IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12608

Secure Banking Using Ethereum Blockchain

Pranav Parmeshwar Thorve[1], Prof. Dr. Ninad More[2]

D. Y. Patil Institute of Engineering and Technology ambi, Pune[1]

Guide, D. Y. Patil Institute of Engineering and Technology ambi, Pune[2]

Abstract: This paper researches blockchain technology applications for the banking sector. Blockchain is a decentralized ledger used to securely exchange digital currency, perform deals and transactions. Each member of the network has access to the latest copy of encrypted ledger so that they can validate a new transaction. Blockchain ledger is a collection of all Bitcoin transactions executed in the past. Basically, it's a distributed database which maintains a continuously growing tamper proof data structure blocks which holds batches of individual transactions. The completed blocks are added in a linear and chronological order. Each block contains a timestamp and information link which points to a previous block. Bitcoin is peer-to-peer permission-less network which allows every user to connect to the network and send new transaction to verify and create new blocks. Satoshi Nakamoto described design of Bitcoin digital currency in his research paper posted to cryptography listserv in 2008. Nakamoto's suggestion has solved long pending problem of cryptographers and laid the foundation stone for digital currency

Keywords: Blockchain, Decentralized, Bank.

I. INTRODUCTION

Development in IT has enabled new advancements in many industries, not least the financial industry. Banks and companies do not desire to land behind in the development process and are investigating how IT-technologies can be applied in the best way in their branch. One of the most important innovations in recent times is the Blockchain technology. (Guo & Liang, 2016) The characteristic of blockchain technology, building trust faster between people and the potential to change the financial structure, is a major reason why financial leaders are attracted to this technology (Chang et al., 2020). Blockchain technology, also referred to as Distributed Ledger Technology (DLT), is an underlying infrastructure that can be simply described as an immutable ledger shared with the participants on the network, peer-to-peer, without intermediaries between them (Gupta, 2020; Drescher, 2017). The transactions are executed in a decentralized manner. The transactions are stored in so-called blocks, which contain a timestamp, and are cryptographically linked to each other by a hash of the previous block to form an ordered, sequential, blockchain (Chang et al., 2020; Dashkevich et al., 2020; Osmani et al., 2020). Once a block is added to the blockchain, it cannot be altered or erased (Chang et al., 2020; Dashkevich et al., 2020; Osmani et al., 2020).

Banking and financial institutions are using Blockchain based technology to reduce risk and prevent cyber fraud. For example, Nasdaq has announced its plan to launch Blockchain based digital ledger technology which will help to boost their equity management capabilities. Standard Chartered is partnering with DBS Group to develop an electronic invoice ledger using a Blockchain. The Blockchain metadata is stored in Google's LevelDB by Bitcoin Core client. We can visualize Blockchain as vertical stack having blocks kept on top of each other and the bottommost block acting as foundation of the stack. The individual blocks are linked to each other and refers to previous block in the chain. The individual blocks are identified by a hash which is generated using secure hash algorithm (SHA-256) cryptographic hash algorithm on the header of the block .

A block will have one parent but can have multiple child each referring to the same parent block hence contains same hash in the previous block hash field. Every block contains hash of parent block in its own header and the sequence of hashes linking individual block with their parent block creates a big chain pointing to the first block called as Genesis block. Nowadays, we can see that banks have started implementing Blockchain technologies through forming consortiums such as R3 consortium which is one of the most leading and significant in the world (Guo & Liang, 2016). In Europe, a joint venture between twelve major banks, including Nordea, has been established to create the Blockchain platform “we.trade” for many essential purposes, including reducing the time of cross-border transactions and creating an atmosphere of transparency and trust between the involved parties.

Project Resource

Linux, VS code, 4 GB RAM, High speed internet connection.

DOI: 10.17148/IJARCCE.2023.12608

II. LITERATURE SURVEY

1. Bitcoin : A peer to peer Cash System , by Satoshi Nakamoto
Blockchain is a transaction database which contains information about all the transactions ever executed in the past and works on Bitcoin protocol. It creates a digital ledger of transactions and allows all the participants on network to edit the ledger in a secured way which is shared over distributed network of the computers. For making any changes to the existing block of data, all the nodes present in the network run algorithms to evaluate, verify and match the transaction information with Blockchain history

2. Managed Blockchain by Greg Luckock Blockchain is a distributed ledger technology, commonly used in the crypto currency Bitcoin. The Financial Times (2016) defines Blockchain as a \network of computers, all of which must approve a transaction has taken place before it is recorded, in a `chain' of computer code. The details of the transfer are recorded on a public ledger that anyone on the network can see." The proposal was to distribute electronic transactions rather than maintain dependency on centralized institutions for the exchange. When looking at Bitcoin the new concept is the Blockchain framework based on research for time stamping packages and protecting the chain of custody. Blockchain is essentially a simplified payment verification system. Bitcoin and by extension, Blockchain, are realizing steady growth. At the time of this chapter, statistics from Blockhain.info indicate a 314.7M in transactions per day. Despite the growth, many questions surround widespread adoption of Bitcoin. However, the underlying framework has gained attention with application outside of the financial world.

3. Cloudbased Smart Health-care Platform to tackle Chronic Disease by Saman Sargolzaei, Ben Amaba, Mohamed Abdelghani" The objective of the current work was to design and develop a cloud-based smart health data analysis platform for real-time patient-specific health monitoring and analysis with long-term surveillance to support learning based information processing system benefiting from cloud and mobile technologies. A DevOps approach to cloud-based applications development was used to create a platform for remote health data recording.

4. Multi-signature addresses by M. Rosenfeld The private keys needed to spend from a wallet can be spread across multiple machines, eliminating any one of those machines as a single point of failure, with the rationale that malware and hackers are unlikely to infect all of them. The higher the number of keys required to spend the funds (ie the higher M is in M-of-N), the more difficult it would be for an attacker to successfully steal your funds, however the more cumbersome actually using that wallet becomes. The multisig wallet can be of the mof-n type where any m private keys out of a possible n are required to move the money. For example a 2-of-3 multisig wallet might have your private keys spread across a desktop, laptop, and smartphone, any two of which are required to move the money, but the compromise of any one key cannot result in theft. This can be used in conjunction with hardware wallets. By requiring that keys from multiple hardware wallets sign transactions, it can vastly reduce the likelihood that a malicious party that handled your hardware wallet could steal your funds, because in order for it to do that, the malicious party would have to compromise multiple hardware wallets. If each hardware wallet you use in a multisig wallet is made by a different company, it would be incredibly difficult for them to secretly conspire on an attack.

5. Blockchain beyond Bitcoin by S. Underwood As an emerging decentralized architecture and distributed computing paradigm underlying Bitcoin and other cryptocurrencies, blockchain has attracted intensive attention in both research and applications in recent years. The key advantage of this technology lies in the fact that it enables the establishment of secured, trusted, and decentralized autonomous ecosystems for various scenarios, especially for better usage of the legacy devices, infrastructure, and resources. In this paper, we presented a systematic investigation of blockchain and cryptocurrencies. Related fundamental rationales, technical advantages, existing and potential ecosystems of Bitcoin and other cryptocurrencies are discussed, and a six-layer reference model of the blockchain framework is proposed

III. PROBLEM DESCRIPTION

Banks that operate in the financial sector use a traditional system, which is considered the backbone of global trade finance and it is estimated that about more than a trillion dollars is transferred around the world every day using this system. Over the years, many important innovations and technologies, such as credit card systems, the Internet and mobile applications, have been applied to the financial system. These new technologies have been of much benefit in helping banks in conducting their operations through increasing efficiency, convenience and speedier transactions, and reducing the distance between the concerned parties.

Despite these steps toward more advanced technology, there are still many limitations that banks need to address in order to stay relevant and competitive for the finance market’s requirements and assumptions in today’s landscape. The

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12608

transactions are slow and inefficient, expensive, and there are security risks which can have disastrous consequences. Because the banks act as the central system for transactions, a simple mistake made by a bank may lead to serious consequences for the bank and every participant in that system. Furthermore, this centralized system has been vulnerable to cyberattacks conducted by 7 malicious groups or individuals which has led to massive losses and damage to the reputation of financial institutions.

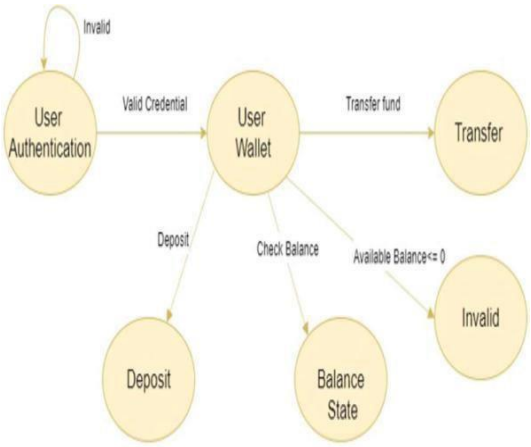
Nearly half of all bank customers in the world have been exposed to fraud and crime attempts during their operations, such as when conducting transactions with stock exchanges, payment gateways, or money transfer agencies. Another big problem for the financial industry is that half of the world's population simply do not have access to a bank account, therefore forcing them to conduct transactions with parallel payment systems.

The process of granting letter of credits and loans to small and medium enterprises (SMEs) and to individuals has usually been challenging due to a lack of customer information and has needed much effort leading not only to more difficulties for the banks and their expansion plans, but also to troubles for the SMEs and individuals themselves in getting their loan applications granted by banks.

All these problems can be addressed with Blockchain technology. Instead of participants keeping their own ledgers and records, blockchain lets participants share a ledger through a peer-to-peer system, thus reducing the need for intermediaries. This leads to a more economical and efficient way of conducting transactions. The need for intermediaries is further reduced by using automated smart contracts. The blockchain system is also less vulnerable to fraud and cyberattacks because it uses a consensus model to validate each transaction.

There are some challenges with blockchain, however. Werbach (2018) states that Blockchain technology is vulnerable. Because of the nature of distributed ledger technology, a critical vulnerability lies outside the blockchain in the endpoints where blockchain-based platforms are accessed. Blockchain technology uses asymmetric encryption, which requires the use of a private- and public key in order to get access to the transaction conducted on the blockchain. If the private key is obtained by a hacker, the hacker could get access to the network. Moreover, vulnerabilities may exist in smart contracts; for example, in 2016, a smart contract called DAO was attacked and exploited, resulting in financial losses of about 60 million dollars.

IV. ACTIVITY DIAGRAM



V. RESULT

Blockchain and distributed ledgers have a bright future. As real-time, open-source and trusted platforms that securely transmit data and value, they can help banks not only reduce the cost of processing payments, but also create new products and services that can generate important new revenue streams. Solidity: Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably, Ethereum. It was developed by Gavin Wood, Christian Reitwiessner, Alex Beregszaszi, Liana Husikyan, Yoichi Hirai and several former Ethereum core contributors to enable writing smart contracts on blockchain platforms such as Ethereum. Solidity is a statically-typed programming language designed for developing smart contracts that run on the

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12608

EVM. Solidity is compiled to bytecode that is executable on the EVM. With Solidity, developers are able to write applications that implement self-enforcing business logic embodied in smart contracts, leaving a non-repudiable and authoritative record of transactions. Writing smart contracts in smart contract specific languages such as Solidity is referred to as easy (ostensibly for those who already have programming skills). As specified by Wood it is designed around the ECMAScript syntax to make it familiar for existing web developers; [citation needed] unlike ECMAScript it has static typing and variadic return types. Compared to other EVM-targeting languages of the time such as Serpent and Mutan, Solidity contained a number of important differences. Complex member variables for contracts including arbitrarily hierarchical mappings and structs were supported. Contracts support inheritance, including multiple inheritance with C3 linearization. An application binary interface (ABI) facilitating multiple type-safe functions within a single contract was also introduced (and later supported by Serpent). A documentation system for specifying a user-centric description of the ramifications of a method-call was also included in the proposal, known as "Natural Language Specification."

Web3.js Api: Web3.js is a collection of inbuilt libraries that help to communicate with local or remote ethereum nodes by using HTTP or Interprocess communication (IPC).Web3 is designed to work from both client and server side. We can consider a web3.js as a gateway between Ethereum blockchain and a smart contract. This can be considered as the most advanced js library available.In blockchain, especially the ethereum is made of nodes that share the same copy of data. By setting a web3 provider in a web3.js will helps the code to understand which node we are going to handle our functions. We can host our own node as a provider. Mostly we use some third-party services that help to maintain nodes in order to provide Dapp services. Some of the main providers include- Infura, MetaMask. Infura is a way to access the ethereum node over Jason-RPC which we can access through their API.With infura we can maintain our ethereum blockchain without setting up and maintaining our own nodes. MetaMask is a web browser add-on which acts as a bridge between and helps to run the Ethereum DApps without running the Ethereum full node. Metamask allows you to manage your Ethereum accounts and private keys, and use these accounts to interact with contracts that are using Web3.js. Metamask uses the infura.io servers as the web3 provider, other than that it also gives their users to choose their own web3 provider.

Truffle framework: Truffle is a development environment, a testing framework and a crypto asset pipeline in one for development in Solidity programming language. [1] The framework can build Distributed Apps (DApps), compile Smart Contracts, deploy Smart Contracts, and inject Smart contracts and DApps into a web app, and can create frontend for DApps and test them. Truffle framework has three main components named Truffle, Ganache, and Drizzle. Truffle Suite is a development environment based on Ethereum Blockchain, used to develop DApps (Distributed Applications). Truffle is a one-stop solution for building DApps: Compiling Contracts, Deploying Contracts, Injecting it into a web app, Creating front-end for DApps and Testing.

Interactive Objects: The interactive objects explorer provides the user with the various interactive objects to interact with and consume knowledge through the touch based interaction. This is implemented using the FLASH HTML support for mobile devices. The framework app lists the HTML interactive files stored on the SD card. The user can then select between those for learning. When a selection is made the HTML code triggers the respective SWF file and the interactive object is displayed. User can then interact using the touch and gain knowledge

VI. BLOCKCHAIN APPLICATIONS IN BANKING SECTOR

Central Bank Digital Currency (CBDC)

Dashkevich et al. (2020) defines a central bank or “monetary authority” as a “financial institution that manages domestic money supply, interest rates and oversees a country’s broader banking system”. A central bank digital currency (CBDC) “at the most basic level, is simply monetary value stored electronically (digitally, or as an electronic token) that represents a liability of the central bank and can be used to make payments” (Engert & Fung, 2017). According to Daskevich et al. (2020), Blockchain technology can be used as an underlying technology for enabling CBDC and states that “CBDC promises to provide central banks with a reliable close to real-time ‘window’ on economic activity to guide monetary policy”, but adds that 10 there is uncertainty whether potential risks could emerge, e.g. immature blockchain technology or a lack of research in the area. Arner et al. (2020) explains that CBDC can be configured using three types of different underlying architectures: The first type is a centralized system which uses a permissioned blockchain and accounts by which participants have direct access to a central bank, but this CBDC could not have cash-like features like anonymous exchange. The second type of architecture is based on a permissionless blockchain where full decentralization is achievable through tokenization and could offer cash-like features. The third type is a hybrid that is a mix of a centralized and decentralized CBDC. It may provide central bank accounts for financial intermediaries, where other participants could use intermediary services to access CBDC-tokens; these tokens could indicate who has the right to the funds stored in the central bank accounts.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12608

Central Bank Payments Clearing and Settlement (PCS)

Dashkevich et al. (2020) states that an important application of blockchain technology for central banks is to improve the clearing and settlement of payments between all banks. All the banks are participants in DLT-based PCS and reach a consensus between each other without the need for an intermediary link to control the transaction. This can help in reducing the time needed to complete the settlement process to be almost instantaneous. Another advantage is the flexibility to decide how long the transaction should take depending on an agreement between the involved parties. Liquidity will be available to the receiving bank faster and will not be stuck in between the parties, which leads to more effective use of the money.

Anti Money Laundering activity

Know-your-customer (KYC) is a principle for combating money laundering. The principle works by verifying a customer's identity and reviewing the behaviours of that customer in order to assess if that customer could potentially commit money laundering. The current KYC-process employed by banks takes between 30 - 50 days to reach an acceptable level. Moreover, for a person who is a customer of several banks, each bank conducts their own KYC-process for that customer, leading to several versions of a person's KYC-data. (Wang et al., 2020) 11 Wang et al. (2020) and Moyano & Ross (2017) claim that Blockchain technology can be used for KYC purposes. Due to the secure nature of Distributed Ledger Technology, banks' customers data can be shared with other banks and other organizations, eliminating the need for these organizations to restart the whole KYC-process. Moyano and Ross (2017) propose a solution with three possible configurations: (1) a centralized solution with a private blockchain and a regulator, (2) a fully decentralized solution which utilizes the permissionless platform, and (3) a hybrid solution where the KYC-data is stored in smart contracts, and where the customer has control over which financial institutions have access to his/her data.

Cross-border payments

Li et al. (2020) describe that another use of a blockchain platform in the banking industry can be for cross-border payment systems. As mentioned in the problem description, the traditional cross-border payment has a lot of deficiencies in which it can be time-consuming with high cost operations and low security. Using blockchain technology will contribute to developing a new solid and real-time cross-border system by which the banks could solve the problems in this aspect. OKLink is an example of a cross-border network built on blockchain technology.

Digital Asset Register and Management

Blockchain systems can be used to build a digital asset register and management which can manage all operations that concern asset ownership (e.g. home, bonds, mortgages, and insurance) and aims at protecting the integrity and convenience of sensitive documents and records (e.g. contracts, records, registrations etc.) (Li et al., 2020).

VII. CONCLUSION

We have included that Information technology has become a critical innovation in almost every industry. Those institutions or teams that can use technology correctly and effectively play a major role in disrupting the status in a leadership position. Those that don't keep up with technology generally do not survive. We think the Blockchain technology as a catalyst for emerging use cases in the financial and non-financial industries such as industrial manufacturing, supply chain, and banking. Blockchain can play a pivotal role in transforming the digitization of industries and applications by enabling secure trust frameworks, creating agile value chain production, and tighter integration with technologies such as cloud computing, and IoT. In producing a cloud-based application called banking, the researchers have demonstrated the capability to apply professional engineering principles, combined with a DevOps approach to iterative development and management, and integration of cyber security distributed computing, and Block-chain technologies. We feel banking is one of many examples that demonstrate the trans-formative capability of Blockchain.

VIII. THE FUTURE OF BLOCKCHAIN TECHNOLOGY IN BANKING SECTOR

We will see greater adoption of blockchain in several aspects of banking services. SBA mentions that VISA and MasterCard are currently investing in blockchain products. He goes on and highlights the e-Krona project that the Swedish central bank is working on. When it comes to the permissionless aspect of blockchain, there is a lot of innovation happening all the time and mentions the third generation of blockchain platforms like EOS and TRON that are looking into solutions on how to upgrade smart contract functionalities.

There is enormous innovation potential with decentralized finance and crypto, and that there is a possibility that they could overtake the whole financial market. He believes that there is not really anything that speaks against decentralized finance being the new standard when it comes to financial instruments and products, and that these products will be more widely available, maybe even free. However, as previously mentioned.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12608

It difficult to provide a specific definition of blockchain and explains that when it comes to Bitcoin, then one can say that it really has a chain of blocks and he claims that there are two types of chains: blockchain and transaction chain. So the original definition of blockchain is "All information is distributed over all nodes and every one has access to everything and everyone also can create a node". On the other hand,the name blockchain is being used even though the implementation is very different.

We will see greater adoption of blockchain in several aspects of banking services. SBA mentions that VISA and MasterCard are currently investing in blockchain products. He goes on and highlights the e-Krona project that the Swedish central bank is working on. When it comes to the permissionless aspect of blockchain, there is a lot of innovation happening all the time and mentions the third generation of blockchain platforms like EOS and TRON that are looking into solutions on how to upgrade smart contract functionalities.

There is enormous innovation potential with decentralized finance and crypto, and that there is a possibility that they could overtake the whole financial market. He believes that there is not really anything that speaks against decentralized finance being the new standard when it comes to financial instruments and products, and that these products will be more widely available, maybe even free. However, as previously mentioned.

It difficult to provide a specific definition of blockchain and explains that when it comes to Bitcoin, then one can say that it really has a chain of blocks and he claims that there are two types of chains: blockchain and transaction chain. So the original definition of blockchain is "All information is distributed over all nodes and every one has access to everything and everyone also can create a node". On the other hand,the name blockchain is being used even though the implementation is very different.

REFERENCES

[1] Adams, J., Khan, H.T.A. and Raeside, R. (2014). Research methods for business and social science students. Los Angeles: Sage.
[2] Al Shorman, Areej, et al. (2020). "Blockchain for Banking System: Opportunities and Challenges." Journal of Theoretical and Applied Information Technology, vol. 98, no. 23, Dec. 2020.
[3] Ali, O., Ally, M., Clutterbuck and Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. International Journal of Information Management, 54, p.102199.
[4] Arner, D.W., Buckley, R.P., Zetzsche, D.A. and Didenko, A. (2020). After Libra, Digital Yuan and COVID-19: Central Bank Digital Currencies and the New World of Money and Payment Systems. SSRN Electronic Journal.
[5] Chang, Victor, et al. (2020). "How Blockchain Can Impact Financial Services – the Overview, Challenges and Recommendations from Expert Interviewees." Technological Forecasting and Social Change, vol. 158, Sept. 2020, p. 120166, 10.1016/j.techfore.2020.120166.
[6] Dashkevich, Natalia, et al. (2020). "Blockchain Application for Central Banks: A Systematic Mapping Study." IEEE Access, vol. 8, 27 July 2020, pp. 139918–139952, 10.1109/access.2020.3012295.
[7] Drescher, D. (2017). Blockchain basics : a non-technical introduction in 25 steps. New York: Apress.
[8] Engert, W. and S. C. Fung, B. (2017). Central Bank Digital Currency: Motivations and Implications.
[9] Garg, P., Gupta, B., Chauhan, A.K., Sivarajah, U., Gupta, S. and Modgil, S. (2020). Measuring the perceived benefits of implementing blockchain technology in the banking sector. Technological Forecasting and Social Change, 163, 37
[10] Goldkuhl, G. (2011). Kunskapande, Institutionen för ekonomisk och industriell utveckling, Linköpings universitet
[11] Guo, Y. and Liang, C. (2016). Blockchain application and outlook in the banking industry. Financial Innovation, 2(1).
[12] Hassani, H., Huang, X. and Silva, E. (2018). Banking with blockchain-ed big data. Journal of Management Analytics, 5(4), pp.256–275.
[13] IBM (n.d.). we.trade. [online] www.ibm.com. Available at: https://www.ibm.com/case-studies/wetrade-blockchain-fintech-trade-finance [Accessed 3 Feb. 2021].