store large data structures in a secure and efficient way.
- Timestamp. It is necessary to record the time when the block was created. Timestamping is a method used to track the creation or modification time of a document in a secure way. This method is becoming an essential tool in the business world today since it permits the involved parties to identify the origin and availability of a document on a particular date and time.
- Other Information. Other information contains digital signatures, nonce values, nBits and a few other user defined values. Every user has two keys, a private and public key. A digital signature containing these two keys is involved in both signing phase and verification phase. The private key is kept confidential and is used to sign a transaction to encrypt the data. The public key is known by everyone and is used to validate and decrypt the data in the verification phase of the transaction, consequentially confirming data authenticity. A nonce value is basically a 4-byte value starting with 0 and increments each time a hash calculation is performed. The nbits value determines the target threshold value of a valid block hash as explained in [58, 46].

2.4. **Consensus algorithms.** Byzantine Generals (BG) problem was discussed in [25] in detail. The BG problem arose because of a set of generals who were commanding a percentage of Byzantine army circled the city. Some of the commanding generals favored the option of attacking the city while the other generals preferred the option of retreating. Nevertheless, the attack would be unsuccessful if only a part of the generals attacked the city. Therefore, a major challenge is that a consensus on attack or retreat had to be reached in a disseminated environment. This is also the challenge faced by blockchain, since the blockchain network is distributed with no central authority or central node present. A few consensus algorithms are shown in Figure 3 and they are discussed later in this section.

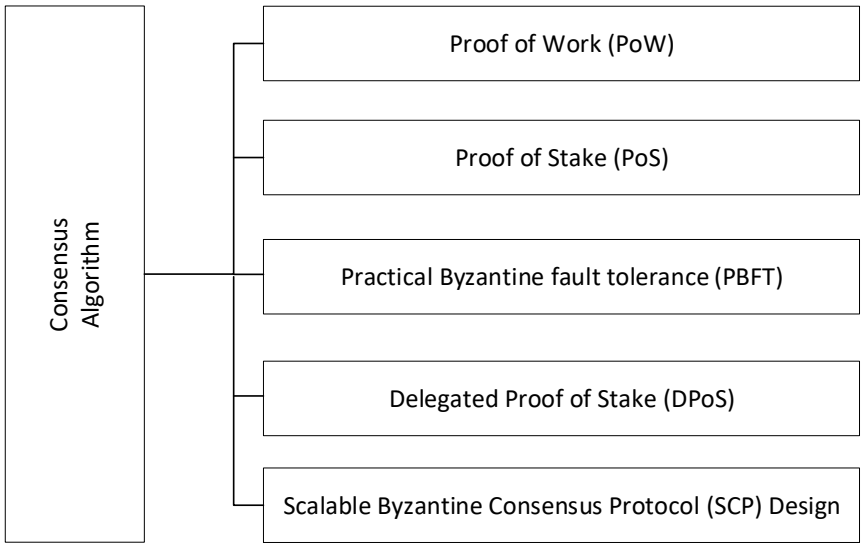

FIGURE 3. Consensus Algorithms

1) Proof of Work (PoW). Proof of Work (PoW) protocol is a fiscal measure to discourage the attacks of Denial of Service and other network service exploitations such like spams that eat up the processing time of computer [48, 2]. In blockchain, somebody is nominated to record the transactions by selecting a random user or node. However, this leads to vulnerability attacks. If a node desires to publish a block with transactions, a lot of computational calculations need to be done to verify the random user or node selected. In PoW, nodes that calculate hash values are called miners. Every node in the network calculates the hash value of block header that contains a nonce. Then the miners change this value frequently to generate different hash values. This protocol entails that the calculated values be equal to or smaller than a specified value. Once a node reaches the target value, it broadcasts the block to other nodes and they in turn confirm the accuracy of the hash value. If a block is authenticated, other nodes add this new validated block to their own blockchain. The process of calculating the hash values is called mining. In a decentralized system, valid blocks are produced simultaneously by multipling nodes that find the nonce approximately at the same time. This would result in fork generation. Forks are resolved when the next block is generated. In PoW, the

longest chain is the reliable and correct one. To find the longest valid chain, a lot of computational power is wasted. Some protocols use side applications along with PoW to mitigate the loss.

2) Proof of Stake(PoS). Proof of Stake (PoS) is a protocol which states that a user or miner can mine or validate transactions in a block depending on the amount the user holds. This protocol trusts that if people have more currency involved, they are less likely to attack the network. Miners in PoS need to prove the proprietorship of the amount of money. However, this selection method is unjust based on the research from the richest person in the network, in which it explains the protocol in detail and provides examples for better understanding [29].

In this protocol the blockchain tracks a set of miners and any miner must hold the base cryptocurrency to become a validator. The miner sends a specific form of transaction that locks the cryptocurrency as deposit. The process of creating and validating a new block is then undertaken by all validated participants. The PoS algorithm has many flavors to it depending on the ways the rewards are assigned. From an algorithmic potential, the ways can be classified as chain-based PoS and Byzantine Fault Tolerance (BFT) style PoS. In chain-based PoS, the validator is selected pseudo-randomly for a time slot and is allocated the authority to create a block. The created block must have the previous block as a precursor to achieve a single continuously growing lengthening chain of blocks. In BFT-style PoS, miners are randomly permitted to suggest the creation of a new block. However, approving the block is canonical and is carried out by a multi-round voting process, where every validator votes for a precise block and finally, all validator agree upon the validity of the block to the blockchain.

3) Practical Byzantine Fault Tolerance (PBFT). Practical Byzantine Fault Tolerance (PBFT) is an imitation algorithm created to endure byzantine faults. [27] discussed the protocol in detail, showing that in order to tolerate the byzantine fault we need to understand the byzantine problem that can be described as an agreement problem where a cluster of generals, individually commanding a percentage of the Byzantine army, enfold a city. The generals want to articulate a plan to attack the city. Basically, the generals need to decide on the course of action which would be either to attack the city or to retreat. The most important thing is that all generals reach a mutual decision. If only a few generals attack the city, the attack would fail. The byzantine problem gets even more complex by the existence of disloyal generals who may cast a vote for an insignificant strategy. PBFT algorithm handles up to 1/3 malevolent byzantine replicas. Once a new block is resolute in a round, a primary is selected based on predefined rules and is responsible to order the transaction for every round. The entire process is divided into three phases: pre-prepared, prepared and commit. In all the phases, the node enters the next phase only after receiving 2/3 of the votes from all the nodes in the network. In PBFT, every node is known by other nodes in the network and can query each other. Delegated Byzantine Fault Tolerance (dBFT) is an algorithm like PBFT. Howver, in dBFT a group of professional nodes are voted to record transactions as opposed to random nodes.

In the byzantine consensus algorithm new blocks are determined in rounds. A sponsor is selected to broadcast an uncorroborated block in a round. The validation of a transaction can be done in three steps. The first is the prevote step. In this step, validators indicate the need to broadcast a block for prevoting. It is possible to

skip this step if the validators deem it unnecessary for a particular transaction and directly approve the prevoting of a block or transaction by gaining 2/3 votes from the network. The second step is the precommit step. In this step the validators decide to precommit a block or transaction. To enter this step, the node needs 2/3 votes from the first step. If the prevote step is nullified, the precommit phase goes through the tedious voting phase for broadcast and validation. Once the block receives 2/3 votes for the precommit step, it enters the commit phase, which is the last step. In this step, a node validates a block or transaction and broadcasts a commit for it. The commit phase with 2/3 votes from the block or transaction is accepted to be valid.

4) Delegated Proof of Stake (DPoS). Delegated proof of stake (DPoS) is an algorithm like the PoS protocol. DPoS targets at accomplishing a distributed consensus in a cryptocurrency system. It varies from PoS algorithm in the aspect that in DPoS, coin holders of the cryptocurrency system vote for delegates to validate and process a transaction in return for transaction fees, which is different in PoS where a stakeholder validates and processes a transaction to earn rewards and transaction fees. The difference between PoS and DPoS can be perceived as the difference between a direct democratic and the representative democratic. Stakeholders in a cryptocurrency system elect their delegated, who in turn generate and validate blocks. DPoS is the most quickest, productive, efficient, decentralized, and versatile consensus model available. DPoS ascendance the power of stakeholder approval voting to resolve consensus issues in a fair and democratic way. Deterministic selection of block producers allows transactions to be confirmed in an average of only one second. Perhaps most importantly, the consensus protocol is designed to protect all participants against unwanted regulatory interference [28].

A transaction is swiftly confirmed if fewer nodes need to be validated, but this form of block validation could lead to the tampering of the block parameters such as the size and interval by the delegates selected. DPoS process involves usage of trusted subnetworks within a larger network in which the nodes can be divided into either a server or the client. A server contribute the consensus process and each server contains a unique node list (UNL) while the client would transfer funds. In order to validate a transaction, the server queries the nodes listed in the UNL. If the agreements reach at least 80%, the transaction is validated and added to the ledger. With the nodes point of view, the ledger or transaction remains accurate and correct till the percentage of faulty nodes in the UNL remains below 20%.

5) SCP design. SCP design is a computationally-scalable byzantine consensus protocol for blockchains and this algorithm deals with a transaction or blocks in terms of epochs or periods of time. Each epoch targets and decides on a set of values. [35, 36] discusses in detail about the steps in this protocol. It is pointed out that the main idea of SCP design is to efficiently use the computational power available. This protocol divides the computational power available into sub-committees and every committee runs a consensus protocol internally to agree on a single outcome. A consensus committee is responsible to collect and combine the values decided by all the committees. It is also responsible for computing a cryptographic summary and broadcasting it to the entire network. As the number of committees increases, the total computational power of the network increases correspondingly.

In the last step in an epoch, the concluding committee creates a set of random public bit strings that are used by consequent epochs as a randomness source. The

processor executes 5 steps in each epoch. The first step is committee formation, which is a local computation at every processor. The local computation reveals the virtual and committee identity to the processor that partakes in an epoch. The second step is committee overlay join, where processors communicate to learn the identities of other processors involved in their committee. The third step is intra-committee consensus, in which processors run an authenticated protocol to agree on a value. Every committee involved sends the value to the nominated final committee. The following fourth step is final consensus broadcast, where final committee computes a final value from all the received values and broadcasts the concluding result to network. The fifth and last step is shared randomness generation, where the final committee runs a disseminated scheme to generate a adequately impartial random value.

2.5. **Types of blockchains.** Figure 3 illustrates the three forms of blockchain, including public blockchain, private blockchain, and consortium blockchain [33, 52, 57]. Figure 5 displays the corresponding pattern representations. These three forms are discussed in detail in this section.

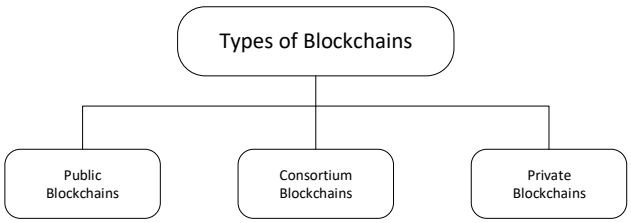

FIGURE 4. Types of Blockchains

2.5.1. *Public blockchain.* In this type of blockchain, everyone in the network can validate the transaction and can partake in the process of attaining consensus. Blockchain was initially designed to cut out the central authority in a secure way in an exchange of asset scenario. It ensures the decentralizing by setting up a block of peer-to-peer transactions. Each transaction is associated with the blockchain before it is written to the system. Thus, it can be confirmed and synced with every node in the network. Anybody with a computer and internet connection can be enrolled as a node and can be provided with the complete blockchain history. The redundancy of public blockchain makes it extremely secure. However, it very slow and inefficient. The electric power required to validate each transaction is monumental and increases dramatically with every node that gets added to the network.

On the other hand, the benefit of the public network is the anonymity of the user and full transparency of the ledger. Compared to a private blockchain, costs are excessive and speeds are unhurried. However, public blockchain is faster and less expensive than the accounting systems and methods used before the usage of blockchain. A decentralized network is the heart of the blockchain and a public blockchain is the most efficient way to decentralize a network. Since security is a key factor for the users of blockchain, the competitors of blockchain in the industry are still suggestively more expensive and sluggish than a public blockchain network notwithstanding the slowness when compared to a private blockchain.

2.5.2. *Private blockchain.* Private blockchain is the restricted type of blockchain that allows the middleman back so to say, to a certain extent. Private blockchains have a strict management with respect to the authority of the data access in the network. None of the nodes in the network can participate in the verification and validation of transactions. Instead, a company or organization initiates, verifies and validates each transaction. This provides a higher level of efficiency in the verification and validation of transactions. The only significant deficiency of private blockchains is that it does not provide decentralized security as provided by the public blockchains.

On the other hand, the benefit of private blockchain is that a company can select the access rights to individuals and permit a higher level of privacy when compared to public blockchains. A private blockchain is pertinent to a traditional and governance model based business. Using a privately-run version of blockchains can bring the organization into the 21st century. Private blockchains are more prone to acceptability by the government based or private sector companies as they allow a central authority to be present with a more secure, more efficient and faster technology.

2.5.3. *Consortium blockchain.* Consortium blockchain is a combination of public and private blockchains and can be perceived as partly decentralized. In this blockchain network, data or transaction details can either be open source or private and the node has the authority to choose in advance. It is vital to realize the distinction between a consortium blockchain and a completely private blockchain. However, the difference is not explored in depth up until now. In general, the consortium blockchain is a hybrid between the low trust of public blockchains and the single highly trustable entity model of private blockchains, whereas private blockchains can be precisely defined as traditional centralized systems with cryptographic verification and validations attached.

This type of blockchain allows a set of predetermined nodes to verify and validate transactions or blocks instead of allowing any person with an Internet connection or a single company to have full control to verify and validate transactions or blocks. A consortium blockchain provides many of the same advantages associated with private blockchains. They mainly focusing on efficiency and transactional privacy without accumulating and authorizing a single company or organization. Consortium blockchains operate under the management of a group of entities like board members or council of elders. This platform provides an exceptional advantage to organizational partnerships providing endless possibilities.

3. **Security and privacy issues in future trends and applications of blockchains.**

As illustrated by Figure 6, we discuss the security and the privacy of blockchain along with their impact with regards to different trends and applications in this section.

3.1. **Security of blockchains.**

Security in blockchain can be defined as the protection of transaction information and data in a block (whatever form of data) against internal and peripheral, malevolent and unintentional threats. Typically, this protection involves detection of threat, prevention of threat, appropriate response to threat using security policies, tools and IT services. Some important ideas and principles in security are listed below:

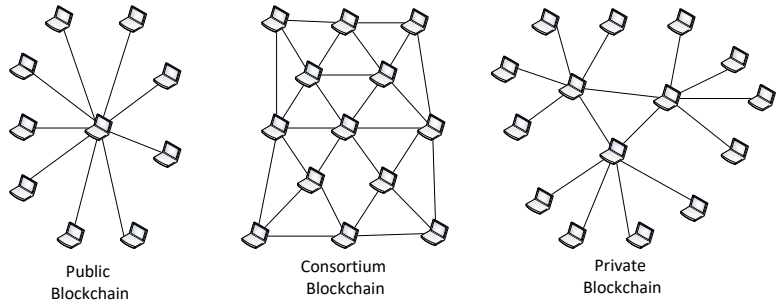

FIGURE 5. Pattern Representation of Blockchain Types

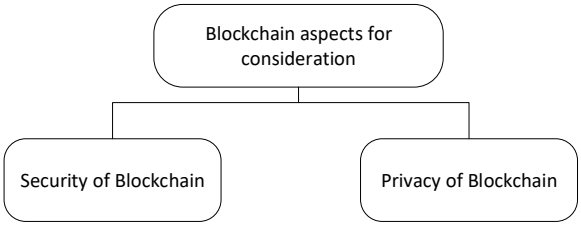

FIGURE 6. Aspects of Blockchain

a). Defense in penetration. This is a strategy which uses numerous corrective measures to protect the data. It follows the principle that protecting data in multiple layers is more efficiently as opposed to single security layer.

b). Minimum privilege. In this strategy the access to data is reduced to the lowest level possible to reinforce elevated level of security.

c). Manage vulnerabilities. In this strategy we check for vulnerabilities and manage them by identifying, authenticating, modifying and patching.

d). Manage risks. In this strategy we process the risks in an environment by identifying, assessing and controlling risks.

e). Manage patches. In this strategy we patch the flawed part like code, application, operating system, firmware etc. by acquiring, testing and installing patches.

Blockchain technology uses many techniques to achieve the security of transaction data or block data, irrespective of the usage or data in the block. Many applications such as bitcoin use the encryption technique for data safety. [45, 14] explained in detail about using a combination of public and private key to securely encrypt and decrypt data. The other most secure concept of blockchain is that the longest chain is the authentic one. This eliminates the security risks due to 51% majority attack and fork problems. As the longest chain is the ultimately authentic, the other attacks become null and void as they end up being orphaned forks. [31] discusses blockchain security enhancement achievements for blockchain systems like Smart pool, Quantitative framework, Oyente, Hawk and Town Crier. We will learn about it in the later sections of this paper.

3.2. **Privacy of blockchains.** Privacy is the capability of a single person or a group to seclude themselves or data therefore expressing themselves discerningly. Privacy in blockchain means being able to perform transactions without leaking

identification information. At the same time, privacy allows a user to remain compliant by discerningly divulging themselves without showcasing their activity to the entire network.

The goal of enhancing privacy in blockchains is to make it extremely difficult for other users to copy or use other users' crypto profile. An immeasurable volume of variations can be perceived when applying blockchain technology. Some common characteristics are particularly significant and are summarized as follows [59]:

a). Stored data sorting. Blockchain provides the flexibility to store all forms of data. The privacy perspective in blockchain varies for personal and organizational data. Although privacy rules are applicable for personal data, more stringent privacy rules apply to sensitive and organizational data.

b). Storage distribution. The nodes in the network that stores complete copies of the blockchain are called full nodes. The full nodes in combination with the append-only characteristic of blockchain leads to data redundancy. This redundancy of data supports two key features of blockchain technology including transparency and verifiability. The compatibility of application with data minimization decides the level of transparency and verifiability of that network for an application.

c). Append-only. It is impossible to alter the data of previous blocks in the blockchain undetected. The append only feature of blockchain in certain cases does not curtail to the right to correction of users, especially if data is recorded incorrectly. Special attention needs to be provided while assigning rights to data subjects in blockchain technology.

d). Private vs public blockchain. The accessibility of blockchain is remarkable from the standpoint of privacy. In an advanced level the restricted data on a block can be encrypted for conditional access by authorized users as every node in the blockchain has maintains a copy of the entire blockchain.

e). Non-permissioned vs permissioned types of blockchain. With public or non-permissioned blockchain applications, all users in principle are permitted to add data. Permitting the restoration of trusted mediators influences the distribution of control over the network.

3.3. **Security and privacy challenges and solutions for blockchain applications.** In this section we review some of the different applications using blockchain technology. We also discuss the security and privacy challenges as well as the proposed solutions. Figure 7 depicts the areas in which blockchain is mainly coming into use.

3.3.1. *Blockchain in finance.* Blockchain was initially developed as the backbone for Bitcoin, which is a popular decentralized digital currency. Blockchain off late is used in numerous digital currencies such as Altercoin, Peercoin, Ethereum [50], Karma [47], Hashcash [4], and BinaryCoin. Most of the digital currencies use the blockchain structure as the base even though they use different consensus algorithms for verification and validation of blocks. [45] discusses the bitcoin currency and blockchain in finance in detail and pointed out that the most import part of blockchain in finance sector is the use of smart contracts. Figure 8 represents a commonly financial transaction using smart contracts. In this paper, we further discuss security related and privacy related concerns while using blockchains in the finance domain.

Common security related concerns of any organization while using blockchain are ensuring authorized parties to access correct and appropriate data. Warranting the

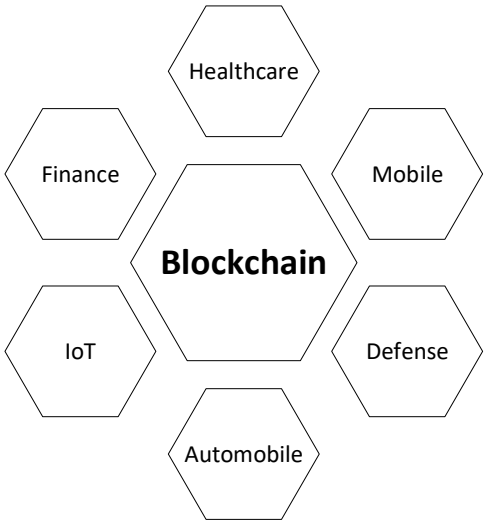

FIGURE 7. Areas of Application of the Blockchain Technology

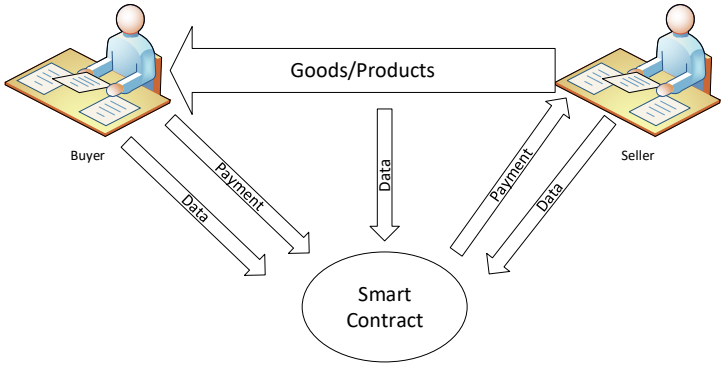

FIGURE 8. Blockchain in Financial Transactions

security of data and data access in the blockchain network is fundamental. Gaining access to the blockchain network and the data can enforce the need to implement authentication and authorization control. Blockchain allows full encryption of data blocks and efficiently assures confidentiality. Encrypting data can provide organization with levels of protection from data confidentiality and data access control in a blockchain network. Using the private and public keys in conjunction with encryption of data provides the network and the organization with a higher level of security. A very vital aspect of information systems is the maintenance of data consistency and integrity. Blockchain ensures data integrity based on its basic characteristics of immutability and traceability. The amalgamation of sequential hashing technique and cryptography makes it extremely arduous for any user or nodes in the network to tamper the data in blockchain.

The right to be forgotten ensures the privacy of user in any network, which is especially significant with regards to data immutability. The biggest challenge

is guaranteeing the implementation of this right in a technology that is based on the principle of not erasing any data. Opportunely, blockchain provides multiple solutions. One of them is to encrypt personal information in the network. In the case that we forget the keys, the data is inaccessible and can ensure the safety. Another option is to concentrate on the value of blockchain to offer irreversible facts by writing the hash of transactions to it, while the transactional data is stored outside the system. Traceability is the ability to track the time and information regarding a transaction in blockchain as every transaction is digitally signed and timestamped. This feature helps with non-repudiation of data that guarantees that data can be duplicated. Hence, it increase the reliability of blockchain.

3.3.2. *Blockchain in healthcare.* Blockchain in the healthcare domain needs to be public and would need to be scalable, secure and maintain the data privacy. The blocks in healthcare mostly contain health records, documents and images. [34] discusses the healthcare blockchain in detail and showed that the data faces storage implications and throughput limitations. If data is stored in bitcoin modeled blockchains, every user would contain a copy of health record of every individual in the network. This is not an ideal storage method and is bandwidth intensive. It creates a wastage of network resources and data throughput concerns. To implement the use of blockchains in the healthcare domain, we need to device an access control manager for data management and storage. The actual blockchain contains only an index or list of all the users data. It works like a catalog of metadata about patients and locations and the data is stored to be accessed by an authorized user. To improve data access efficiency, the data is encrypted, timestamped, and retrieved with the help of a unique identifier. All healthcare related data is stored in blockchain data repositories called data lakes. Data lakes are extremely valuable in research and analysis since they can store any form of data. Data lakes also support technologies such as interactive querying, mining and analyzing texts and machine learning. Figure 9 shows an overall view of blockchain transactions in the healthcare area.

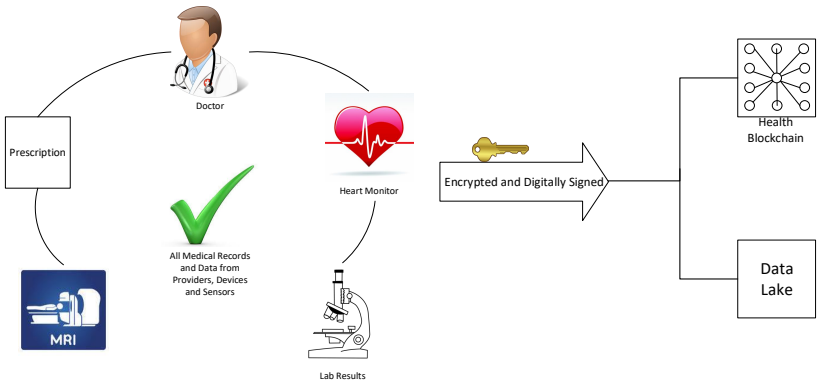

FIGURE 9. Blockchain in Healthcare Transactions

To maintain privacy, the data in data lakes is encrypted and signed digitally and can be accessed by authenticated users only. It is also digitally signed and encrypted before a new record is being placed in the data lake. Every user has complete access to his data and can controls how his/her data is shared. A pointer is maintained to

access and update each record with the help of users' unique identifier. The user can assign access rights to other users and selectively authorize users to update his/her data on the blockchain.

Blockchain technology offers numerous advantages for the healthcare domain, as it contains components like open source, commodity hardware and open APIs. These components help fast and easy interoperability between systems and can be scalable to larger volumes of data and users. Blockchain allows users to access shared data source to attain timely, precise and comprehensive healthcare data. Moreover, the commodity hardware of the blockchain provides low cost computation and it addressed the interoperability challenges within healthcare domain. Another advantage of blockchains distributed architecture is its built-in fault tolerance and disaster recovery feature. As data is spread across many servers, a single point of failure does not exist.

3.3.3. *Blockchain in IoT.* IoT is defined as a system of interconnected computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction [8, 9]. Most common usa,ge of blockchain is in data storing and access in IoT. The user must be able to access data remotely from any location in a secure way and ensure the privacy of data stored in the network. While creating his/her account, the user sets up permissions and required controls for his/her account. After checking permissions and extracting previous block number and hash value, the user generates a random unique id and sends data to storage by using this id. The validity of transaction is verified and the storage availability is confirmed. The service provider for an application may need to access data stored for a certain period or epoch of time. Users like service providers create a multisig transactions that are signed by the service provider and the service requester. The transsactions are sent to the cluster head of that network. Then the cluster head verifies the request as a transaction by either broadcasting it to his own cluster or other cluster heads. To ensure privacy, the user uses methods such as safe answer, noise introduction to protect data, The output of a multisig transactions can either be set to 1 or 0 to indicate if the user has access to data or not respectively. These multisig transactions can be treated as proof that date was sent by the user and can be used to inform other users of misconduct if any. Figure 10 states the major advantages of using blockchain in IoT.

FIGURE 10. Blockchain in Internet of Things

As abundance of devices are added to IoT every day, organizations are identifying the potential of IoT and blockchain to improve business processes and accelerate

growth. The urgent need of secure IoT model in performing even common tasks sensing, processing, storing data and communicating is increasing as well. The public blockchain provides a great advantage to these problems as everyone is participating and the information is protected by a private key. With no single central authority controlling it, the model based on blockchain involves a great deal of trust. The biggest challenge of implementing blockchain in IoT is the scalability, since the response time to requests increases as the number of computing devices increases.

3.3.4. *Blockchain in mobile applications.* A mobile application can be described as a software application that has been specifically developed for mobile devices like smartphones and tablets. Blockchain supports peer-to-peer data service in mobile applications, as discussed in [14] and [41] about peer-to-peer file transfer and direct payment. [51] further states that the first miner successfully solving the puzzle to validate a transaction using any of the consensus techniques a reward is specified. This is called speed game amid miners and the puzzle cannot be handled using mobile devices. To achieve mobile blockchain processing we can use the edge computing concept. We consider a group of N mobile application users represented as $N = 1, 2, ..., N$. Each user or node is trying to solve the puzzle using hashing power and computing power for a reward associated with the solution. Mobile users run mobile blockchain application with the help of edge computing nodes for miners deployed with edge computing service providers. This service provides computing resources to mobile users which is priced by the service provider. Figure 11 illustrates the usage of blockchain in mobile applications.

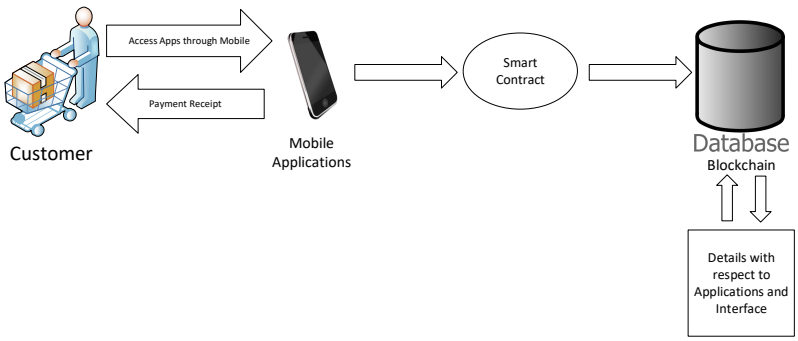

FIGURE 11. Blockchain in Mobile Applications

Blockchain can add an immense value to the security strategies regarding mobile applications. It is more secure to use in different applications that specially focusing on sensitive data, since blockchain does not have any single point of failure. Blockchain is ideal to use when there is a stringent requirement for authentication to protect data. The major use of mobile based applications arose in accessing the digital wallets. Most of the mobile application allow user to pay using digital wallets, or in cases like bitcoin it allows users to make transactions online through mobile devices using the edge computing services provided in the network. Therefore, using mobile applications makes the application portable and more acceptable.

3.3.5. *Blockchain in defense.* To overcome highly congested environments in the future, the defense must depend on cyber-enabled systems and the data they contain.

The current cyber defense seems to be faltering and incremental enhancements fall short to the growing cyber threat. Blockchain technology overturns the cyber security paradigm due to its trustless, transparent and fault tolerant thereby reducing the probability of data compromise. [5] discusses in detail about the application of blockchain technology in national defense. The core elements in the working of blockchain, like secure hashing, backlinked data structure and consensus mechanism, play a significant role as attributing the security factor of blockchains. Given that any permissioned user in the network can access the data on the network, a major issue for blockchain security is confidentiality of data. This can be overcomes by encrypting data and maintaining an access control by storing it in blockchains.

Blockchain can be used in defense application by acting the operational or support roles as follows:

a). Cyber defense. This is a low-cost, high payoff application of blockchain. Firstly, blockchain ensures that all digital events are widely perceived by transmitting them to all other nodes in the network and thereafter uses different consensus algorithms to validate and verify. Once the secured the data is timestamped and stored, it cannot be manipulated. In case that the data is altered or updated, it is again timestamped and the log is maintained. The modern weapon and component details can be imaged, hashed and secured in the database and continuously monitored using blockchains. This is discussed in detail in [44].

b). Supply chain management. The growing concern regarding supply chain management in defense leads to the need of a technology to establish the origin and owner traceability. Blockchain provides a solution to these issues as discussed in [26].

c). Resilient Communications. In the highly contested environments, blockchain provides resilient communication because of its capability to securely generate, protect and share data in an impervious manner. The resilience offered by blockchain is discussed in [32]. All these characteristics ensure the reliability of verified data transmission across the world, notwithstanding malicious attacks against paths of communication, nodes or the blockchain itself.

3.3.6. *Blockchain in automobile industry.* Modern vehicles are increasingly connecting to online or network based applications and hence provide an excellent base for the use of blockchain technology. As mentioned in [10, 40, 21], automotive security architectures need to address a few requirements to placate the future needs for smart vehicles. Automotive security architectures need to address the challenges to satisfy the needs of future services of smart vehicles from the perspectives listed as follows:

a) Scalability. The architecture is essential, since the vehicular ecosystem entails numerous vehicles and each tailors with abundant electronic control units.

b) Safety. A secure architecture of a smart vehicle should protect the user against threats involving security breaches occurring due to malfunction as well as due to numerous autonomous driving functions.

c) Centralization. A centralized architecture leads to single point of failure hence compromising the security of the system. Therefore, decentralized architecture is more preferred due to the low scale ability of the centralized architecture.

d) Maintainability. The automotive architecture must address software and hardware maintainability for a fixed period and the extend-ability option for maintainability of a vehicle.

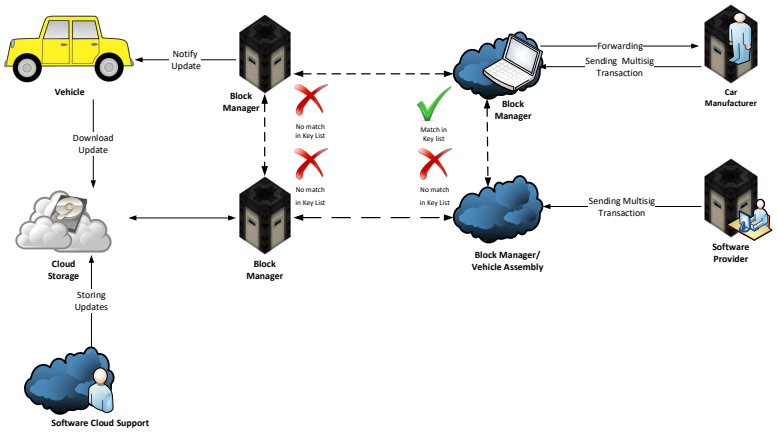

FIGURE 12. Blockchain in Automobile Applications

Wireless Remote Software Updates (WRSU) is one of the most challenging and critical security issue in the automotive industry. WRSU needs to upgrade of fixing errors in the functionality of electronic control units whenever a installation of software upgrade needs to be performed. In doing so, WRSU supports the complete lifecycle of a vehicle as it can come into the vehicle lifecycle as early as vehicle's development and assembly till its maintenance and more. Today, the main effort is made into efficiency and security of the WRSU architecture for a better management of vehicular data. Figure 12 depicts the entire software update process based on the WRSU architecture. The software provider generates a latest version or an upgrade of software, and then stores it in the cloud that is available to all the overlay nodes. Then he/she creates a multisig transaction and encrypts it with his/her private key and digital signature. The public key of the car manufacturer and block managers is used to forward the transactions with a list of keys, thereby providing data integrity. The transaction is then sent to overlay since the current transaction containing a single key cannot be treated as valid by all block managers. The block managers only broadcast the transaction to the network. Once the transaction is received by the block manager of the cluster containing the concerned car manufacturer, he/she verifies the software version and sends an acknowledgment to the block manager. The transaction is broadcast to all the block managers and verified with the public key of software provider and the car manufacturer. The smart vehicle receives the transaction from the block manager and verifies it. The vehicle then downloads the software directly from the cloud storage using its authentication parameters.

Furthermore, as discussed in [10], the blockchain structure can be used in multiple ways in the automotive industry such as insurance, electric and smart charging services, car leasing and sharing services.

4. **Challenges and opportunities.** The blockchain technology faces a few future opportunities as well as challenges. Although significant, the challenges can be overcome with the maturity and enhancement of the technology in the future. This will lead to a plethora of future opportunities for blockchain to be implemented and accepted. The challenges and opportunities would be discussed in detail in this section.

4.1. **Challenges.** A challenge can be defined as an implicit demand for proof. Some of the major challenges currently faced by blockchain technology are listed below.

4.1.1. *Scalability.* With ever increasing volume of blockchain usage and the surge in the sheer number of transactions daily, the blockchain is becoming progressively colossal in size. All transactions are stored in each node to get validated. The source of current transaction needs to be validated first before the transaction to be validated. The restricted block size and the time interlude used to produce a new block also plays a part in not fulfilling the requirement of processing millions of transactions simultaneously in real time scenarios. In the meantime, the size of the blocks in blockchain might create an issue of transaction delay in case of small transactions, as miners would prefer to validate transactions with bigger transactional fees. As mentioned in [58], the proposed solutions to the scalability issue of blockchains can be categorized in two categories: storage optimization and redesigning of blockchains. This database would maintain rest of the non-empty addresses. A light weight client could also be used as an alternate to fix the scalability issue. In redesigning, the blockchain can be fragmented into a key block and a micro block, with the key block being responsible for leader elections while the micro block being responsible for transaction storage.

4.1.2. *Privacy leakage.* The blockchain is mainly vulnerable to leakage of transactional privacy due to the fact that the details and balances of all public keys are visible to everyone in the network. The proposed solutions to achieve anonymity in blockchains can be broadly classified into mixing solution and anonymous solution. Mixing is a service that offers anonymity by transferring funds from multiple input addresses to multiple output addresses. Anonymous is a service which unlinks the payment origins for a transaction to prevent transaction graph analysis as discussed in [58].

4.1.3. *Selfish mining.* Selfish mining is another challenge faced by blockchains. A block is susceptible to cheating if a small portion of hashing power is used. In selfish mining, the miners keep the mined blocks without broadcasting to the network and create a private branch which gets broadcast only after certain requirements are met. In this case, honest miners waste a lot of time and resources while the private chain is mined by selfish miners.

4.1.4. *Personal identifiable information.* Personal Identifiable Information (PII) is any information that can be used to extricate an individual's identity. [12] discusses the PII with respect to communication and location privacy.

4.1.5. *Security.* Security can be discussed in terms of confidentiality, integrity and availability as discussed in [37]. It is always a challenge in open networks such as public blockchains. Confidentiality is low in distributed systems that imitate information over its network. Integrity is the metier of blockchains although there exist many challenges. Availability in blockchains is high in terms of readability due to wide replication compared to write availability. The 51% majority attack is more theoretical in a large blockchain network because of these properties.

4.2. **Opportunities.** Opportunities can be stated as a chance to integrate blockchain technology in existing applications to improve efficiency and usage use as well as to promote this technology in future applications. Some of the future opportunities are listed in more details as follows.

4.2.1. *Strategic alignment and governance.* Active management of connections between enterprise progressions and administrative priorities that aims to facilitate operative actions for business performance improvement can be referred to as strategic alignment. The analysis includes the evaluation of different processes on how they can be improved with the usage of blockchain technology. The risks of these strategies analogous to the lock-in effects might also need to be analyzed.

Governance is more in relation to suitable and transparent accountability in terms of tasks, parts and decision processes for different projects and operations. Blockchain technology fluctuates governance towards a more outwardly oriented coopetition as a new management mode for processes. As discussed in [37], implications of the governance have four perspectives. Firstly, dedicated roles that coordinates both internal and external cohorts for setting up blockchain support need to be defined. This requires both technical and jurisprudential facts. Secondly, policies need to be defined for the usage and the related process of blockchain. Thirdly, a set of guidelines need to be defined for the usage of public, private and consortium blockchains. This would help us foresee the attack scenarios and be better prepared for them. Finally, smart contracts can be used to launch new models of governance epitomized by DAO.

The governance of blockchain technology proposes that most enterprise applications need to operate on dedicated and private blockchains. The governance factor ensures that the applications are not single-owner applications but shared by a group of competitors. For instance, banks need to work together to devise innovative payment systems to develop trade finance solutions that will abjure the public blockchains to achieve the required throughput and confidentiality. On the other hand, private blockchains need to come to an agreement upon governance rules to operate under. In the future, international standards need to be set to achieve consensus on an enormous number of standards such as memberships, access controls, data classification and storage, measurement to verify and validate transactions, blockchain ownerships, management and maintenance etc. Blockchain technology will ensure adequate benefit to overcome both technological and governance hurdles and attain widespread usage in the future.

4.2.2. *Information technology.* Information technology incorporates all the systems supporting process execution. Blockchain technology enables and provides abundance of opportunities for process execution, although multiple challenges exist and still need to be dealt with. Firstly, implementing processes with blockchains requires new software components and the integration of development environments. Secondly, the blockchain-based process execution provides rise to new challenges in terms of security and privacy such as how to prevent confidential business data leakage. While the visibility of encrypted data on a blockchain is restricted, it is up to the participants in the process to ensure that these mechanisms are used according to their confidentiality requirements. Some of these requirements are currently investigated in the financial industry4. Further challenges can be expected with the

enactment of the General Data Protection Regulation5. Finally, inherent limitations of blockchains must be considered including computational power, data storage, throughput, and processing costs. Rather than using an existing blockchain, an alternative such as private blockchains could be adopt to reduce costs.

The potential of blockchain technology is enormous. With acquisition of time and maturity the technology, blockchain will be able to support transaction capacities necessary to support most innovativeness and huge scale applications along with the supporting the establishment of governance rules in the imminent decades. The enterprise blockchains currently in use are relatively small scale. Single user applications include those that use blockchain technology to track the ownership of an expensive or precious item. Every ledger owns and manages its blockchain, which is ideal for non-high frequent transactions. Though blockchain processing speed does not have a hard limit, the biggest challenge to future applications is the high throughout and confidentiality bundled together as a requirement. Achieving these two aspects together will result in the higher acceptance and usage of blockchain technology in the future. The applications in the innovative phase technology solutions are the future of evolving markets such as data science, machine learning, IoT etc. One of the most exciting features of blockchains is the option of micro-payments along with smart contracts. This combination creates an interesting solution to stream financial payments which is contradictory to the traditional bi-weekly or monthly pay. With simple smart contracts, any employee or professional can be paid in real time while they are on the job. They can track the progress of their work by setting miniature keystrokes to measure productivity and effectiveness of work quality and make real time payments. This type of real time payment was almost possible by using blockchain but with larger amounts network clogging hindered with micro payments options. The micro payments are advantageous to the business as well as to the employees, since this method ensures that better employees be paid more and incentives will be aligned in a better way. Moreover, the micro payments help the remote employees in real time and keep account of their work, the impact of this blockchain usage is profound.

Digital advertising expressions face contests related to domain frauds, bot traffic, lack of transparency and payment models. The major issue is the alignment of incentives leading to disheartening to advertising and publishers. Blockchain is the solution to bring the required transparency to the supply chain and can bring trust to trustless environments. It enables the companies to thrive by reducing the number of bad players in the supply chain. Though blockchain is in its infancy, the underlying technology is here to stay and can be a very big factor in improving business. The most imperative feature of blockchain is to provide incomparable security in an insecure internet where phishing, malware, DDOS, spam and hacks in the global business. A significant advantage of blockchain over other software ledgers is that it is based on cryptography and is immutably programmed, making it impossible for anyone to go back a step and change information on blockchains. The distributed aspect of blockchains also provides a crucial benefit, making it enormously problematic to bring down in case of controlling government or illegitimate business practices. Finally, blockchain is a prodigious tool to use when enormous amount of important documentations need to be stored like healthcare, copyrights, logistics etc. The smart contracts in blockchain remove the need or middlemen to legalize contracts in user friendly ways.

Blockchain is viewed upon as a digital ledger system by many people. However, the encrypted database structure of blockchains is revolutionary and holds true potential. Internet allows us to stretch our ability to push boundaries and has moved at a faste speed with respect to protect against spyware, viruses and hackers. Blockchain has the potential to essentially mark a extensive assortment of processes and technologies. Blockchains address these concerns with a ledger comprising verifiable and validated history of transactions. It minimizes the need for organization to provide risk mitigation and trusted services, thus resulting in mortgage closure for a fraction of cost and time with considerably higher degrees of trust.

4.2.3. *Other industry prospects.* Blockchain can provide access to banking and payment sector by providing financial services to billions of users around the world, including third world countries without having access to traditional banking. Blockchains are used by many banking institutions to make their business operations faster, more efficient and more secure. There is an increasing investments to blockchains in the banking and payments startups and projects. Cybersecurity is another interesting and leading sector for blockchains. Although the blockchain ledger is public, the data is verified and encrypted using advanced cryptography, making it less prone to hacking and modifications without authorization. Supply Chain Management is another area of blockchain technology implementation. Transactions can be documented in a permanent decentralized record and monitored in a secure and transparent manner. This reduces time delays and human errors significantly. The blockchain technology can also be used to monitor costs, labor, waste and emissions at every point, since supply chains have stern implications to understand and control environmental impact of products by verifying authenticity. Furthermore, blockchain can be used to forecast the changes on the entire approach to research, consulting and analysis.

IoT uses blockchain as a new concept to create a decentralized network of IoT devices that operates like public ledgers for substantial number of devices. This could eliminate the need for a central location to handle communication like updating softwares, manage bugs and monitor energy usage. Trust management is the root of global insurance market to integrate real world data with smart contracts. Private transport and ride sharing use blockchains to create decentralized versions of peer-to-peer sharing applications, thus allowing car owners and users to arrange terms and conditions in a secure way without the third parties. The electronic wallets allow car owners to pay for parking, tolls, and top ups automatically for their vehicles. Traditionally centralized servers can be extremely vulnerable to be hacked. Instead, blockchains store data in cloud storage in a decentralized manner, which makes it more secure and robust. Inefficiency and corruption are the most common criticisms in charity spaces preventing money from reaching the intended people. Blockchain technology can be used to track donations in a secure, transparent and verifiable way to make sure that the donated money reaches the intended party. Blockchain can also be used for voting by registering voters and verificating identity, since vote counting in a traditionally centralized servers can be extremely vulnerable to hacking, data loss or human errors. Voting is a significant area that can be disrupted by blockchains, since blockchain could create an immutable and publicly viewable ledger of recorded votes and provide the much need transparency in the voting system of the world. Government systems are habitually deliberateimpervious and predisposed to corruption. Implementing a blockchain based system

can suggestively improve security, efficiency and transparency of government operations.

The public welfares system is an alternative subdivision that suffers from deliberateness and bureaucracy. Another industry depending on legacy systems and suitable for interruption is healthcare. In hospitals, there are often victims of hacking of data because of obsolete infrastructures. The major contest hospitals face is the absence of a protected podium to store and share data. Blockchain technology permits hospitals to store data like medical records securely and share it with approved authorities or patients, which can improve data security and assist with accurateness and swiftness of diagnosis.

Energy management is a highly centralized industry. Energy manufacturers and consumers cannot buy it from each other directly and need to involve a trusted private intermediary. Blockchain technology can provide a better and more efficient solution to this problem. Online music is another sector where blockchain can be implemented. Numerous companies are developing ways for musicians to get paid unswervingly from their fans, instead of sharing large percentages of sales with platforms or record companies. Smart contracts automatically solve licensing issues and catalog songs with their respective creators in a better and efficient manner. One of the other sectors is retail, in which we need to trust the retail system which in turn bonds us to the store or marketplace. Blockchain based retail utilities work contrarily by connecting buyers and sellers and excluding middleman as well as the fees associated with them. In such cases, trust comes from smart contract systems, the security of interaction, and built in reputation administration systems.

Real estate faces issues with transparency, fraud and slipups in public records. With respect to buying and selling real estate, blockchain technology can speed up the real estate sector by reducing the need for paper-based records and can assist with tracking, verifying, ownership, accuracy of documents and transferring property deeds. Crowdfunding has developed a prevalent method of fundraising for innovative startups and projects in recent years. However, the crowdfunding platforms charge high fees. In blockchain based crowdfunding, trust is created over smart contracts and online reputation systems. This could remove the need for a middleman and reduce the cost. Projects advance funds by emancipating their own tokens that characterize value and can be exchanged for products, services, or cash whenever needed. Any industry dealing with data or transactions of any kind can be disrupted by blockchain technology. The space is undeveloped and there exist many opportunities.

5. **Conclusion.** Blockchain technology is exceedingly recognized and appraised due to its decentralized infrastructure and peer-to-peer nature. These characteristics have the potential to support a plethora of requirements in different areas and applications. In this paper, we propose a comprehensive survey by initially discussing the structure of blockchains and its major components and characteristics. Then we endeavor to highlight the security and privacy issues faced by the blockchain technology in the different areas of its usage. Finally, the future applications, opportunities, and challenges of blockchain technology are summarized.

With the rapidity of its growth and development, we believe that blockchains will soon become a very common and well-known phenomenon. Blockchain can be compared to the Internet a few decades ago in certain extent. Since the core of blockchains is secure and supportive, gradually many major applications that require security and non-repudiation will move on this technology. Although there

still exist some limitations in blockchains and many innovative applications are difficult to be implemented, blockchain is likely to become the technology that everybody would move towards with its maturity. We plan to take an in-depth investigation on blockchains in the future.

REFERENCES

[1] Data aggregation scheduling in probabilistic wireless networks with cognitive radio capability, in *2016 IEEE Global Communications Conference (GLOBECOM)*, 2016, 1–6.

[2] Security implications of blockchain cloud with analysis of block withholding attack., *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, 458.

[3] C. Ai, M. Han, J. Wang and M. Yan, An efficient social event invitation framework based on historical data of smart devices, in *2016 IEEE International Conferences on Social Computing and Networking (SocialCom)*, IEEE, 2016, 229–236.

[4] A. Back et al., Hashcash-a denial of service counter-measure.

[5] N. Barnas, Blockchains in national defense: Trustworthy systems in a trustless world, Blue Horizons Fellowship, Air University, Maxwell Air Force Base, Alabama.

[6] Z. Cai, Z. He, X. Guan and Y. Li, Collective data-sanitization for preventing sensitive information inference attacks in social networks, *IEEE Transactions on Dependable and Secure Computing*, (2016), 1–1.

[7] N. Capurso, T. Song, W. Cheng, J. Yu and X. Cheng, An android-based mechanism for energy efficient localization depending on indoor/outdoor context, *IEEE Internet of Things Journal*, **4** (2017), 299–307.

[8] F. Chen, P. Deng, J. Wan, D. Zhang, A. V. Vasilakos and X. Rong, Data mining for the internet of things: Literature review and challenges, *International Journal of Distributed Sensor Networks*, **11** (2015), 431047.

[9] A. Dorri, S. S. Kanhere and R. Jurdak, Blockchain in internet of things: challenges and solutions, arXiv preprint, `arXiv:1608.05187`.

[10] A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak, Blockchain: A distributed solution to automotive security and privacy, *IEEE Communications Magazine*, **55** (2017), 119–125.

[11] Z. Duan, M. Yan, Z. Cai, X. Wang, M. Han and Y. Li, Truthful incentive mechanisms for social cost minimization in mobile crowdsourcing systems, *Sensors*, **16** (2016), p481.

[12] A. S. Elmaghraby and M. M. Losavio, Cyber security challenges in smart cities: Safety, security and privacy, *Journal of Advanced Research*, **5** (2014), 491–497.

[13] J. A. Garay, A. Kiayias and N. Leonardos, The bitcoin backbone protocol: Analysis and applications., in *EUROCRYPT (2)*, **9057** (2015), 281–310.

[14] F. Gierschner, Bitcoin and beyond.

[15] M. Han, Z. Duan and Y. Li, Privacy issues for transportation cyber physical systems, in *Secure and Trustworthy Transportation Cyber-Physical Systems*, Springer, Singapore, 2017, 67–86.

[16] M. Han, J. Li, Z. Cai and Q. Han, Privacy reserved influence maximization in gps-enabled cyber-physical and online social networks, in *2016 IEEE International Conferences on Social Computing and Networking (SocialCom)*, IEEE, 2016, 284–292.

[17] M. Han, M. Yan, J. Li, S. Ji and Y. Li, Generating uncertain networks based on historical network snapshots, in *International Computing and Combinatorics Conference*, Springer, Berlin, Heidelberg, 2013, 747–758.

[18] M. Han, M. Yan, J. Li, S. Ji and Y. Li, Neighborhood-based uncertainty generation in social networks, *Journal of Combinatorial Optimization*, **28** (2014), 561–576.

[19] Z. He, Z. Cai and J. Yu, Latent-data privacy preserving with customized data utility for social network data, *IEEE Transactions on Vehicular Technology*, **67** (2018), 665–673.

[20] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun and Y. Li, Cost-efficient strategies for restraining rumor spreading in mobile social networks, *IEEE Transactions on Vehicular Technology*, **66** (2017), 2789–2800.

[21] H. Heinecke, K.-P. Schnelle, H. Fennel, J. Bortolazzi, L. Lundh, J. Leflour, J.-L. Maté, K. Nishikawa and T. Scharnhorst, *Automotive Open System Architecture-An Industry-Wide Initiative to Manage the Complexity of Emerging Automotive E/E-Architectures*, Technical report, SAE Technical Paper, 2004.

[22] S. Ji, Z. Cai, M. Han and R. Beyah, Whitespace measurement and virtual backbone construction for cognitive radio networks: From the social perspective, in *Sensing, Communication, and Networking (SECON), 2015 12th Annual IEEE International Conference on*, IEEE, 2015, 435–443.
[23] P. Jin Ho and P. Jong Hyuk, Blockchain security in cloud computing: Use cases, challenges, and solutions., *Symmetry (20738994)*, **9** (2017), 1–13.
[24] A. Kiayias and G. Panagiotakos, Speed-security tradeoffs in blockchain protocols, *IACR Cryptology ePrint Archive*, **2015** (2015), 1019.
[25] V. King and J. Saia, Scalable byzantine computation, *ACM SIGACT News*, **41** (2010), 89–104.
[26] K. Korpela, J. Hallikas and T. Dahlberg, Digital supply chain transformation toward blockchain integration, in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017, 10pp.
[27] R. Kotla, L. Alvisi, M. Dahlin, A. Clement and E. Wong, Zyzzyva: Speculative byzantine fault tolerance, in *ACM SIGOPS Operating Systems Review*, ACM, **41** (2007), 45–58.
[28] D. Larimer, Delegated proof-of-stake white paper, 2014.
[29] D. Larimer, Transactions as proof-of-stake, 2013.
[30] J. Li, Z. Cai, J. Wang, M. Han and Y. Li, Truthful incentive mechanisms for geographical position conflicting mobile crowdsensing systems, *IEEE Transactions on Computational Social Systems*, (2018), 1–11.
[31] X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen, A survey on the security of blockchain systems, *Future Generation Computer Systems*, (2017), URL `http://www.sciencedirect.com/science/article/pii/S0167739X17318332`.
[32] X. Liang, J. Zhao, S. Shetty and D. Li, Towards data assurance and resilience in iot using blockchain, in *Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE*, IEEE, 2017, 261–266.
[33] I.-C. Lin and T.-C. Liao, A survey of blockchain security issues and challenges., *IJ Network Security*, **19** (2017), 653–659.
[34] L. A. Linn and M. B. Koo, Blockchain for health data and its potential use in health it and health care related research, in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, 2016.
[35] L. Luu, V. Narayanan, K. Baweja, C. Zheng, S. Gilbert and P. Saxena, Scp: A computationally-scalable byzantine consensus protocol for blockchains., *IACR Cryptology ePrint Archive*, **2015** (2015), 1168.
[36] D. Mazieres, The stellar consensus protocol: A federated model for internet-level consensus, *Stellar Development Foundation*.
[37] J. Mendling, I. Weber, W. V. D. Aalst, J. V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C. D. Ciccio, M. Dumas, S. Dustdar et al., Blockchains for business process management-challenges and opportunities, *ACM Transactions on Management Information Systems (TMIS)*, **9** (2018), Article No. 4.
[38] M. Moser, Anonymity of bitcoin transactions.
[39] M. Pilkington, Blockchain technology: Principles and applications, *Browser Download This Paper*.
[40] M. Steger, C. Boano, M. Karner, J. Hillebrand, W. Rom and K. Römer, Secup: Secure and efficient wireless software updates for vehicles, in *Digital System Design (DSD), 2016 Euromicro Conference on*, IEEE, 2016, 628–636.
[41] K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang and Z. Han, Performance analysis and application of mobile blockchain, arXiv preprint, `arXiv:1712.03659`.
[42] T. Swanson, Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems, *Report, available online, Apr*.
[43] D. Tapscott and A. Tapscott, Blockchain.
[44] W. Tirenin and D. Faatz, A concept for strategic cyber defense, in *Military Communications Conference Proceedings, 1999. MILCOM 1999. IEEE*, vol. 1, IEEE, 1999, 458–463.
[45] F. Tschorsch and B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, *IEEE Communications Surveys & Tutorials*, **18** (2016), 2084–2123.
[46] D. Verma, N. Desai, A. Preece and I. J. Taylor, A blockchain based architecture for asset management in coalition operations, SPIE, 2017.

[47] V. Vishumurthy, S. Chandrakumar and E. G. Sirer, Karma: A secure economic framework for peer-to-peer resource sharing, in *Proceedings of the 2003 Workshop on Economics of Peer-to-Peer Systems, Berkeley CA*, 2003.
[48] M. Vukolić, The quest for scalable blockchain fabric: Proof-of-work vs. bft replication, in *International Workshop on Open Problems in Network Security*, Springer, 2015, 112–125.
[49] Y. Wang, Z. Cai, X. Tong, Y. Gao and G. Yin, Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems, *Computer Networks*, **135** (2018), 32–43.
[50] G. Wood, Ethereum: A secure decentralised generalised transaction ledger, *Ethereum Project Yellow Paper*, **151** (2014), 1–32.
[51] Z. Xiong, S. Feng, D. Niyato, P. Wang and Z. Han, Edge computing resource management and pricing for mobile blockchain, arXiv preprint, arXiv:1710.01567.
[52] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso and P. Rimba, A taxonomy of blockchain-based systems for architecture design, in *Software Architecture (ICSA), 2017 IEEE International Conference on*, IEEE, 2017, 243–252.
[53] L. Zhang, Z. Cai and X. Wang, Fakemask: a novel privacy preserving approach for smartphones, *IEEE Transactions on Network and Service Management*, **13** (2016), 335–348.
[54] X. Zheng, Z. Cai, J. Li and H. Gao, Location-privacy-aware review publication mechanism for local business service systems, in *INFOCOM 2017-IEEE Conference on Computer Communications, IEEE*, IEEE, 2017, 1–9.
[55] X. Zheng, Z. Cai and Y. Li, Data linkage in smart iot systems: A consideration from privacy perspective., *IEEE Communications Magazine*.
[56] X. Zheng, G. Luo and Z. Cai, A fair mechanism for private data publication in online social networks, *IEEE Transactions on Network Science and Engineering*.
[57] Z. Zheng, S. Xie, H.-N. Dai and H. Wang, Blockchain challenges and opportunities: A survey, *Work Pap*.
[58] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in *Big Data (BigData Congress), 2017 IEEE International Congress on*, IEEE, 2017, 557–564.
[59] G. Zyskind, O. Nathan et al., Decentralizing privacy: Using blockchain to protect personal data, in *Security and Privacy Workshops (SPW), 2015 IEEE*, IEEE, 2015, 180–184.

Received December 2017; revised February 2018.

E-mail address: ainamdar@students.kennesaw.edu
E-mail address: menghan@kennesaw.edu
E-mail address: ywang63@students.kennesaw.edu