SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 5, NO. 6
ISSN: 2054 -7420

The Blockchain: Overview of "Past" and "Future"

Arif Sari
Faculty of Business, Department of Management Information Systems,
Girne American University, Kyrenia, Cyprus;
arifsari@gau.edu.tr

ABSTRACT

Variety of network technologies deployed for ease of use and emerging technologies developed for better communication, enhanced security and faster delivery. The global financial crash of 2007-2008 created a lot of distrust between financial institutions and other stakeholders in societies across the globe. The general dissatisfaction caused members of the computing world to begin to ponder if there were electronic ways to ensure that disintermediation could be achieved. This would essentially get rid of the banks as middlemen or the very worst reduce their overall power and boost anonymity regarding transactions. The "Blockchain" is the end result of these deliberations and efforts. It is an unstoppable, trust-based, immutable, peer-to-peer distributed database that has found success in today's world. Its most prominent application is in the crypto-currency field. However, it is slowly but surely being applied to other fields as well. This research paper highlights the previous trends in security and network field and exposing the importance of Blockchain technology interims of specific pros and cons.

Keywords: Blockchain, Blocks, Bitcoin, Distributed networks, Smart contracts.

1 Introduction

The global financial crisis of 2007 and 2008 was a rude awakening for both developed and developing economies alike. The mismanagement perpetrated by the mega banks and other financial institutions reverberated across the globe with catastrophic consequences. Businesses have closed and unemployment rates shot up in several countries all over the world. It certainly did not help public confidence that many of the key actors in this tragedy were allowed to walk away with huge bonuses while average people were left with nothing. It is this sentiment that led to the conclusion that banks had too much power. In fact, at the time, a new phrase was coined by the government of the US; "too big to fail". The sentiment that banks had too much power led several participants in the economics and computer science field to begin to explore other alternatives to the current financial system. In 2008, a white paper called, "Bitcoin: A Peer-to-Peer Electronic Cash System" was published by Satoshi Nakamoto. This white paper discussed the technicalities of developing a peer-to-peer electronic cash system called "Bitcoin" which would essentially cause disintermediation and improve transaction anonymity for its users. The ultimate effect of such a system would be the dilution or elimination of the power wielded by the banks and other financial middlemen. According to Nakamoto, this electronic cash system would run on a system without any central authority to regulate and eliminate double spending. It would also be based on a system where information would be transmitted via chains of data known as blocks. Deloitte

DOI: 10.14738/tnc.56.4061
Publication Date: 5th December 2017
URL: http://dx.doi.org/10.14738/tnc.56.4061

describes the blockchain as a distributed ledger where data is stored in fixed structures referred to as blocks. They go on to say that the crucial components of a block at its header and its content. Furthermore, the header contains metadata such as the time at which the block was created, its unique reference number and a link that points back to the previous block. On the other hand, the content is comprised of digital assets, instruction statements and transactions. Finally, they describe the common properties of all blockchain as follows:

- Blockchains are digitally distributed across a peer-to-peer system in real-time
- Blockchains are based on reaching consensus amongst the peers
- Identity is proved on a blockchain by using digital signatures and cryptographic techniques
- Changing a record on the blockchain is a daunting and near impossible process. Hence, the key requirement of the immutability of the ledger is met
- The entire system is time-stamped and programmable

This research paper seeks to explain the concept of the block chain and discuss the potential and existing applications of this technology. The following sections elaborate the previous related work done in the field of network security and communication before getting into details about Blockchain technology. The importance of the technology and proposed blockchain technology is elaborated with specific pros and cons before concluding the research paper.

2 Related Work

Countries faced with many challenges because of corruption in government and public services. The virtualization of E-government services and practices helped developed and developing countries to decrease corruption and emerging technologies deployed to enhance e-government systems in different countries [1-2]. However due to variety of problems in existing virtualization technology and telecommunication infrastructure, the blockchain technology started to spread among developed and developing countries.

The researchers focused on developing variety of different technologies in order to enhance secure communication environments [3-8]. The proposed mechanisms targeted to reach maximum efficiency with high level of security during data transmission in order to prevent intruders to gain unauthorized access. The governmental and non-governmental organizations focused on deployment of different technologies to propose a secure environment and protect user/customer data. The different security environments required different security proposal where all intermediaries and all nodes communicate in secure environment and shared data is prevented from alteration or modification [9-14].

The most important aspect of providing security was focusing on different layers of communication and proposing a lightweight communication platform that would be scalable, flexible and fault-tolerant. The proposed security solutions against any kind of attack necessitate separate mechanisms that will focus on different events on data such as anomalies [15-21]. However the emerging technology called "Blockchain" provided all these series of functions together free of charge. Even the deployment of different application in different environment, such as Big data and cloud environment become much easier and applicable due to security and flexibility of the blockchain environment [22-23].

Researchers support different ideas about blockchain as it will decimate the financial sector. According to them, the effect of the blockchain on the financial services industry will be as devastating as the effect of

the Internet on the music industry. Ultimately, it will leave the power and near monopoly of banks in tatters. They posit that, bitcoin will be the catalyst that will drive individuals and organizations to adopt the blockchain. They also talk about how the blockchain will enable other mechanisms such as smart contracts, asset registries, etc. that transcend the scope of banks and other financial services entities. The ability of blockchain technology to disrupt the financial services sector has not been lost on the banks. In fact, banks are beginning to build their own blockchains and are expected to implement them in 2017 [27]. Gupta goes on to paint a rather intriguing picture of how the blockchain could be used for transactions in the future. For instance, he describes a scenario where driverless electric cars will be able to use the blockchain to pay for recharge services at charging stations and drones will utilize the same system to pay landing fees at landing pads. Despite all these delightful prognostications, he admits that it is difficult to really know how far the technology will go in terms of adoption and implementation. Despite all these fanciful illustrations of the potential applications of blockchain technology to our world, perhaps a more in-depth look at the technology would be appropriate. Researcher describes the blockchain as a network of value as opposed to the Internet which is a network of information [27]. Perhaps this suggests that the blockchain is a potential upgrade for the Internet in the sense that the blockchain is a more reactive type of network to its users and environment. He goes on to discuss how all blockchains are based on the concept of a distributed ledger which allows users on a particular blockchain to deduce the state of the ledger at any given point in time. Users are also allowed to make additions to the block chain and the acceptance and balancing of these additions/transactions is carried out by common agreement via a consensus algorithm. This algorithm essentially regulates how new transactions can be added to the blockchain and verified as the true state of the data/information in the distributed ledger. The consensus algorithm is decentralized making it hard to corrupt or manipulate. Also, the system is secure due to a combination of decentralization, game theory and cryptography. The consensus algorithm has an aspect referred to as “proof of work” which incentivizes the members of the blockchain to process and regulate transaction addition and maintenance using cryptography as a valid tool. For instance, on the bitcoin blockchain, any network node can take part in the consensus. Each node competing in the consensus is referred to a miner. These miners compete in time spans of ten minutes to generate the next block of transactions to be added to the blockchain. A node is rewarded with bitcoin for successfully adding a block to the blockchain. Hence, this encourages miners to continue engaging in the aforementioned competition because it leads to asset growth.

The innovation in information and information is known as blockchain which is good for static data and dynamic data, making a record in a system. In blockchain data can be save in three forms [24-27];

Unencrypted data – it the fully transparent and can ready by every participant.

Encrypted data – Participant can read it with decryption key.

Hashed data – can be accessible beside the purpose that made it to show the data wasn’t interfered with [28].

Bitcoin has secured by 3,500,000 TH/S in more than 10,000 well known banks around the world, blockchain is so large and has cumulative so much computing power [28]. Bitcoin comparatively a new form of digital currency and it became common, where not many people know about and are making effort to use it [28]. The blockchain used as an emerging technology that has the potential to secure the transaction and to prevent intruders for unauthorized access. Apart from this, the blockchain have nothing

to do with bitcoin and especially for Wall Street purposes. Blockchain is far more beyond bitcoin and have much work to do with [32].

Bitcoin and other digital currency is getting known in 2017, but the more focus is on now blockchain. It is beyond virtual currency and has much more possible way other than just serving to bitcoin [29].

3 Importance of Development

As described above, blockchains have the potential to revolutionize the world of technology and communication. At the very least, it is very likely to disrupt the financial industry and turn it on its head. The technology also has the potential to disrupt other markets such as the entertainment industry, the energy industry and even electoral processes. The group of researchers has described as how the blockchain can cause disintermediation in the entertainment industry [31]. Essentially, artists would be able to earn more because they would be able to sell their content directly to consumers using smart contracts. The various levels of middlemen would be eliminated and artists would be able to regulate content consumption and sale via smart contracts; programmable bits on a blockchain. In the energy sector, a scenario is described where independent generators of energy via renewable sources such as solar, are selling energy to one another via blockchains [30]. The large utility firms across the world are taking note of the trend and quite a few in countries such as Austria and Germany have started experimenting with blockchain technology. A comparison of the applications of blockchain technology in the financial services, entertainment and utilities industries generates a clear theme: disintermediation. The decentralized, distributed, transparent, programmable and anonymous nature of the blockchain is a death knell for middlemen. Smart and proactive companies are taking note and embracing the technology in a bid to remain relevant with time.

4 Methodology

As described above, blockchains have the potential to revolutionize the world of technology and communication. At the very least, it is very likely to disrupt the financial industry and turn it on its head. The technology also has the potential to disrupt other markets such as the entertainment industry, the energy industry and even electoral processes. Researchers describe how the blockchain can cause disintermediation in the entertainment industry [31]. Essentially, artists would be able to earn more because they would be able to sell their content directly to consumers using smart contracts. The various levels of middlemen would be eliminated and artists would be able to regulate content consumption and sale via smart contracts; programmable bits on a blockchain. In the energy sector, researchers describe a scenario where independent generators of energy via renewable sources such as solar, are selling energy to one another via blockchains [32]. The large utility firms across the world are taking note of the trend and quite a few in countries such as Austria and Germany have started experimenting with blockchain technology. A comparison of the applications of blockchain technology in the financial services, entertainment and utilities industries generates a clear theme: disintermediation. The decentralized, distributed, transparent, programmable and anonymous nature of the blockchain is a death knell for middlemen. Smart and proactive companies are taking note and embracing the technology in a bid to remain relevant with time.

The Hash

Researchers defines a hash is the encrypted output of a bitstring. It is always a fixed-length output regardless of the length of input bitstring. The hashing algorithm used is usually SHA256. Also, on a blockchain, hashes must be collision-resistant. This means that is should not be possible to find colliding inputs. In other words, once a bitstring has been hashed, a slight alteration to it creates a completely different hash of the same length. On a blockchain, if a block's hash is tampered with, the hash will change and will not correspond to the hash recorded all along the blockchain. This will indicate that the block is invalid and it will be ultimately dropped from the blockchain [33].

The Nonce

A nonce is an abbreviation of "number used once". In a blockchain, it is generally a very large random number, usually 32-bits and it is typically used once. The nonce plays a key role in the computation and validation of a hash in a block on a blockchain. It is a key part of the "proof-of-work" algorithm which is employed by the block chain to ensure that data validity on the blockchain is maintained and miners are rewarded for their computational expenditures on the blockchain [34].

The Transactions

The transactions are quite simply that; transaction records. They are records of the transactions between users. In the case of bitcoin, it would comprise of transaction values and wallet ids. Transactions are generally visible to every member of the block chain. However, the use of wallet ids ensures that the actual owners and nature of the transactions are anonymous.

How it works

According to a research explained in the literature [34], when transactions are pushed to the blockchain to be processed and added, the following scenario plays out:

- Nodes on the network compete to be the first to process said transactions. They do this to receive a reward for their computational expenditure
- The computational expenditures occur due to nodes competing with each other to guess the correct nonce that when combined with the block payload generates an appropriate and corresponding hash. On average, this process takes about 10 minutes to complete. The successful node is rewarded with cryptocurrency.
- Once the cryptographic "puzzle" is resolved, the block is added to the blockchain and broadcast to all nodes.

5 Implications

The blockchain is a consensus based, secure, distributed, immutable network of value. The distributed nature of the network, the consensus and the proof-of-work algorithms ensure that it is difficult to corrupt or manipulate data on the distributed network. To do so, you would need an exponentially increasing degree of computational power. Therefore, it is unlikely that any one node will be able to effect a change to an already added block on the blockchain and even then, all the other nodes on the blockchain would have to successfully validate it for it to be accepted on the blockchain.

From the business perspective, the aforementioned aspects of blockchain technology make it viable for many industries/sectors. The distributed ledger paradigm and overall transparency of the system means

that it is quite difficult to attack or corrupt the transactions housed on the network. The fact that the blockchain is programmable creates a paradigm where transactions can automatically regulated by smart contracts. These are scripts that essentially regulate how a transaction will proceed. As stated earlier, several industries have taken notice and have begun to experiment with the technology.

Many companies started to deploy blockchain technology to replace current database systems or conventional RFID based systems in order to trace complete transactions of the organizations in a secure environment [35].

6 Conclusion

In conclusion, it is clear that blockchain technology maybe the future of digital communication. It has the potential to disrupt so many industries; the financial industry is the most obviously affected. It is an open, distributed, secure and programmable system where elements of cryptography and game theory ensure that the system works. Many companies and other organizations are working to get it effective in all possible manners. People discuss that in the future people will use blockchain in their daily life not only in the form of transaction but also it will give them a complete way to use it in their organization for record keeping and many more. Blockchain can provide positive shift in the dynamic market. One of the reason that a blockchain is have such impact compare to centralize system is that the centralize system it can work but it also a single time failure whereas in blockchain there are distributed ledger where recording of all transaction is not going to happen in one place but also its written in thousands and thousands of places it can't go down and it is always transparent and people can always look it up, so it's difficult and almost impossible to hack because the one have to hack every single computer at the same time or he/she has to double all network at once that is impossible to do so, or possible with quantum computers which are not easy to produce to conduct such operation today. There are indicators that the technology is receiving greater adoption and relevance across several industries. In other words, it is unlikely that interest in blockchain technology is going anywhere but up.

REFERENCES

[1] Sari, A. (2016); "E-Government Attempts in Small Island Developing States: The Rate of Corruption with Virtualization", Science and Engineering Ethcis, Springer , pp.XX. ISSN-O: 1353-3452, DOI: 10.1007/s11948-016-9848-0.

[2] Sari, A., Akkaya, M., Abdalla B., (2017) "Assessing e-Government systems success in Jordan (e-JC): A validation of TAM and IS Success model". International Journal of Computer Science and Information Security, Vol.15, No.2, pp.277-304, ISSN:1947-5500.

[3] Alzubi, A., Sari, A., (2016) "Deployment of Elliptic Curve Cryptography (ECC) to Enhance Message Integrity in Wireless Body Area Network". International Journal of Computer Science and Information Security, Vol.14, No.11, pp.1146-1153, ISSN:1947-5500.

[4] Sari, A, Akkaya, M., Fadiya, S., (2016) "A conceptual model selection of big data application: improvement for decision support system user organisation" International Journal of Qualitative Research in Services, Vol.2, No.3, pp. 200-210. http://dx.doi.org/10.1504/IJQRS.2016.10003553

[5] Alzubi, A. and Sari, A. (2016) Deployment of Hash Function to Enhance Message Integrity in Wireless Body Area Network (WBAN). Int. J. Communications, Network and System Sciences, Vol.9,No.12, pp. 613-621. http://dx.doi.org/10.4236/ijcns.2016.912047

[6] Sari, A., Rahnama, B., Eweoya, I., Agdelen, Z. (2016) Energizing the Advanced Encryption Standard (AES) for Better Performance. International Journal of Scientific & Engineering Research, Vol.7, No.4, pp.992-1000, ISSN 2229-5518.

[7] Kirencigil, B.Z., Yilmaz, O., Sari, A., (2016) Unified 3-tier Security Mechanism to Enhance Data Security in Mobile Wireless Networks. International Journal of Scientific & Engineering Research, Vol.7, No.4, pp. 1001-1011, ISSN 2229-5518.

[8] Yilmaz, O., Kirencigil, B.Z., Sari, A., (2016) VAN Based theoretical EDI Framework to enhance organizational data security for B2B transactions and comparison of B2B cryptographic application models.International Journal of Scientific & Engineering Research, Vol.7, No.4, pp. 1012-1020, ISSN 2229-5518.

[9] [9] Akkaya, M., Sari, A., Al-Radaideh, A.T., (2016) Factors affecting the adoption of cloud computing based-medical imaging by healthcare professionals. American Academic & Scholarly Research Journal, Vol.8, No.1, pp.13-22.

[10] Sari, A., Onursal, O. and Akkaya, M. (2015) Review of the Security Issues in Vehicular Ad Hoc Net-works (VANET). Int. J. Communications, Network and System Sciences, Vol. 8, No.13, pp. 552-566. http://dx.doi.org/10.4236/ijcns.2015.813050 .

[11] Sari, A. and Karay, M. (2015) Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks. Int. J. Communications, Network and System Sciences, Vol.8, No.13, pp. 567-577. Doi: http://dx.doi.org/10.4236/ijcns.2015.813051.

[12] Cambazoglu, Ş. and Sari, A. (2015) Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite. Int. J. Communications, Network and System Sciences, Vol.8, No.13, pp. 533-542. http://dx.doi.org/10.4236/ijcns.2015.813048.

[13] Sari, A. and Akkaya, M. (2015) Fault Tolerance Mechanisms in Distributed Systems. International Journal of Communications, Network and System Sciences, Vol.8, No.12, pp. 471-482. doi: http://10.4236/ijcns.2015.812042.

[14] Sari, A. and Karay, M. (2015) Comparative Analysis of Wireless Security Protocols: WEP vs WPA. International Journal of Communications, Network and System Sciences, Vol. 8, No.12, pp. 483-491. doi: http://10.4236/ijcns.2015.812043.

[15] Sari, A. (2015) “A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. Journal of Information Security”, Vol.6, No.2, pp. 142-154. doi: http://dx.doi.org/10.4236/jis.2015.62015.

[16] Sari, A. (2015) “Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite”. International Journal of Communications", Network and System Sciences, Vol.8, No.3, pp. 29-42. doi: http://dx.doi.org/10.4236/ijcns.2015.83004.

[17] Sari, A. (2015) "Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks". International Journal of Communications, Network and System Sciences, Vol. 8, No.3, pp. 19-28. doi: http://dx.doi.org/10.4236/ijcns.2015.83003.

[18] Sari, A. (2014); "Security Approaches in IEEE 802.11 MANET – Performance Evaluation of USM and RAS", International Journal of Communications, Network, and System Sciences, Vol.7, No.9, pp. 365-372, ISSN: 1913-3723; ISSN-P: 1913-3715, DOI: http://dx.doi.org/10.4236/ijcns.2014.79038.

[19] Rahnama, B., Sari, A., & Ghafour, M. Y. (2016). Countering RSA Vulnerabilities and Its Replacement by ECC: Elliptic Curve Cryptographic Scheme for Key Generation. In D. G., M. Singh, & M. Jayanthi (Eds.) Network Security Attacks and Countermeasures (pp. 270-312). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8761-5.ch012

[20] Sari, A., (2015), "Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks", New Threats and Countermeasures in Digital Crime and Cyber Terrorism, (pp. 66-94). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8345-7. April 2015.

[21] Rahnama, B.; Sari, A.; Makvandi, R., "Countering PCIe Gen. 3 data transfer rate imperfection using serial data interconnect," Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2013 International Conference on , vol., no., pp.579,582, 9-11 May 2013 doi: http://doi.acm.org/10.1109/TAEECE.2013.6557339.

[22] Sari, A.; Rahnama, B., (2013) "Simulation of 802.11 Physical Layer Attacks in MANET," Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on , vol., no., pp.334,337, 5-7 June 2013, http://dx.doi.org/10.1109/CICSYN.2013.79 .

[23] Sari, A., Rahnama, B (2013). "Addressing security challenges in WiMAX environment". In Proceedings of the 6th International Conference on Security of Information and Networks (SIN '13). ACM, New York, NY, USA, 454-456. DOI=10.1145/2523514.2523586 http://doi.acm.org/10.1145/2523514.2523586

[24] Deloitte. (2016). Blockchain: Engima. Paradox. Opportunity.

[25] Ito, J., Narula, N., & Ali, R. (2017, March 08). The Blockchain Will Do to the Financial System What the Internet Did to Media.

[26] Nakamoto, S. (2008, October). Bitcoin: A Peer-to-Peer Electronic Cash System.

[27] Arbogast, S. (2016, November 21). What Qualifies as a Blockchain? Retrieved November 12, 2017, from Chainskills: http://chainskills.com/2016/11/21/what-qualifies-as-a-blockchain/

[28] Gupta, V. (2017, February 28). A Brief History of Blockchain.

[29] Meola, A. (2017, 28 sep). Business insider. Retrieved 28 sep, 2017, from Business insider: http://www.businessinsider.com/blockchain-technology-applications-use-cases-2017-9

[30] Basden, J., & Cottrell, M. (2017, March 27). How Utilities Are Using Blockchain to Modernize the Grid.

[31] Tapscott, D., & Tapscott, A. (2017, March). Blockchain Could Help Artists Profit More from Their Creative Works.

[32] Crowe, P. (2016, 5 March). Business insider. Retrieved March 2016, 2016, from business insider : http://www.businessinsider.com/what-is-blockchain-2016-3

[33] Kelsey, J. (2016). Introduction to Blockchains. Crowe, P. (2016, 5 March).

[34] Acheson, N. (2016, June 6). How does Proof of Work, um, work? Retrieved November 2017, from Decentralize Today: https://decentralize.today/how-does-proof-of-work-um-work-f44642b24215

[35] Sari, A. (2014); "Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks", Transactions on Networks & Communications, Society for Science and Education, United Kingdom, Vol.2, No.5, pp. 1-6, ISSN: 2054-7420, DOI: http://dx.doi.org/10.14738/tnc.25.431.

