A Survey: Reliability Solutions using Block Chains

Dr. C K Raju[#1], Ms. Jyothi B[#2]

[#1]Associate Professor, [#2] P G Student & Department of CSE & SSIT
Tumkuru, Karnataka, India

Abstract *— This paper surveys blockchain-based approaches for several security services. These services include authentication, confidentiality, privacy and access control list, data and resource provenance, and integrity assurance. All these services are critical for the current distributed applications, especially due to the large amount of data being processed over the networks and the use of cloud computing. Authentication ensures that the user is who he/she claims to be. Confidentiality guarantees that data cannot be read by unauthorized users. Privacy provides the users the ability to control who can access their data. Provenance allows an efficient tracking of the data and resources along with their ownership and utilization over the network. Integrity helps in verifying that the data has not been modified or altered. These services are currently managed by centralized controllers, for example, a certificate authority. Therefore, the services are prone to attacks on the centralized controller. On the other hand, blockchain is a secured and distributed ledger that can help resolve many of the problems with centralization. The objectives of this paper are to give insights on the use of security services for current applications, to highlight the state of the art techniques that are currently used to provide these services, to describe their challenges, and to discuss how the blockchain technology can resolve these challenges. Further, several blockchain-based approaches providing such security services are compared thoroughly. Challenges associated with using blockchain-based security services are also discussed to spur further research in this area.*

Keywords *— cloud computing, cloud storage, cryptographic storage architecture***.**

I. INTRODUCTION

A blockchain is a secured, shared and distributed ledger that facilitates the process of recording and tracking resources without the need of a centralized trusted authority. It allows two parties to communicate and exchange resources in a peer-to-peer network where distributed decisions are made by the majority rather than by a single centralized authority. It is provably secure against attackers who try to control the system by compromising the centralized controller. Resources can be tangible (e.g., money, houses, cars, lands) or intangible (e.g., copyrights, digital documents, and intellectual property rights). In general, anything that has a value can be tracked on a blockchain network to reduce its security risks and save the cost of security monitoring for all involved [1].

Recently, the blockchain technology has attracted tremendous interest from both academia and industry. The technology started with Bitcoin, a cryptocurrency that has reached a capitalization of 180 billion dollars as of January 2018 [2], [3]. According to the Gartner report in 2016, the blockchain technology is receiving billions of dollars in research and enterprise investments and much more is expected to come in the near future [5]. The technology currently spans several applications that are popular and driving the networking research. Such applications include healthcare [6], Internet of Things (IoT) [7], [8], and cloud storage [9].

Among the blockchains' promising applications are network monitoring and security services including authentication, confidentiality, privacy, integrity, and provenance. Currently, these services are provided by trusted third-party brokers or using inefficient distributed approaches. Fig. 1 illustrates the differences between the traditional and the blockchain-based access control. The same concept can be applied to the other security guarantees.

This survey focuses on the use of the blockchain technology to provide network security services and applications. We present the use of these services in the current applications, discuss the conventional techniques that provide these security services, and illustrate their challenges and problems. Then, we present how the blockchain technology can be used to resolve the associated challenges and highlight several proposed blockchain-based approaches that provide the desired security services. Finally, we discuss the current challenges faced with blockchain and some of the potential future research directions in this field.

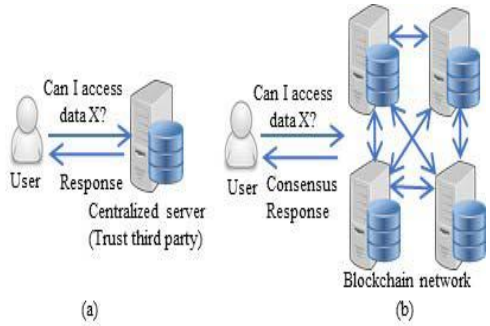

Fig. 1. (a) Traditional centralized access control guarantees (b) Blockchain based access control guarantees.

It should be noted that the details of the blockchain technology and how it is used in other domains are out of the scope of this paper. We refer the readers to [1] and [2] for more details on the blockchain technology.

II. RELATED WORK

With the current growing interest in the blockchain technology, many new platforms and applications have been proposed. Several survey papers have been written to highlight the benefits of this technology for the current applications. Examples of such surveys include the blockchain technology for IoT [8], healthcare [6] and decentralized digital currencies [12]. Other surveys have discussed blockchain challenges, opportunities, and future visions. For example, Lin and Liao [13] discuss the blockchain security issues and challenges. The work in [14] presents a thorough survey on blockchain security and privacy issues including possible attacks and countermeasures. Moreover, a recent special issue of IEEE spectrum is dedicated to blockchains and their potential uses [15]. This paper investigates the use of the blockchain technology in a different set of applications with rising interests that have not been discussed in the prior surveys. We aim to provide a comprehensive survey on the use of the blockchain technology in security services. The services can be offered by an enterprise and verified globally, offered by an enterprise but not verified, or presented as a research work. We strive these services to give insights on the current state-of-the-art technology and its challenges and discuss how the blockchain technology can be used to resolve these challenges.

III. SECURITY SERVICES AND MECHANISM

When data according to the X.800 family of standards [16], security services can be defined as the services that aid the open system interconnection protocols in providing adequate security to the transferred data over the system. These services can be divided into six categories: authentication, data privacy, data integrity, data confidentiality, non-repudiation and data provenance. The authentication service includes data origin authentication and entity authentication. The mechanisms to achieve this service include encryption and digital signature schemes. These mechanisms can be provided using public key cryptography, which will be explained later in Section III. The data privacy service can be achieved by access control mechanisms. The data confidentiality service can also be obtained by encryption and; therefore, public key cryptography can be used. The data integrity service can be achieved by message authentication codes using the secret key or the public key cryptography. The integrity mechanisms include replicating of the data and validating that replicas match. The non-repudiation service assures that no one can deny his/her action later and this can be provided using digital signature schemes; therefore, public key cryptography techniques can be employed.

Further, we add the data provenance as another service to achieve tracking and monitoring of the data or resources. Therefore, our discussion will include services such as authentication, data privacy, data integrity, and data confidentiality. Authentication and confidentiality are both provided by the public key cryptography; hence, these two will be combined in the same section. Privacy and integrity will be discussed in separate sections. It should be noted that nonrepudiation is already provided by blockchain as will be explained later in Section II; therefore, we will not consider it among the services discussed later in the paper.

IV. BLOCK CHAIN BACKGROUND

The architecture In this section, a brief introduction to the blockchain technology is first presented. Following that, mining or block construction techniques are explained. The appealing characteristics of blockchains are also discussed along with a comparison of different open-source blockchain implementations. The objective of this section is to introduce the readers to the blockchain technology and its key principles.

A. Blockchain Architecture: A blockchain consists of a database and a network of nodes, as llustrated in Fig. 2. A blockchain database is a shared, distributed, fault-tolerant and append-only database that maintains the records in blocks. Although the blocks are accessible by all the blockchain users, they cannot be deleted or altered by them. The blocks are connected to each other in a chain as each block has a hash value of its predecessor. Each block contains several verified transactions. Also, each block includes a timestamp indicating the creation time of that block, and a random number (nonce) for cryptographic operations. The blockchain

network consists of nodes that maintain the blockchain in a peer-to-peer, distributed fashion. All nodes have access to the blocks, but they cannot completely control them.

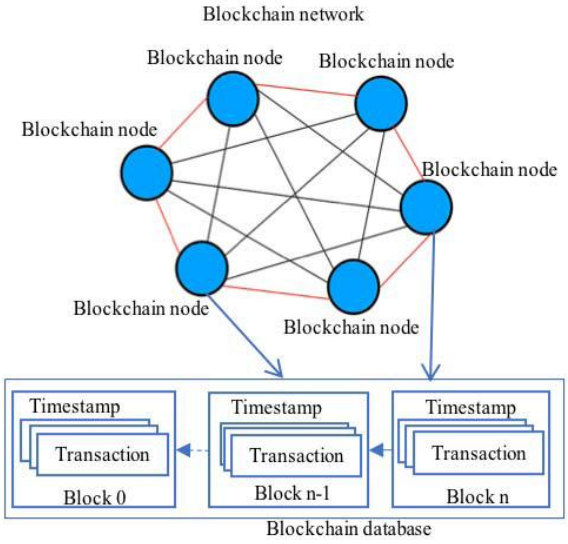

Fig 2. Blockchain network, database, blocks, and transactions.

The blockchain technology allows the communicating parties to interact in the absence of a trusted third-party. The interactions are recorded in the blockchain database providing the desired security requirements. When a blockchain user needs to interact with another user, it broadcasts its "transaction" to the blockchain network. Several nodes in the network check if the interactions are valid and construct a new block of valid transactions by mining (i.e., combining several valid transactions). The making of the blocks will be discussed further in the next subsection. If the new block is found valid, it is attached to the blockchain database and cannot be deleted or altered later. Otherwise, the block is dropped. Both the transactions and the blocks are signed; hence, they cannot be reverted or denied in the future.

The blockchain technology has three generations that support money transactions, assets, and smart contracts, respectively. The first generation was published by Satoshi Nakamoto in 2009 [1]. The application of this generation was restricted to money transactions and was implemented as a part of the Bitcoin cryptocurrency, which was the first application utilizing the blockchain concept. The second generation of the blockchain technology had broader use cases that exchanged assets rather than just money. In this generation, users own "shares" or "assets" and they can exchange any type of assets, including goods, properties and even votes [2]. In the third generation of the blockchain, smart contracts were introduced. A smart contract is a programmable contract that is checked by everyone in the network; thus, it compels both communications parties to strictly follow the contracts. The capabilities of blockchains were enhanced significantly within the third generation which led to its worldwide popularity and an increasing interest in its applications for several other critical services [7].

B. Mining a Block in a Blockchain: Mining is the process of creating blocks that will be attached to the database. In some of the blockchain applications, such as in Bitcoin, the miner who creates the first valid block is rewarded. This reward is given by the system and is generally in terms of money for financial applications. Mining is one of the critical concepts in the blockchain technology. It allows nodes to create blocks which will be validated by others as well. If the new block is found as valid, it is attached to the blockchain database. Nodes that try to create blocks are called *"mining nodes."* The mining nodes race to validate the transactions and create a new block as fast as they can to win the reward. Several approaches exist to decide which miner wins, including proof of work (PoW) [17], proof of Stake (PoS) [18], Proof of Space (PoSpace) [17], Proof of Importance (PoI) [2], Measure of Trust (MoT) [11], minimum block hash [17], and Practical Byzantine Fault Tolerance (PBFT) [18]. In the following, we summarize these major mining approaches.

- *Proof of Work:* PoW is the mining technique used in Bitcoin and is currently used by many other blockchain technologies. It requires the mining nodes to solve a hardmathematical puzzle that is changed frequently and has been agreed by all the miners.
- *Proof of Stake:* Unlike PoW, PoS does not require the mining nodes to solve a computationally expensive mathematical puzzle. Instead, the next block creator or miner is chosen in a pseudo-random way. The chance of a node being chosen to create the new block depends on the node's wealth or stake.
- *Proof of Space:* PoSpace is similar to PoW except that the puzzle requires a lot of storage. A miner proves its ability to create a new block by allocating the required storage space to perform mining.
- *Proof of Importance:* PoI is a mining technique that calculates the significance of an individual node based on the transaction amount and the balance of that node.

C. Blockchain Open-Source Implementation: As there are many open-source implementations of the blockchain technology, the choice of which implementation to use is challenging. In Table IV, we compare different aspects of several popular blockchain implementations. We will be referring to these implementations throughout this paper when we discuss the blockchain-based security services. It is important to keep these features in mind to highlight the properties of each implementation. It should be noted that these are not the only implementations and many others exist in the literature. However, these are the most popular ones used in the majority of the blockchain applications.

V. BLOCKCHAIN-BASED PKI CONCEPT

The distributed, the event-recording and non-reproducibility features of the blockchain technology make it a desirable technique for several applications. Particularly, these properties prove the blockchains' suitability for PKI and domain name services (DNS). Since the blockchain-based PKI solutions are distributed; they have no centralized point of failure. The trust is built based on the majority vote of the miners; hence, there is no single trusted third-party and it does not require prior trustworthiness in the system. More importantly, the blockchain technology has several open-source implementations, which helps build cost-effective and efficient solutions.

In the following, we discuss several approaches to achieve blockchain-based PKI.

A. Instant Karma PKI: In a The Instant Karma PKI (IKP) framework extends the traditional CA approach by recording the CA behavior to the blockchain database. In this way, misbehaving or compromised CAs can be detected by the network and a riposte must happen. The event recording feature of the blockchains facilitates the CA tracking and monitoring by the blockchain users and helps detect the misbehaving CAs. This approach can reduce the trust problem in the traditional CA-based algorithm as eventually misbehaving CA can be detected.

B. Pemcor: In Pemcor utilizes the blockchain database as a distributed and secure data store [36]. The idea is to let the CA issue a certificate which is not signed. Instead, the hash value of the certificate is stored in the blockchain which is controlled by authorities, like by banks or governments. Such authorities share two blockchain databases, one for the generated certificates and one for the revoked certificates. When verifying, the authority checks its maintained blockchain data stores. If the hash of the certificate exists in the generated certificate blockchain and is not in the revoked certificates blockchain, the certificate is valid; otherwise, it is not. This idea is simple and provides several advantages such as an easy verification with low delay guarantees.

C. Gan's Approach: Gan [37] propose a key-based authentication system dedicated to the IoT environments. The idea is to use a private blockchain for storing the nodes' latest public keys, validating the keys, and allowing others to request the nodes' keys. The architecture of this approach is illustrated in Fig. 3, where a Centralized CA (CCA) is assumed to be fully secured. Several validators, donated as Device Manufacturer Validators (DMVs), are connected to the CCA.

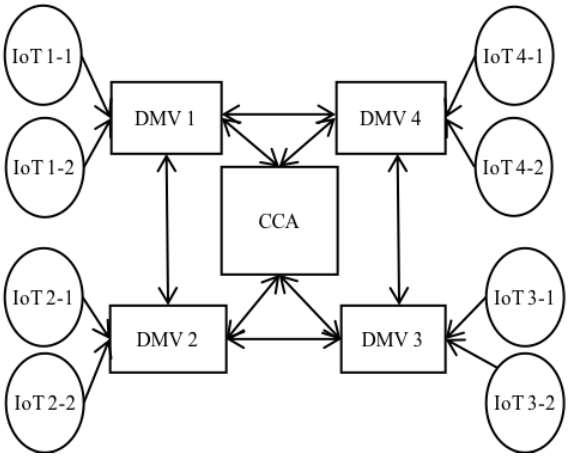

Fig 3: The architecture of Gan's approach.

The DMVs are hosted by the IoT manufacturers and they are required to have the computational capabilities to generate the public/private keys, to perform mining and to maintain the blockchain database. The IoT devices are connected to these validators and are assumed to be simple without any computational capability. Initially, a DMV joins the blockchain network by requesting the CCA to authenticate it. The CCA validates the DMV and constructs a transaction that contains the DMV public key, the validator address, and the CCA's signature. The transaction is submitted to the blockchain and the DMV is now known to the others. Accordingly, the DMV can add a new IoT node by submitting a transaction containing the node's public key and address to the blockchain. Furthermore, the DMVs can update or revoke their IoT devices' public keys by submitting transactions.

D. Distributed PKI (DPKI): Allen *et al.* [38] sketch the principles of an appropriate blockchain-based PKI, which is referred to as Distributed PKI (DPKI). The DPKI uses the blockchain technology as a distributed, trustless database that eliminates the need for a CA and gives the users the direct control and ownership of their data. This work uses a Web registration domain, where the user spawns its public/private key and submits the public key to the blockchain network as a transaction. In this work, it is claimed that the blockchain technology can resolve the traditional problems and protects the network against man in the middle attacks. This rotection is granted by linking the most recent key of the user to his/her identity.

The paper did not include any implementation-related aspects; nevertheless, it introduced the possibility of blockchain-based PKI, which was later implemented in many other works as will be discussed next.

VI. BLOCK CHAIN CHALLENGES

Despite the potential benefits of the blockchain technology, it still has some challenges that limit its practicality for the security applications discussed in the previous sections. In this section, we highlight some of these challenges and relate them to the security applications studied in this paper.

A. Privacy and Anonymity: One of the blockchain's main properties and advantages is providing pseudo-user anonymity. This is critical for security as the public blockchains are open and the user information would be exposed to attackers. However, for most of the discussed approaches, the transactions relate the user identity to their public key, the ACL, or the provenance data. For example, the blockchain-based ACL mechanisms relate the ACL to the users directly; therefore, the users are no longer anonymous. The same issue is applied to the blockchain-based key management and blockchain-based provenance. That is, the privacy and the anonymity features of the blockchains are flawn. Bitcoin resolves the anonymity problem by using the user's public key as the user identification. However, this provides pseudo-anonymity and further research is needed to provide fully anonymized approaches that meet the security application requirements.

B. Computations and Mining Nodes: In most of the current applications, the nodes are simple and do not have high computational capabilities. That is, the blockchain clients need to be simple in order to satisfy the low computation capability requirements. On the other hand, the security services, in general, require significant computations in encryption, decryption, and signature. Moreover, as discussed in Section II, the blockchain technology needs to have mining nodes with high computational power. For most of the proposed techniques, the mining challenge would be resolved by allowing the application nodes to be the blockchain clients and by introducing dedicated mining nodes that are added just to perform mining. However, the high computational power required for these nodes adds to the cost of the system. A better approach would include reducing the computational needs for the mining and relating the mining powers to the node trustworthiness or its reputation in the system. Further, simpler cryptographic schemes can be developed to reduce the computational needs for signing and encrypting the data.

C. Communication Overhead: Current applications are highly dynamic; therefore, they require frequent changes in the access lists and the provenance data. This forces the nodes to send frequent transactions to update the ACL or modify the provenance information. On the other hand, the blockchain technology is a peer-to-peer network, which indicates that a significant overhead will be added in terms of the network traffic and the system processing capabilities. The transactions and the blocks need to be broadcast as opposed to unicast in the traditional techniques. Thus, the overhead added to the network is significant and a considerable challenge. The storage and the processing overhead bring additional challenges in adopting the blockchains for security applications.

D. Scalability: The blockchain technology is believed to scale better than the traditional centralized techniques. However, as reported in [82], the technology performs poorly as the number of users and networking nodes increases [82]. This is a major challenge, especially with network security applications, where thousands of users need to be served and the network scales up fast. Furthermore, the dynamicity of the system adds to the scaling problem as the nodes need to frequently send update transactions. The Ethereum platform and the Hyperledger platform have their own promises for scalability. However, the

performance tests done in [15] show that both platforms still suffer from some aspects of scalability issues.

E. Time Consumption: Providing security services requires fast processing capabilities, especially in the current networks, where milliseconds can cost billions of dollars. Further, mining and achieving consensus are still time-consuming in the blockchains. The proposed approaches resolve the problem by making decisions from the local blockchain logs without requiring distributed consensus. For example, in the blockchain-based ACL mechanisms, the access decisions are made based on the local copies of the blockchain database. However, this defeats the technology decentralized architecture and its consensus as the nodes need to trust the local blockchain database and make centralized decisions. Many promises have been made to resolve Bitcoin's time issues in Ethereum and Hyperledger platforms. However, the time required for mining is still two or three seconds as compared to the milliseconds requirement. Furthermore, building encryptions and security techniques over the blockchains exacerbates the problem of time complexity since such techniques are complex and time-consuming. Thus, faster mining and processing techniques are needed to be able to employ the blockchains for real-time applications.

VII. CONCLUSION

In this paper, we presented a comprehensive survey on the utilization of the blockchain technology in providing distributed security services. These services include entity authentication, confidentiality, privacy, provenance, and integrity assurances. The entity authentication and the confidentiality can be achieved by the public key cryptography using encryption and the signature schemes. Thus, we discussed different blockchain-based key management for public key cryptography.

Finally, we explained how the blockchains can help resolve these problems; explored different blockchain-based approaches and presented a comparison of such approaches. At the end, we studied the challenges that are currently restricting the blockchain's practicality for security applications. The blockchain technology seems to have a great potential in many applications; however, its practicality in security applications is still questionable due to several challenges. Future research directions include resolving these challenges and testing the different blockchain approaches in large scale and real-time environments.

REFERENCES

[1] M. Pilkington, "Blockchain technology: Principles and applications," in Research Handbook on Digital Transformations. Cheltenham, U.K.: Edward Elgar, 2016. Accessed: Feb. 13, 2018. [Online]. Available: https://ssrn.com/abstract=2662660

[2] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, "Bitcoin-NG: A scalable blockchain protocol," in Proc. 13th Usenix Conf. Netw. Syst. Design Implement. (NSDI), Berkeley, CA, USA, 2016, pp. 45–59.

[3] Crypto Currency Market Capitalization. Accessed: Aug. 15, 2017. [Online]. Available: https://coinmarketcap.com/currencies/

[4] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Accessed: Feb. 13, 2018. [Online]. Available: http:// www.bitcoin.org/bitcoin.pdf

[5] STAMFORD. Gartner's 2016 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business. Aug. 2016. Accessed: Feb. 13, 2018. [Online]. Available: http://www.gartner.com/ newsroom/id/3412017.

[6] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in Proc. IEEE 18th Int. Conf. e-Health Netw. Appl. Services (Healthcom), Munich, Germany, 2016, pp. 1–3.

[7] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[8] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA), Agadir, Morocco, 2016, pp. 1–6.

[9] B. Betts. Blockchain and the Promise of Cooperative Cloud Storage. Aug. 2016. Accessed: Feb. 13, 2018. [Online]. Available:http://www.computerweekly.com/feature/Blockchain-and-the-promiseof-cooperative-cloud-storage

[10] L. Mearian, FinTech Builds on Blockchain for International Mobile Payments, Comput. World., Framingham, MA, USA. Accessed: Jan. 22, 2017. [Online]. Available: https://www.computerworld.com/ article/3233187/mobile-wireless/fintech-builds-on-blockchain-forinternational-mobile-payments.html

[11] J. Brantley, "Blockchain can help transform supply chain networks in the chemicals and petroleum industry," Armonk, NY, USA, IBM Cross Bus. Unit, White Paper, 2017. Accessed: Feb. 13, 2018. [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ ssialias?htmlfid=CHJ12351USEN

[12] S. Ahamad, M. Nair, and B. Varghese, "A survey on crypto currencies," in Proc. 4th Int. Conf. Adv. Comput. Sci. (AETACS), 2013, pp. 42–48.

[13] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," Int. J. Netw. Security, vol. 195, no. 5, pp. 653–659, 2017.

[14] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," IEEE Commun. Surveys Tuts., to be published.

[15] M. E. Peck, "Blockchain world—Do you need a blockchain? This chart will tell you if the technology can solve your problem," IEEE Spectr., vol. 54, no. 10, pp. 38–60, Oct. 2017.

[16] Bitcoinwiki. Proof of Work. Accessed: Feb. 13, 2018. [Online].Available:https://en.bitcoin.it/wiki/Proof_of_work

[17] Bitcoinwiki. Proof of Stake. Accessed: Feb. 13, 2018. [Online].Available:https://en.bitcoin.it/wiki/Proof_of_Stake

[18] Wikipedia. Proof of Space. Accessed: Feb. 13, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Proof-of-space