International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: http://dx.doi.org/10.7324/IJASRE.2018.32610

Volume 4, Issue 2
February-2018

A Primer on Blockchain

Matthew N. O. Sadiku, Yonghui Wang, Suxia Cui, and Sarhan M. Musa

[1]Roy G. Perry College of Engineering

Prairie View A&M University

Prairie View, TX 77446

U.S.A

ABSTRACT

Originally developed as the accounting method for the virtual currency Bitcoin, Blockchains are appearing in a variety of commercial applications today. Blockchain technology is a type of distributed digital ledger that uses encryption to make entries permanent and tamper-proof and can be programmed to record financial transactions. It is used for secure transfer of money, assets, and information via a computer network such as the Internet without requiring a third-party intermediary. It is now being adopted across financial and non-financial sectors. As a catalyst for change, the Blockchain technology is going to change the business world and financial matters in major ways. This paper provides an introduction to Blockchain.

Key Words: Blockchains, Bitcoin, Distributed Systems, Distributed Ledger Technology.

1. INTRODUCTION

Contracts, transactions, and their records are critical, defining structures in our economic, legal, and political systems, but they have not being able to keep up with the world's digital transformation. Blockchain (BC) promises to solve this problem. Blockchain (also known as "distributed ledger technology") is a peer-to-peer network that sits on top of the Internet. It was introduced in 2008 as part of a proposal for Bitcoin.. Bitcoin is the first application of BC technology. But what is Bitcoin?

Bitcoin is a cryptographic electronic payment system that purports to be the world's first cryptocurrency. It has become the most talked about cryptocurrency. The software is completely open source so that any developer can download it, modify it, and create his own version of the software. This unique feature has led to an explosion of alternative bitcoin implementations, popularly known as altcoins. Some of the popular implementations include IxCoin, Namecoin, Litecoin, Ripple, Dogecoin, and Bitcoin. Some of the key benefits of Bitcoin include security, transparency, lower transaction costs, anonymity, and resilience. Although Bitcoin is a revolutionary idea, its implementation suffers some problems such as instability, deflation, lack of replicability, computational inefficiency, and lack of regulation or enforcement [1].

The Blockchain could bring everything that is good about Bitcoin and translate it into decentralized applications. Blockchain refers to new applications of a distributed database technology that builds on a tamper-proof records of time-stamped transactions. By decentralizing it, Blockchain makes data transparent to everyone involved and this eliminates the risks that come with data being held centrally. A Blockchain facilitates secure online transactions.

The first Blockchain was conceived in 2008 by an anonymous person or group known as Satoshi Nakamoto, who published a white paper introducing the concept of a peer-to-peer electronic cash system he called Bitcoin [2,3]. Bitcoin and Ethereum are the first two mainstream Blockchains. Other modern Blockchains include Namecoin, Peercoin, Ether, and Litecoin.

2. HOW BLOCKCHAIN WORKS

The term "Blockchain" refers to the way BC stores transaction data – in "blocks" that are linked together to form a "chain." The chain grows as the number of transactions increases. A block is created whenever a transaction is made. A block is the "current" part of a Blockchain, which records some or all of the recent transactions. The block is broadcasted to all nodes for validation.

Once completed, a block goes into the Blockchain as a permanent database. Each time a block gets completed, a new one is generated. Each data item in a BC has a timestamp. A BC is an ordered chain of blocks. All data of a transaction are traceable based on the chain structure of BC.

The Blockchain was designed so these transactions are immutable,i.e. they cannot be deleted. Thus, Blockchains are secure and meddle-free by design. Data can be distributed, but not copied. When it comes to digital assets and transactions, you can put almost anything on a Blockchain. Different scenarios call for different Blockchains.

The BC technology currently has the following features [4,5]:

2.1 Peer-to-Peer (P2P) network:

The first requirement of BC is a network, an infrastructure shared by multiple parties. This can be a LAN at a small scale or the Internet at a large scale. Communication occurs directly between peers instead of through a central node. All nodes participating in a BC are connected in a decentralized P2P network. Transactions are broadcast to the P2P network. Due to some limitations of P2P networks, some vendors have provided cloud-based BCs.

2.1. Cascaded encryption:

A BC uses encryption to protect transaction data. Blocks are encrypted in a cascaded manner, i.e. the encryption result of the previous block is used in encrypting the current block. The BC is secured by public key cryptography, with each peer generating its own public-private key pairs.

2.2. Distributed Database:

A BC is digitally distributed across a number of computers. Each party on a BC has access to the entire database and no single party controls the data or the information. Since BC is decentralized, there is no need for central authorizes such as banks.

2.4. *Transparency with pseudonymity:*

Each node or participant on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others.

2. 5. *Irreversibility of records*:

Once a transaction is entered in the database and the accounts are updated, the records cannot be altered. Records on the database is permanent, chronologically ordered, and available to all others on the network.

There are two types of Blochains: public and private. Public Blockchains are cryptocurrencies such as Bitcoin, enabling peer-to-peer transactions. Private Blockchains use Blockchain-based platforms such as Ethereum or Blockchain-as-a-service (BaaS) platforms running on private cloud infrastructure. They limit access to the predefined list of known individuals. A private BC is an intranet, while a public BC is the Internet. Companies will be disrupted the most by public Blockchains.

BCs may be permissioned or permissionless. In a permissioned BC, each participant has a unique identity. Permissionless BCs allow anyone to join, participate or leave the protocol execution without seeking permission from a centralized or distributed authority.

3. APPLICATIONS

Most applications of BC involve cross-organizational business processes, exploiting the neutral ground provided by a BC. Blockchain has been applied by government and non-government organizations. Some of its cutting-edge applications are provided text.

- *Smart contracts*: Smart contracts are often regarded as the killer application of Blockchain. BC can be used to create smart contracts which can be executed or enforced without human interaction. Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Such contracts permit trusted, transparent, and irreversible transactions and agreements to be carried out among disparate, anonymous parties without the middleman. They turn BC into a middleman to execute all manner of complex business deals, legal agreements, and automated exchanges of data. An example of smart contract utilization is in the music industry, musicians can share free-trade music and ensure that the profits go back to the artists. If contracts are automated through Blockchain, what will happen to traditional structures, processes, and intermediaries like lawyers and accountants? [6].
- *Business*: Some have claimed that Blockchain will revolutionize business and redefine companies and economies. BC protocols facilitate businesses to use new methods of processing digital transactions. BC technology has a large potential to transform business and to bring significant efficiencies to global supply chains, payment system, remittances, national digital currency, financial transactions, banking, asset ledgers, insurance, real estate, stock exchange, etc. The distributed ledger technology systems enable businesses and banks to streamline internal operations, dramatically reducing mistakes caused by traditional methods for reconciliation of records. For example, the transfer of a share of stock can now take up to a week, but with BC it could happen in seconds [7].
- *Healthcare*: Appling BC in heathcare serves to improve patient care. BC technology offers patients and care-givers the ability to securely share patient identity and healthcare information across platforms. Imagine a future where patients hold the keys to their healthcare passport. Imagine a better quality of care for both patients and care providers [8].
- *Supply chain*: This is one of the most obvious Blockchain application. Different partners can access the distributed ledger with the necessary permissions. BC can be used to capture information about the shipment of goods. Each participant in a supply chain can see the movement of goods through the supply chain and understand where a particular container is in transit.
- *Internet of things*: IoT will play a major role in both civilian and military contexts. IoT security is a serious issue. BC technology can be used to enhance security of IoT. It has the potential to facilitate secure sharing of IOT datasets and securing IoT systems [9]. BC integrates and automates machine-to-machine and IoT payment network for the machine economy.
- *Notary public*: BC can be used to verify authenticity of a document without the need of centralized authority. Using BC for notarization secures the privacy of the document. It eliminates expensive notarization fees and ineffective means of transferring documents. Law firms are using BC technology as a cost effective way to certify documents [10].
- *e-Voting*: On regular basis, votes are recorded, counted, and checked by a central constituted authority. Blockchain-enabled e-voting enables voters to carry out these tasks by themselves and hold a copy of the voting record. An illegitimate vote will not be allowed because other voters will notice that it is not in agreement with the rules. This approach may work well for a minor organizational elections with a small number of voters and limited resources [11].

Blockchain can also be used in identity management, utilities, real estate, law, tax reporting, postal service, notary public, microgrid, wireless networks, agriculture, architecture, patents, aircraft maintenance, online gaming, food safety, and music industry. The potential applications for BC technology are almost without limit.

4. BENEFITS AND CHALLENGES

There are a couple of reasons why so many people in the technology and financial sectors are excited about the promise BC holds. First, BC is a great solution to the age-old human problem of trust. It enables trustless networks by allowing parties to conduct transactions even though they do not trust each other. The absence of a trusted middleman results in faster reconciliation between parties. BC removes the intermediary and moves towards democratization and decentralization [12]. Second, by allowing digital information to be distributed but not copied, BC technology has created the backbone of a new form of Internet. There is no single point of failure from which digital assets can be hacked or corrupted. Third, the decentralized nature of BCs makes them an equality technology that can be used to expand freedom, actualization, and realization of all entities, both human and machine. The potential benefits of BC extend into business, political, humanitarian, social, technological, and scientific realms. These benefits make some to believe that BC has become the fifth disruptive computing paradigm after mainframes, PCs, the Internet, and mobile/social networking [13].

Blockchain technology is not without challenges. There are hurdles to commercial adoption. A major challenge is security. Companies need to have a security standards and systems to protect them from attackers or bad actors. Managing the Blockchains

DOI: dx.doi.org/10.7324/IJASRE.2018.32610

requires substantial computational power in order to maintain security. Regulating and standardizing digital currency and money transmission is difficult. There are legal challenges surrounding Blockchain. Blockchain will disrupt all kinds of legal work, notary publics, contracts, lawyers, and judges. Other real challenges include complexity, politics, regulatory approval, security of online transactions, and consumer privacy. The ever-growing size of the Blockchain is considered by some to be a problem, creating issues of storage and complexity.

In spite of these challenges, the demand for Blockchain-based services is on the rise and the technology is advancing at a rapid pace. Developers have built an array of applications on Blockchains.

5. CONCLUSION

Blockchain is a member of the larger family of distributed-ledger technologies, which encompass all techniques for decentralized record keeping of transactions and data sharing across multiple servers, institutions, or nations. It is perhaps the main technological innovation of Bitcoin. It is the invisible technology that is disrupting the world. It is the heart of the fourth industrial revolution.

Recognizing BC as a revolutionizing technology across the industries, many people are excited about the possibilities that Blockchain technology will bring. Financial managers understand that the Blockchain has the potential to change the financial world.

For more information, one should consult several books on Blockchain available on Amazon.com and *Ledger*, the first peer-reviewed academic journal dedicated exclusively to cryptocurrency and Blockchain.

REFERENCES

[1] A. Guadamuz and C. Marsden, “Blockchains and Bitcoin: Regulatory responses to cryptocurrencies*,” Peer-reviewed Journal on the Internet*, vol. 20, no. 12, Dec. 2015.

[2] “Blockchain,” Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Blockchain

[3] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,”
https://bitcoin.org/bitcoin.pdf

[4] M. Iansiti and K. R. Lakhani, “The truth about Blockchain,” *Harvard Business Review*, Jan./Feb. 2017.
https://hbr.org/2017/01/the-truth-about-blockchain

[5] W. T. Tsai et al., “A system view of financial blockchains,” *Proceedings of IEEE Symposium on Service-Oriented System Engineering*, 2016, pp. 450-457.

[6] V. Shermin, “Distrupting governance with blockchains and smart contracts,” *Strategic Change*, vol. 26, no. 5, 2017, pp. 511-522.

[7] M. Gupta, *Blockchain for Dummies*. Hoboken, NJ: John wiley & Sons, 2017.

[8] S. Manski, “Building the blockchain world: technological commonwealth or just more of the same?” *Strategic Change*, vol. 26, no. 5, 2017, pp. 511-522.

[9] M. Banerjee, J. Lee, and K. K. R. Choo, “A blockchain future to Internet of things security: a position paper,” to appear in *Digital Communication and Networks*, 2017.

[10] M. Crosby et al., “BlockChain Technology”, Sutardja Center for Entrepreneurship & Technology Technical Report, UC Berkeley, Oct. 2015.

[11] P. Boucher, “How blockchain technology could change our lives,” *European Parliamentary Research Service*, Feb. 2017.

[12] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of things*,” IEEE Access*, vol. 4, 2016, pp. 2292-2303.

[13] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O’Reilly Media, 2015.

AUTHORS

Matthew N.O. Sadiku is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interest include computational electromagnetics and computer networks. He is a fellow of IEEE.

Yonghui Wang is currently an associate professor with the Department of Engineering Technology, Prairie View A&M University, Prairie View, TX. His research interests include digital signal processing, image and video coding, and wavelets.

Suxia Cui is an associate professor of Electrical and Computer Engineering Department at Prairie View A&M University. She has published journal and conference articles in the field of wavelets, image processing, and video coding. Her research interests include data compression, signal classification, image and video processing.

Sarhan M. Musa is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Sprint and Boeing Welliver Fellow.

DOI: dx.doi.org/10.7324/IJASRE.2018.32610