FRI-2G.302-1-CSN-14

OVERVIEW OF THE BLOCKCHAIN TECHNOLOGIES AND THEIR USE IN THE TELECOMMUNICATION SYSTEMS AND PROCESSES [14]

Assoc. Prof. Plamen Zahariev, PhD
Department of Telecommunications,
"Angel Kanchev" University of Ruse
Tel.: 082 888 663
E-mail: pzahariev@uni-ruse.bg

Eng. Jordan Raychev, PhD Student
Department of Telecommunications,
"Angel Kanchev" University of Ruse
Tel.: 082 888 353
E-mail: jraychev@uni-ruse.bg

Assist. Prof. Diyana Kinaneva, PhD
Department of Telecommunications,
"Angel Kanchev" University of Ruse
Tel.: 082 888 353
E-mail: dkyuchukova@uni-ruse.bg

Abstract: *The blockchain technology is not a new paradigm, but with the global adoption of the cryptocurrencies, this almost three decades old technology has been reborn and is now again on the rise. Initially considered as a technology for decentralised control and security, the blockchain is now being used also for electronic voting systems, auctions, bank transaction and most widely for untraceable and secure Internet payments. What is little known to the public is the fact that the blockchain technology originated as an alternative to the widely known and used at the time cryptographic solutions for protection of the data, which was transmitted over the telecommunication networks. The paper introduces some of the most widely known application areas for the blockchain technology. A special focus is set on the implementation of this technology in the telecommunication systems and networks. The paper also investigates the ways the blockchain technology is currently being used for educational purposes and for research initiatives.*

Keywords: *blockchain, cryptocurrencies, telecommunication networks, AES, bitcoin*

INTRODUCTION

The blockchain technology is not a new paradigm, but with the global adoption of the cryptocurrencies, this almost three decades old technology has been reborn and is now again on the rise. Initially considered as a technology for decentralised control and security, the blockchain is now being used also for electronic voting systems, auctions, bank transaction and most widely for untraceable and secure Internet payments [2].

The blockchain is essentially a distributed list of records, public ledger of transactions or digital events that have beene executed between participants and distributed among them. Each occurred transaction in the public ledged is verified by a consensus of a majority of participants in the system. The verification mechanism ensures that each transaction is verified and no one has tampered with it. Once certain data is verified and entered in the distributed ledger, the information cannot be erased from it. Bitcoin [3] is the most well-known example of using the blockchain technology. It is a distributed peer to peer digital currency where each occurred transaction between peers is verified by the rest of the network. Even tough the bitcoin itself is highly controversioal [1] the underlying blockchain technology has worked flawlessly and found wide range of application in financial and non-financial world.

[14]

OVERVIEW OF BLOCKCHAIN TECHNOLOGY

The blockchain technology is a growing list of public records, called blocks which are typically linked by a cryptographic hash function – each new block of the chain contains a cryptographic hash of the previous block, a timestamp, indicating when the event has occurred and a transactional data, which is typically represented by merkle tree [8]. The blockchain technology has several main properties which are depicted in fig. 1.

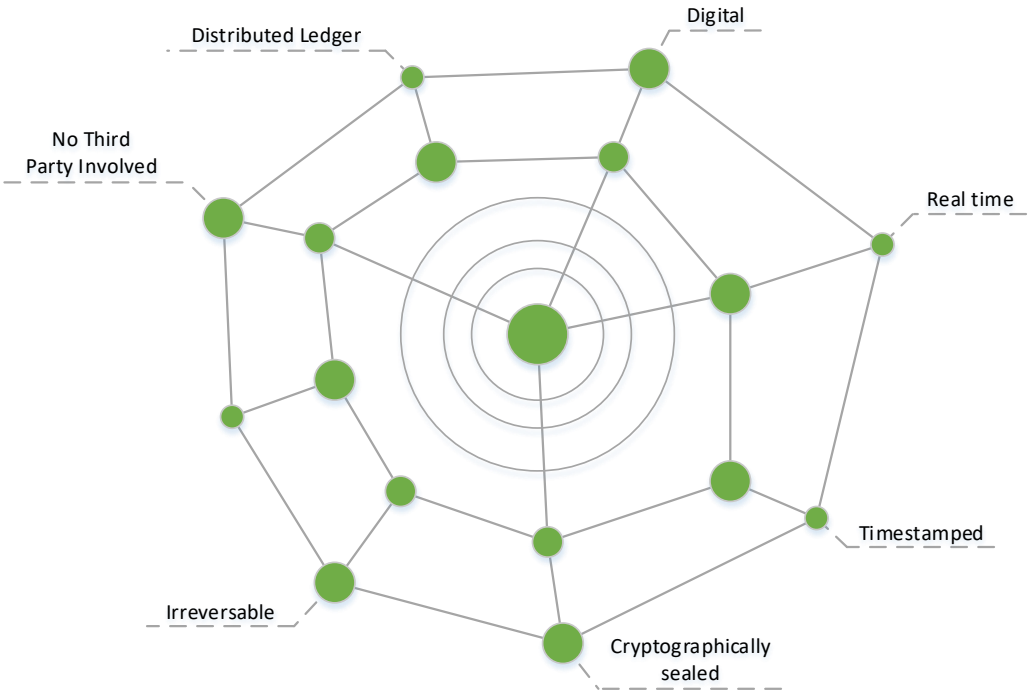


Fig. 1. Main properties of block chain technology

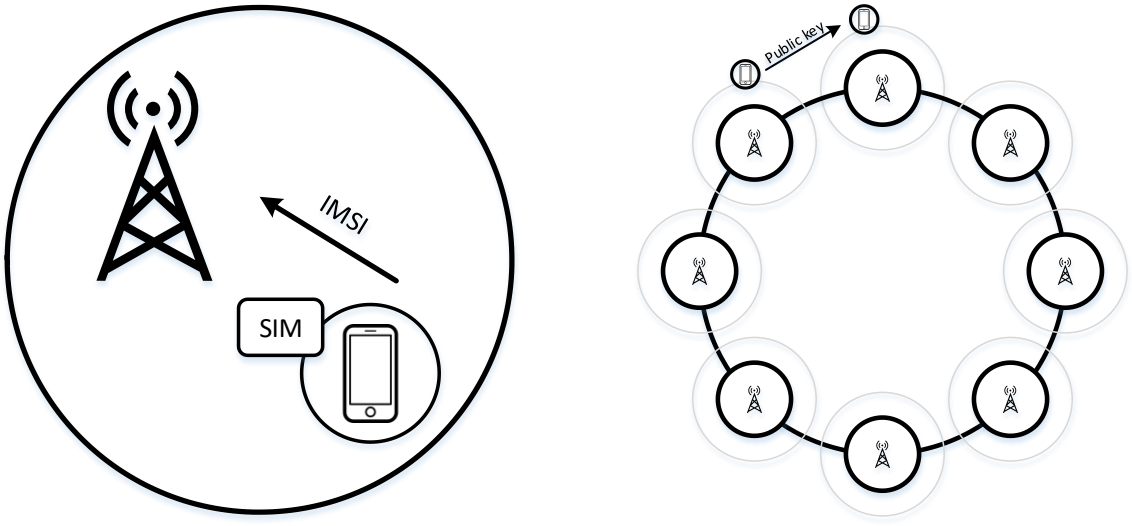
The **distributed ledger** property of blockchain's technology is a consensus of replicated, shared and synchronized data which is geographically spread across multiple sites including countries, institutions and others. The main benefit of this property is the fact there is no central administration point or centralized data storage. Because every participant in the system posseses a copy of the ledger, it cannot be lost if for example one of the nodes fail for some reason (the ledger cannot be lost). The bissest drawback of this property is the fact that each participant has to download the ledger when he or she connects for the first time to the system (network). The bitcoint blockchain ledger for example is around 210 GB as of today [11]. Another property of blockchain technology is the fact that all distributed data is purely **digital** and does not have any physical equivalent. Digital data has several benefits over their physical counterpart including but no limited to easier distribution, better accuracy, lower costs and **real time** updates. As already mentioned in the begginig of the section, each block of the chain contains an UNIX time **timestamp** making it harded for adversary to manipulate the blockchain. In bitcoint blockchain for example a valid timestamp is considered any timestamp that is greater than the median timestamp of eleven previous blocks in the chain and less than the network adjusted time plus two hours. The network adjusted time is the median of the timestamps returned by all nodes that are connected to a particular node. As a result of that, each block in the chain could have different timestamp which may not be even ordered. Besides the security provided by timestamping each and every block, the blockchain technology relies on a **cryptographic hash** functions to function properly. Each block of the blockchain contains some sort of data (currenty, votes and so on) and a hash pointer which points to a previous block, hence creating the chain itself. A hash pointer is similar to a pointer in programming languages but instead of just pointing to the address of previous block it also contains a hash of the data that is inside the previous block. If for example an adversary tampers with the last block of the chain and tries to alter the data, because of the properties of hash function, a slight

change in the data would result in completely new hash. That slight change in last block would change the hash of the previous block and so on and so forth. This changes the structure of the chain which is not even possible, hence making it **irreversible**. The last but certainly not the least property of blockchain technology is the fact that no third parties are involved in the process. Some consider this propery a drawback, but in reallity any person with little to no knowledge of blockchain could use the network and benefit from it.

BLOCKCHAIN APPLICATIONS IN TELECOMMUNICATIONS

Fraud detection and prevention

Fraud detection and prevention continue to be topics of relevance among servie providers (SP) with annually costs of around 38 billion dollars [12]. Given that service providers have not yet found effective and working mechanism that could detect and prevent frauds. Blockchain as a technology has the potential to reduce losses due to fraud and minimize costs for fraud detection applications if properly implemented. Subsription identify theft for example are one area where blockchain technology could be implemented and prevent it successfully. Subsriber identify information is required for SP in order to create individual accounts and assign particular services to that subscribers. SIM (Subscriber Identifitcation Module) is a physical card (chip) which stores the International Mobile Subscriber Identity (IMSI) and related information required to identify and authorize particular user. Each time a mobile device is turned on, it broadcasts a signal containing the IMSI to the nearest base station. That identification number links the device to the account with the carrier. Subscription ID theft occurs when a sub-scriber uses false identification or another subscriber's (victim) ID to obtain services. There are many ways in which a subscriber's identity can be com-promised (email phishing, SIM cloning, etc.). Due to the multiple-play services provided by telecom operators, an ID theft can result in compounded losses through the access to many services under a stolen identity. The blockchain solution to that problem is the use of RSA cryptography (public-private cryptography) which is inherent in a blockchain. Instead of broadcasting the IMSI to the net-work to identify the device, the phone-generated public key is broadcasted instead. The device generates this public key from the private key that is stored securely on it. Neither the carrier nor any other third party needs to know the private key, fig. 2.



A) B)

Fig. 2. Identify authentication in current system (A) compared to a blockchain alternative (B)

In fig. 2B, each cell tower has a knowledge of the public key associated to a particular user. The public key associated with a device (user) is known by all base station in the blockchain network making the authentication process faster and more reliable.

5G enablement

5G technology implementation is another example to potentially benefit from the blockchain technology. To realize the 5G promise of ubiquitous access across various networks, SPs will need to handle heterogeneous access nodes and diverse access mechanisms. Selecting the fastest access node for every user or machine will be a central challenge in the future. Blockchain can enable a new generation of access technology selection mechanisms to build sustainable solutions. Current systems like ANDSF (Access Network Discovery and Selection Function), is an entity which helps in the discovery/selection of access networks, such as WiFi, WiMax, and LTE, in the device vicinity, providing them with rules policing the connection to these networks. It consists of a list of access networks, such as WiFi, that may be available in the vicinity of a device. This information is received in response to a device request which contains its location and capability, such as types of supported interfaces, among others. The received information assists the device in expediting connection to these networks. The ANDSF response contains the following information: the type of access technology (WiFi, WiMAX, etc.), the access network identifier, and technology-specific information (such as one or more carrier frequencies). The main issue is that the system is centralized in a client-server model where the rules stored on the server (ANDSF) are pushed to the client (device). This causes delays and does not allow for seamless provisioning between access networks for the device. Also, the provisioning of rules is not a real-time process – meaning the rules cannot be changed dynamically.

The 3GPP (LTE, GPRS) and non-3GPP (WiMax, WLAN, WiFi) access networks in a given area can be networked via a blockchain where each access point (WiFi router, SP cell tower, etc.) can serve as a node in the network monitoring the devices. Rules and agreements between the various access providing networks can be coded as smart contracts. These contracts can be dynamic in nature wherein any time a policy needs to be changed, only the contract code needs to be changed. When a device broadcasts its identity, it is accepted into the network by the corresponding SP cell. Once the device broadcasts its location, the access node that can best provide service to the device is called upon to do so. Location-based services can also be enabled by being a part of this blockchain network and hence always knowing which devices are in the vicinity.

IoT connectivity

A blockchain can enable secure and error free peer-to-peer connectivity for thousands of IoT devices with cost-efficient self-managed networks [5,6]. For example, machines within a manufacturing plant will be able to communicate and authenticate themselves via the blockchain to steer production processes. Active manual inter-vention by the workforce will for example only be needed if individual machines require service on the basis of predictive maintenance indicators. In addition, the risk of a production shutdown owing to corrupted or hacked machines could be limited, thanks to the distributed and consensus-based authentication of data in the blockchain network. To cope with the increased connectivity demand for devices with low-power consumption, traffic, and bandwidth needs, telcos build Low Power Wide Area Networks (LPWAN). Telcos are facilitating appropriate IoT use cases for regionally and globally operating companies to push and fully amortize LPWANs. These use cases often require appropriate platforms to manage single IoT devices and connect the internal application landscapes accordingly. The current challenges within the IoT field is that devices and sensors usually carry sensitive information about core assets or in some way pertaining to customers of the company, which makes data and network security an essential and costly pillar of IoT connectivity. Also, the size of the network defines network routing and management complexity, leading to varying system landscapes without a common platform. A blockchain based solution allows for highly secure peer-to-peer self-managed mesh networks using a sufficiently large number of nodes. These blockchain network nodes can be represented by single embedded IoT sensors with the ability to verify every block being changed within the blockchain. For a start, these networks can be introduced into a private environment based in mid-range cell towers with relatively low investment requirements. By establishing such a network in a public blockchain language (e.g. Bitcoin or Ethereum [4]), further expansion or evolution into a public blockchain enables seamless connectivity and security.

CONCLUSION

Blockchains concept and technology has grown tremendously in the last decade and are far beyond its use for bitcoin generation and transactions. Blockchains properties such as timestamping, decentralized distribution, security, privacy and inherent data provenance has found its use in many application other than crypto currencies. Few possible application areas have been reviewed in the current paper. The adoption of blockchain appears to be secure especially with the global emergence of Internet of Things. Besides the well-known security benefits, the blockchain technology ensure strong data redundancy due to the distributed nature of the technology and hence survivability.

ACKNOWLEDGMENTS

This paper reflects the results received during the implementation of Project №2018-FEEA-02, funded by the Scientific and Research Fund of the University of Ruse “Angel Kanchev”. The study was financially supported by the University of Ruse “Angel Kanchev” contract №BG05M2OP001-2.009-0011-C01, "Support for the development of human resources for research and innovation at the University of Ruse “Angel Kanchev”", which is funded with support from the Operational Program "Science and Education for Smart Growth 2014 - 2020" financed by the European Social Fund of the European Union.

REFERENCES

[1] S. Underwood, Blockchain Beyond Bitcoin, Communications of the ACM, vol. 59, no. 11, pp. 15-17, November 2016, DOI: https://doi.org/10.1145/2994581

[2] Maaruf Ali and Mahdi H Miraz, "Cloud Computing Applications," in Proceedings of the International Conference on Cloud Computing and eGovernance - ICCCEG 2013, Internet City, Dubai, United Arab Emirates, 2013, pp. 1-8

[3] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Available: https://bitcoin.org/bitcoin.pdf, 2008

[4] G. Wood, Ethereum: A secure decentralised generalised transactionledger, Available: http://gavwood.com/paper.pdf, 2014

[5] A. Dorriet al., Towards an optimized blockchain for IoT, Second International Conference on Internet-of-Things Design and Implementation, ACM, 2017, pp. 173–178.

[6] K. Christidis and M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access, vol. 4, pp. 2292–2303, 2016.

[7] P. Danzi et al., Distributed proportional-fairness control in microgrids via blockchain smart contracts, 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2017.

[8] A. Narayanan et al., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.

[9] R. C. Merkle, A digital signature based on a conventional encryption function, Conference on the Theory and Application of Cryptographic Techniques, Springer, 1987, pp. 369–378.

[10] G. Eibl and D. Engel, Influence of data granularity on smart meter privacy, IEEE Transactions on Smart Grid, vol. 6, no. 2, pp. 930–939, 2015.

[11] https://www.blockchain.com/en/charts/blocks-size

[12]http://v2.itweb.co.za/whitepaper/Amdocs_LINKED_2017_CFCA_Global_Fraud_Loss_Survey.pdf