PROTECTION ARMED FORCES USING BLOCKCHAINS: A POSITION OF THE TALENT ANALYSIS

R.Mohana Sundaram, Assistant Professor-Computer Science Vivekanandha college of Arts and Sciences for women

K.Maheswari, Assistant Professor-Computer Science New Prince Shri Bhavani Arts and Science College

ABSTRACT

The analysis blockchain-based approaches for several analysis armed forces. These services include confirmation, discretion, privacy and admission control list (ACL), data and supply attribution, and reliability 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. Validation ensures that the user is he/she claims to be. Discretion guarantees that facts cannot be read by unconstitutional users. Privacy provides the users the ability to control who can access their facts. Derivation allows a capable tracking of the facts and resources along with their rights and exploitation over the network. Reliability helps in verifying that the facts has not been tailored or misused. These services are currently managed by centralized controllers, for example, credential ability. Therefore, the services are lying on your front to attacks on the centralized director. On the other hand, blockchain is a secured and scattered ledger that can help resolve many of the problems with centralization. The objectives of this paper are to give insights on the use of protection services for current applications, to emphasize 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 protection services are compared thoroughly. Challenges associated with using blockchain-based security services are also discussed to prompt further research in this area.

Index Terms—blockchains, public key cryptography, provenance, data privacy, access control list.

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. 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 . 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. The technology currently spans several applications that are popular and driving the networking research. Such applications include healthcare, Internet of Things (IoT) , and cloud storage. Generally, the blockchain technology has proven its potential in any application that currently requires a centralized ledger. A practical example that employs blockchains is the Interbank Information Network provided by JP Morgan which provides fast, secured, and cheap international payments .In addition, supply chain systems by IBM is exploring the potential of using blockchain in their services.

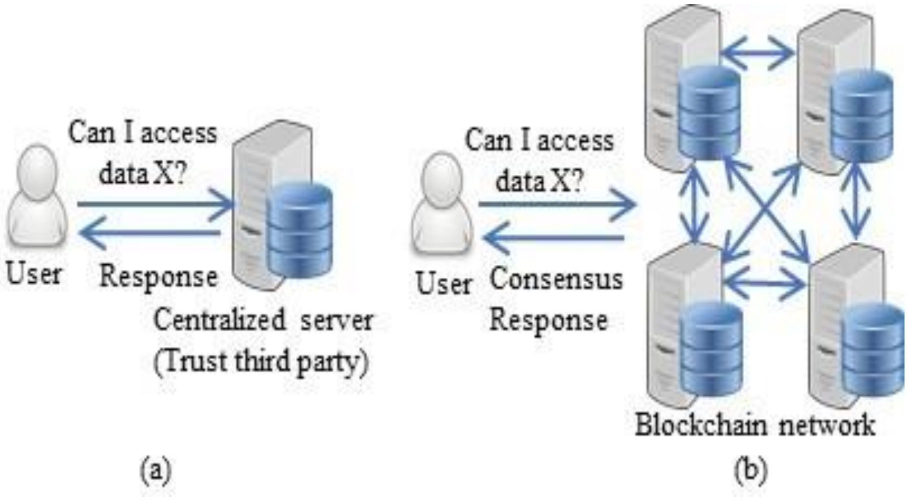


Fig. 1: (a) Traditional centralized access control guarantees (b) Blockchain-based access control guarantees

A. 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, healthcare and decentralized digital currencies . Other surveys have discussed blockchain challenges, opportunities, and future visions. 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.

B.Security Services and Mechanisms

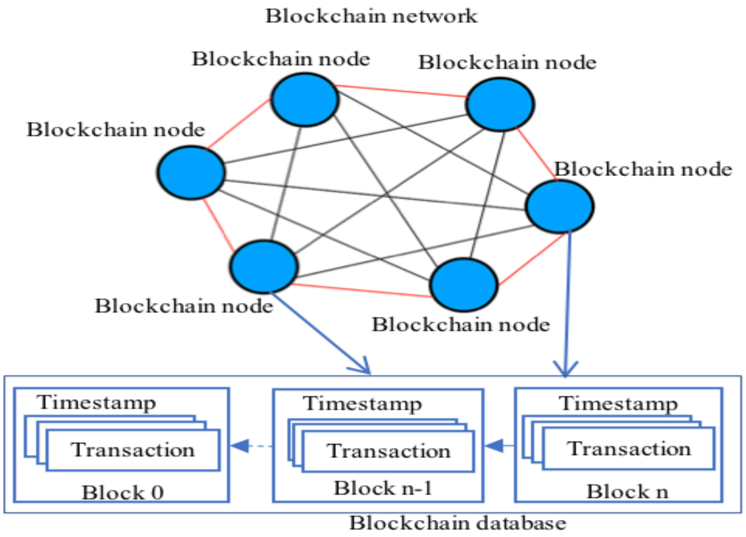
According to the X.800 family of standards, security services can be defined as the services that aid the open system interconnection protocols in providing adequate security to the transferred data over the system. These services can be divided into six categories: authentication, data privacy, data integrity, data confidentiality, non-repudiation and data provenance. In this paper, we consider the blockchain-based security services. 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.

II BLOCKCHAIN BACKGROUND

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 illustrated 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.



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.

C. 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 hard- mathematical puzzle that is changed frequently and has been agreed by all the miners. Once a node validates the transactions and solves the puzzle, the block is submitted to the blockchain network. Other mining nodes validate the block to make sure that the submitter is not falsifying. Once it is agreed among the miners that the block is legit, it will be added to the blockchain and the submitter will be rewarded. The agreement here is based on a majority consensus. Thus, it is difficult to fake unless the attackers

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. In other words, the more money a node has, the higher its chances to mine a block. The native version of PoS does not award the miner; however, the extended versions award and punish the creators based on their performance.

Proof of Space: PoSpace is similar to PoW except that the puzzle requires a lot of storage capabilities. 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. It assigns a priority with a hash calculation to the more significant nodes. Further, the node with the highest priority is chosen for the next block creation.

III ENCRYPTION AND THE AUTHENTICATION SERVICES

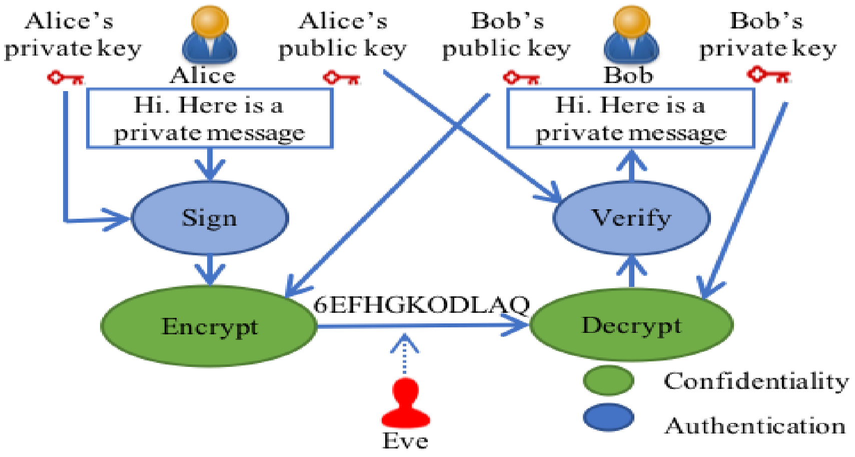
Encryption and authentication are two of the most important security services that must be provided in any network system. In general, these services can be granted using public key cryptography as one of the well-known security frameworks. The public key cryptography techniques require the entities to have private and public information. They need an infrastructure to create, revoke, manage, distribute, use, and store the generated keys or the generated information. In this section, the public key cryptography and its uses in today's applications are first discussed. Following that, an introduction to the public key management techniques and their challenges are presented. Then, an overview of how the blockchains can be used to solve these challenges and some blockchain-based key management techniques are discussed and compared.

A. Public Key Cryptography and Its Services

Public key cryptography, also known as asymmetric cryptography, is a cryptographic technique that uses a pair of keys: public keys which are distributed over the system and private keys which are kept secret. It was introduced initially by Diffie and Hellman in 1975 and is still widely adopted. The basic idea is to use one of the keys to do a task (encryption or signature) and use the other key to do the reverse of that task (decryption or validation). In this way, every entity can verify the message coming from a certain user by the user's public key. The reply message can also be encrypted before sending it back. Only that specific user can sign/decrypt the message with its private key.

The public key cryptography can be used for many security services including the entity authentication and the confidentiality. As illustrated in Fig. 3, the entity authentication service can be provided by the signature/verification procedure. An entity sends a message signed with its private key and everyone can verify/authenticate that entity by validating the signature with the entity's public key. Since the private key is kept confidential, no one can sign the message except the entity itself or someone who has access to the private key. On the other hand, the verification is done with the public keys. Thus, everyone with the user's public information can verify and authenticate that user.

The confidentiality service can be achieved by encryption/decryption, which is a similar procedure. The encryption is done by the sender with the receiver's public key. The decryption is done by the receiver with his private key. Only the receiver, or someone who has the receiver's private key, will be able to decrypt and understand the data. Therefore, the confidentiality is guaranteed.



B. Services' Importance for the Current Applications

Entity authentication and message confidentiality are the most critical services in almost all of the current network applications. A smart healthcare environment is a typical example of the importance of these services. The system is required to secure the transmitted data in order to keep patients' privacy from intruders. Further, it is crucial to authenticate the right doctor, the hospital and the pharmacy and secure their access to the data.

To generate the private/public keys for the system, many algorithms have been proposed, including RSA , ElGamal, and elliptic curve . Discussing these algorithms is out of the scope of this paper. However, in general, these are complex and need an infrastructure to generate and manage the public/private keys. The certificate authorities (CA), the web of trust (WoT) and the entity-based cryptosystem have been introduced to create, manage, use, store, and distribute the keys. In the following subsections, we discuss both the traditional and the blockchain-based key management approaches, including CA and the web of trust. In a later subsection, we discuss the entity-based cryptosystem which is the current trend that extends the CA mechanisms to make a better use of the public key cryptography.

IV. PRIVACY SERVICES

A privacy service offers the user the rights to control and set rules for its data and resources accessed by the network. In other words, it enables the data or resource owners to control the disclosure of their information. This is generally done by letting the user define his access control list (ACL). In this section, we investigate the requirements of providing the data privacy, its importance for the current applications, the traditional techniques for privacy, and the challenges currently faced in providing the privacy service efficiently.

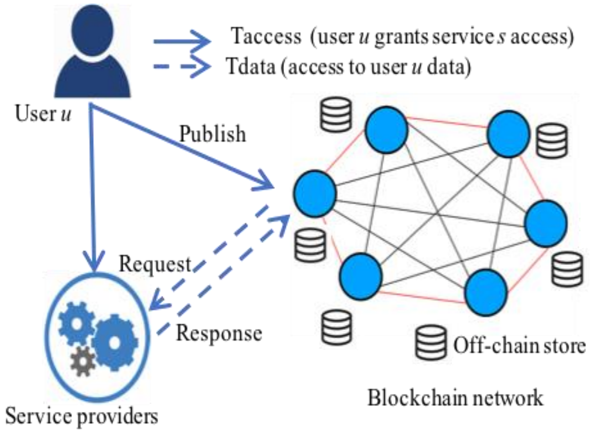
A. Importance of Privacy in Current Applications

The data privacy is a prominent interest in the era of cloud computing and networking systems where many users share the same physical storage or network. Application developers migrate their storage and computations to the clouds and require the data privacy to be granted. Moreover, IoT, healthcare, smart grids, and several other popular networking applications need to process and store a massively large amount of data, generally using cloud computing. Privacy is a critical requirement for most of these applications that are involved with personal information or location knowledge. The problem of privacy is intesified in case of using multiple clouds and internetworking among them.

B. Traditional Techniques for Data Privacy

Generally, the data privacy can be provided by delegating the ACL definitions to the data owners and using encryption techniques to prevent others from accessing the data. Hence, the organizations who amass or process the data have no rights to access the if the ACL does not permit. Design and implementation techniques to provide the privacy service is among the most active research topics, and several techniques have been proposed so far. For example, homomorphic encryption, which allows the computation and the processing the encrypted data and returns encrypted results, is one way to provide the data privacy service [51].

The data is distributed and replicated among the data stores to ensure the privacy and the high availability services.



C. Summary and Comparisons

The data privacy is a critical security aspect that guarantees the user's control over their data disclosures and prevents unauthorized access and processing. In this section, we discussed several blockchain-based approaches providing the data privacy. Such approaches define the ACL either by the smart contracts or by special management transactions. Monitoring of the access rules and the violations can be done by the blockchain nodes to fully eliminate centralization. Table compares the different discussed approaches. It should be noted that these approaches handle the data privacy rather than the user privacy. Most blockchain implementations provide a pseudo-anomalous user privacy using the hashes to identify the users rather than their actual names.

Approach	Blockchain platform	Modifies implementa tion	Smart contract/ transactions	Scalable solution
Zyskind	Ethereum (Enigma platform [59])	Yes	Transactions	No
BBDS	Bitcoin	Yes	Transaction	Yes
FairAccess	Not implemented (Ethereum is planned)	Yes (planned)	Smart contract	No
FairAccess for IoT	Not implemented	Yes (planned)	Smart Contract	No

DRAMS	Ethereum	No	Smart contract	No
[62]	Yes (Bitcoin)	Yes	Transactions	Yes

V SUMMARY

The popularity of the blockchain technology in several nonfinancial applications raised multiple challenges that we discussed in this section. The discussed challenges are related to providing security services and meeting the requirements of the current applications. These challenges include privacy and anonymity, computations and mining nodes, communication overhead, scalability, and time consumption. Privacy and scalability are the most difficult challenges, since they are related to the blockchain-based security applications. A balance between the technology potentials and the its challenges should be considered for efficient designs and solutions. Table XIII summarizes the blockchain-based security application challenges. Till now, the blockchain technology does not seem to be a potential candidate for real- time and delay-sensitive applications. Thus, the future research should tackle these challenges for a practical and widespread use of the blockchain-based security applications.

VI CONCLUSIONS

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. Further, privacy, provenance, and integrity assurance services were studied each in separate sections.

VII. REFERENCES

[1] M. Pilkington, "Blockchain Technology: Principles and Applications," in Research Handbook on Digital Transformations, 2016. [online] Available: https://ssrn.com/abstract=2662660, (accessed February 13, 2018).

[2] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse. "Bitcoin-NG: a scalable blockchain protocol," in 13th Usenix Conference on Networked Systems Design and Implementation

(NSDI'16), Berkeley, CA, USA, 2016, pp. 45-59.

[3] CoinMarketCap.Com, “Crypto Currency Market Capitalization,” [online] Available: https://coinmarketcap.com/currencies/, (accessed August 15, 2017).

[4] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2009. [Online] Available: http://www.bitcoin.org/bitcoin.pdf,. (accessed February 13, 2018).

[4] STAMFORD, “Gartner’s 2016 hype cycle for emerging technologies maps the journey to digital business,” August 2016, [online] Available: http://www.gartner.com/newsroom/id/3412017, (accessed February 13, 2018).

[5] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, 2016, pp. 1-3.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, 2016, pp. 2292-2303.

[7] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, pp. 1-6.

[8] B. Betts, “Blockchain and the promise of cooperative cloud storage”, August 2016, [online] Available: http://www.computerweekly.com/feature/Blockchain-and-the-promise- of-cooperative-cloud-storage, (accessed February 13, 2018).

[9] L. Mearian, “FinTech builds on blockchain for international mobile payments,” Computer World, [online] Available https://www.computerworld.com/article/3233187/mobile- wireless/fintech-builds-on-blockchain-for-international-mobile- payments.html, (accessed January 22, 217).