ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 8, pp. 19664-19666, August, 2017

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

CHALLENGES AND OPPORTUNITIES ASSOCIATED WITH BLOCKCHAINS AND CRYPTOCURRENCIES IN THE BANKING INDUSTRY

Bhardwaj, Samksha*

Birla Institute of Technology and Science, Pilani Campus, Pilani, Rajasthan, India

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0808.0740

ARTICLE INFO

Article History:

Received 16th May, 2017
Received in revised form 25th June, 2017
Accepted 23rd July, 2017
Published online 28th August, 2017

Key Words:

Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts, Banking Industry, Information Security

ABSTRACT

If the current economic market is any indication, blockchain - best known for its groundbreaking application in the cryptocurrency Bitcoin - is the most disruptive technology for the financial sector since the invention of the Internet. While Bitcoin has naturally been the most popular implementation of the technology, blockchains are finding their way into many more applications. This paper explores the working of blockchain technology in Bitcoin, and other, more advanced cryptocurrencies. It goes on to discuss the advantages of incorporating blockchains in the banking industry, and offers potential applications of the same in various industries.

Copyright © Bhardwaj, Samksha, 2017, this is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

INTRODUCTION

Blockchain, originally developed as a transaction ledger for Bitcoin, was developed to allow individuals or businesses to engage in transactions without involving a third party organisation to monitor and verify the validity of the transaction. The elimination of a third party naturally leads to increased security, anonymity, and data integrity. By effectively decentralising transactions, Blockchain technology has the potential to reinvent the financial sector by offering faster, more transparent, and more secure transactions.

In the traditional banking model, transactions necessarily occur via a trusted central authority, i.e., the bank. Privacy is offered by limiting access to the transaction information to only the parties involved and the trusted third party. However, since this model depends on trust for a secure transaction, it has easily exploitable flaws.

Blockchain offers an alternative to a model based on trust by introducing a model based on cryptographic proof. In simple terms, the Blockchain is an incorruptible digital ledger of transactions. Information about the transaction is made public; however, the information about the parties involved in the transaction is private, i.e., an outsider can see that an amount is being transferred but has no knowledge about the identities of the sender or receiver. Each transaction in this global ledger is verified by consensus of a majority of the participants in the system. Once verified, the the transaction information is a permanent part of the blockchain, and cannot be erased.

While the technology is, at the moment, primarily used for keeping a track of economic transactions made via various crypto currencies such as Bitcoin, it can also be adapted to record virtually everything of value to humankind: deeds and titles of ownership, medical procedures, insurance claims, educational degrees, votes, etc. The distributed consensus model proposed by the technology has a disruptive potential comparable to the early days of the early commercial Internet.

Security in Bitcoin Explained

In 2008, an individual or a group of individuals under the name of Satoshi Nakamoto published a paper titled “Bitcoin: A Peer-To-Peer Electronic Cash System” (Nakamoto, 2008). This paper described a peer-to-peer electronic cash system that would allow online payments to be sent from one party to another without involving an intermediate financial institution.

Each payment is secured using a digital signature. The transaction is digitally signed using the private key of the sender and sent to the public key of the receiver. To spend the electronic coin, the owner of the cryptocurrency is required to

Corresponding author:* **Bhardwaj, Samksha
Birla Institute of Technology and Science, Pilani Campus, Pilani, Rajasthan, India

prove ownership of the private key. The receiver of the electronic coin verifies the digital signature using the public key of the sender to establish ownership of the corresponding private key The transaction is broadcast to every node in the Bitcoin network, and its validity is checked based on two important criteria - whether the spender owns the cryptocurrency being spent, and whether the spender has the sufficient amount in his/her account. If the transaction is valid, it is verified and recorded in the public ledger.

The main problem that arises due to this method is the order of transactions recorded - there is no guarantee that the order in which the transactions are generated is the order in which the transactions will be received. This may lead to double-spending of coins in transactions.

The solution to this was the development of a mechanism that enabled a general consensus regarding the order of transactions, now known as Blockchain technology. Transactions are ordered by placing them in "blocks". Every block contains the hash of the previous block, thereby linking these blocks in a linear, chronological order through the Blockchain (Swan, 2015).

To determine which block will be the next in the network, a proof-of-work was introduced - the node generating a block needs to prove that it has enough computing power to solve a mathematical puzzle. While solving the puzzle is a complex, time-consuming task, verifying the solution of the puzzle is fairly trivial.

On an average, ten minutes are required to solve the puzzle and generate a new block in the network. In case multiple blocks are generated at the same time, the Blockchain considers the longest blockchain as the valid one. This is also the basis for the security of the Blockchain - to modify a previous transaction, an attacker would have to redo the proof-of-work of that particular block, all the blocks after it, and then surpass all other transactions generated in the meantime by honest nodes.

Advancements in other cryptocurrencies

Other groups have taken the idea of blockchain and improved upon the core concept in several ways. This has led to several new cryptocurrencies popping up as alternatives to Bitcoin, most notably Ether.

Like Bitcoin, Ethereum is a distributed public blockchain network. However, there are quite significant technical differences between them - while Bitcoin offers a specific application based on the blockchain technology, Ethereum can be used to create an entirely new, separate decentralised application. The Ethereum Virtual Machine (EVM), a Turing complete software that runs on the Ethereum network, allows anyone to run any program, given enough time and memory. The EVM is a revolutionary innovation in technology - instead of having to build an entirely original blockchain for every new application, Ethereum can potentially be used to develop thousands of different applications on all platforms. A potential application of this is in smart contracts, i.e., self-executing contracts.

Other cryptocurrencies, such as Monero and ZCash, have been developed to address the increasing security concerns surrounding Bitcoin. A critical flaw in Bitcoin transactions is the lack of privacy (Vandervort, 2014) due to the public record. If a Bitcoin wallet address is obtained, it is an elementary matter to find out how much money is present in that wallet, and hence, how much money the user has. The Bitcoin community has attempted to offer 'mixing' techniques to solve these problems but this raises further questions of security breaches (Saxena *et al*, 2014).

Monero takes a different approach to these privacy issues by passive mixing, i.e., automatically applying privacy techniques to all the transactions. In Monero, it's possible to know that a transaction has occurred but not but not whence, how much and whither. What this means is that it effectively impossible to own 'tainted' Monero, thus promising fungibility, an important characteristic for any currency to have (Nicolas, 2017).

ZCash (Eli Ben-Sasson *et al*, 2014), another cryptocurrency, uses a new cryptographic concept known as 'zero knowledge proofs' to do the same thing. While ZCash's technology seemingly offers greater anonymity (and greater fungibility), it is highly experimental. Due to the novelty of the cryptographic concepts, it could take decades to determine whether there are fundamentally critical issues involved in this approach or not. In addition, the computational burden involved in these transactions is so severe that the privacy features have been made optional by the developers, which makes using ZCash redundant.

Advantages of Blockchain Technology

Blockchain provides the opportunity for the participants in a network to share a system of records, which will lead to consensus, immutability, and finality in relation to the transfer of assets in the business network. Distributed ledgers have the potential to be disruptive as they may lead to new business models and the current processes would have to move away from a central hub and spoke model (Yli-Huumo *et al*, 2016)

The key transactions in the typical banking industry are the underpinning of asset ownership and asset transfer. Data messages need to be exchanged between the financial institutions (sometimes via 'trusted' intermediaries) to conclude a transaction. Due to the complexity and reliance on trusts, these processes are expensive, inefficient, and vulnerable (Tandulwadikar, 2016). Through modernization and simplification of the traditional siloed design of the financial industry infrastructure, blockchain technology can address some of the limitations of the current processes.

Key benefits of blockchain technology include

- ***Prevention of fraud:*** Since blockchain technology is built upon the concept of verification through a general consensus during transactions, it is more secure and accessible.
- ***Reduction in costs over delayed settlements:*** Due to the distributed payment network, payments and settlements happen in real time, leading to reduced pressure on management to keep the settlement accounts well-funded.
- ***Increase in resiliency:*** Blockchain technology allows all permissioned nodes in the ecosystem to operate the network. Even when some nodes are not available, the

consensus algorithm ensures that the remaining nodes in the network will be able to approve the transaction. As a copy of the ledger is available to all nodes, blockchain technology also adds a high level of redundancy.

- ***Reduced processing time:*** Due to the linear and hierarchical nature of the conventional banking processes, there are often delays in decision making, and longer processing times as well as greater costs. On the other hand, in blockchains, transaction information is conveyed to all approving nodes, and the ledgers of all the nodes are updated instantly, thus leading to reduced cost of processing, reduced decision making time, and enhances transparency of decisions.
- ***Quicker settlements:*** As majority of the data needed for identity verification is present digitally, blockchain technology could implement instant identity verification, reduce duplicate recordkeeping, and minimise error rates. By removing intermediaries, the settlement time could be reduced to mere seconds.
- ***Finality and immutability in transactions:*** Blockchain technology maintains an immutable and chronological record of transactions, guaranteeing immutability and finality. In addition, this could bring about transparency and efficiency leading to reduced risk, and increased trust.

Applications of Blockchains

- ***Smart Contracts:*** Among the most useful applications of blockchains is the concept of smart contracts - business terms that are automatically executed if specific business conditions are met. The implementation of smart contracts would minimise human intervention in the creation and execution of business rules while simultaneously enabling speed of processing (Ramasastri *et al,* (2017).
- ***Trade Finance:*** If corporates, manufacturers, and shippers along with banks adopt blockchain technology for the handling of letters of credit and bills of lading, trade finance would benefit significantly (Yessi, 2015).
- Tracking Healthcare Allowances: A decentralised system would ensure complete transparency, thereby ensuring that healthcare allowance is used effectively and appropriately.
- ***Post-Trade:*** Without the need for central clearing in transactions, and elimination of intermediaries, post-trade processing would naturally become faster and efficient. Since smart contracts are auto-executed, the liabilities of parties would be established over the life cycle.
- ***Loan Syndication:*** Recently, the first working blockchain solution for syndicated loan servicing was demonstrated by Synaps Loans LLC. The project was arranged by Credit Suisse in collaboration with key agent banks, service providers, and fund managers.
- ***Liquidity creator:*** A blockchain-based system could open up cash in exchange for completion of cross-border transactions at lower rates.
- ***Permissioned blockchains:*** Blockchains can be tailored for specific purposes, as per a client's needs. Ethereum offers such a service to companies to make their own apps and services by using blockchain technology.

CONCLUSION

While virtual currencies remain the most popular application of blockchains, the technology has much wider implications than merely cryptocurrencies. With the recent rise of Ethereum, it's fair to predict that the most important applications of blockchains lie outside the currency division. The increase in security, decrease in transaction times along with cost and the assurity of complete transparency while still maintaining anonymity make blockchains a force to be reckoned with. Most importantly, it promotes a decentralisation of power from intermediaries to communities of peers. While decentralisation is still treated with skepticism by some, Bitcoin and blockchains are rising in popularity, and it's essential for the financial industry to utilise this technology and revamp the traditional banking system.

References

Double-spending; (2017). Accessed: 24/6/2017. https://en. bitcoin.it/wiki/Double-spending.

Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, EranTromer, MadarsVirza, (2014). *Zerocash Decentralized Anonymous Payments from Bitcoin*, proceedings of the IEEE Symposium on Security & Privacy (Oakland) 2014, 459-474, IEEE.

Ethereum: White Paper; 2017. Accessed: 10/09/17. https://github.com/ethereum/wiki/wiki/White-Paper

Nakamoto S, (2008). Bitcoin: A peer-to-peer electronic cash system.

Nicolas van Saberhagen.(2017). CryptoNote v2.0; 2013. Accessed: 20/08/17. https://github.com/monero-project/research-lab/blob/ master/whitepaper/ whitepaper.pdf

Ramasastri A. S., *et al*. (2017). Applications of Blockchain Technology to Banking and Financial Sector in India. IDBRT

Saxena A, Misra J, Dhar A.,(2014). Increasing Anonymity in Bitcoin. Financial Cryptography and Data Security. vol. 8438 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; p. 122-139.

Swan M. (2015). Blockchain, Blueprint for a New Economy. "O'Reilly Media, Inc.

Tandulwadikar A. (2016) .Blockchain in Banking: A Measured Approach. Cognizant Reports.

Vandervort D. (2014). Challenges and Opportunities Associated with a Bitcoin-Based Transaction Rating System. Financial Cryptography and Data Security. vol. 8438 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; p. 33-42.

Yessi Bello Perez (2015), "Santander: Blockchain Tech Can Save Banks $20 Billion a Year," CoinDesk,.

Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016). Where Is Current Research on Blockchain Technology?- A Systematic Review. PLoS ONE 11(10): e0163477.

****