INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

A Conceptual Study of Blockchain to Financial Sector

T. KohilaKanagalakshmi[1], Lavita [2], Shweta Biradar[3]
[1]Assistant Professor, Dayananda Sagar Institutions, Bangalore.
[2,3] Student, MCA, Dayananda Sagar Institutions, Bangalore.
Kohilakanagalakshmi.t@gmail.com[1], lavilavita98@gmail.com[2], shwetabiradar9679@gmail.com[3]

Abstract

A Blockchain technology is the basis of Bitcoin which has acknowledged widespread attentions recently. It is also known as distributed, indisputable and digital ledger which registers the transactions in the same order it is generated in a close real-time. In blockchain, transactions take place in a decentralized manner. The subsequent transactions can be included to the ledger only by the agreement of the participants in the network which is known as nodes The subsequent transactions can be added to the ledger only by the agreement of the participants in the network which is known as nodes. The applications of blockchain extending from banking, crypto currency and financial services, risk managements, social services and Internet of things. This paper explains a broad impression of blockchain technology in banking applications and recent advances.

Keywords: Blockchain, Consensus, Distributed ledger, DApps, Smart Contract, Financial sector

1. Introduction

Blockchain is a decentralized peer-to-peer system. It can perform the transactions with no reliable third parties in between. The transactions are added to the ledger databases after verification and acceptance of all the participating nodes. These transactions are non-editable that is, new transactions can be added to the nodes and existing data cannot be deleted. As per Webopedia "blockchain is a type of data structure that enables identifying and tracking transactions digitally and sharing this information across a distributed network of computers, creating in a sense a distributed trust network. The distributed ledger is offered by blockchain which provides a transparent and secure means for tracking the ownership and transfer of assets".[1-5]. The evolution of blockchain technology varies different versions. Blockchain 1.0: Currency - Crypto currencies allows financial transactions based on blockchain technology with bitcoin, "Digital Currency". Blockchain 2.0: Smart Contracts – These are the scripts executed in blockchain environment. The verification is carried out by customers in the blockchain environment. This ensures honest execution of the "contract." Blockchain 3.0: decentralised applications (DApps.) whose backend is placed on blockchain and storage of data in distributed ledger and can have front end stored on decentralized storages such as Ethereum's Swarm. Blockchain 4.0: based on automation of business scenarios in real time. Some or the examples include ERP, Supply chain management, financial transactions, banking, condition-based payments, IoT and asset management, etc.[6-9]

The remainder of the paper is as follows. Section II explains steps involved in blockchain process. Section III identifies consensus mechanism. Section IV introduces smart contract and Section V describes applications of blockchain technology in banking applications. Section VI highlights the issues in blockchain technology. Lastly Section VII concludes the paper.

2. Blochain Process

In its most simplify form, the blockchain communication go through the following steps to get into the blockchain:

1.All the nodes in the system receive the connections and it is tested for accept or reject the transactions.

2.To avoid double spending of the transaction, it is broadcast to all the nodes in the system and the genuineness of the transactions are verified.

3.Even the nodes may cluster several transactions into blocks to share with other nodes in the system. The formation of new blocks will be controlled by consensus.

4.Once the nodes accept the block it will be added to the blockchain network with the help of its hash value.

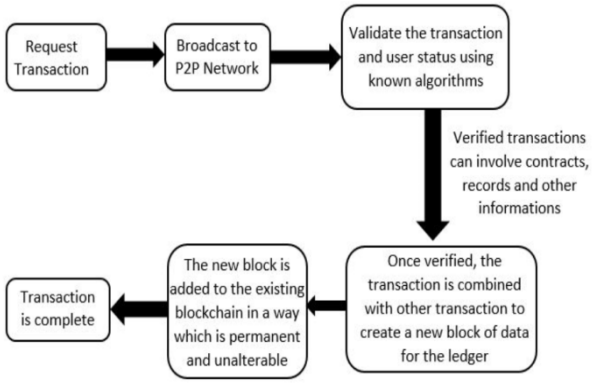

Fig.1. Steps involved in Blockchain Transactions

3. Consensus Mechanism

Blockchains create direct network which can self-correct in absence of a third party to enforce the rules. Data stored on the network as a whole, by definition it is public and data once stored are transparent and cannot be modified by changing any information on the blockchain. This is accomplished by the enforcement of rules through their consensus algorithm. The malfunctions are avoided in the blockchain with the help of consensus mechanism. The validity of the transactions is decided by the consensus algorithm and forking problem is removed in blockchain. When miners parallelly mines a block of transaction then forking problem arise and is avoided by adding a new fork in the linear form of blockchain using consensus mechanism. The longest chain rule concept is used to resolve the forking problem.

3.1. Proof of Work (PoW):

Proof of effort is a blockchain consensus algorithm, applied by Satoshi Nakamoto in 2009. It was firstly used by Bitcoin then later adopted by Ethereum. To add any new blocks into the blockchain, an algorithm is required. The main goal of Proof of work protocol is preventing cyber-attacks such as a distributed denial-of-service attack (DDoS) by which transferring numerous forged requests will be send to the CPU with the determination of draining the resources. In POW, individual nodes of the network need to compute a hash value for the continuously varying block header. The consensus needs that the computed value should less than or equal to some given value. All the nodes in the decentralized network, needs to calculate the hash value uninterruptedly by means of diverse nonces until the goal is reached. When one node finds the appropriate value, all other nodes must jointly confirm the precision of the value. Based on this mining procedure a new block will be created in the blockchain for all the transactions which are used to find the authenticity. The nodes which compute the hashes is known as miners and the miner who resolves the problem first gets a reward. The party with the most power usually mines the block and others just gets their energy wasted because multiple miners compete to create a block at one instance. [10-14]

3.2. Proof of Stake (PoS)

Blocks can also be produced in a blockchain using PoS. The block producers are named as Validator rather than miners. Validators take their chance on the basis of some choice algorithm. The choice is based on account balance, the richest person may guarantee to be leading in the network. As a result, many solutions are projected with the mixture of the chance size to choose which one to form the next block.. In turn, the least hash value along with the size of the stake is used to compute the next generator. Only selected validator can build a block and others cannot play a part, hence saving the energy of the other validators. The validators can get remuneration for honesty and loses their chance if it does mistake. The miners get

their transaction price since they do not get remuneration unlike PoW. [15-19]

3.3. Delegated proof of stake (DPoS)

In DPoS, block producer are nominated by votes by the one who has network tokens. Block producer candidates that receive the most votes are the one who can produce blocks. Users can also give their voting power to another user who can vote on their behalf. In DPoS is based on open-source protocols meaning that if the users disagree with the majority they can fork. Block producers can be voted in or out at any time, so the risk of loss of income and status is one of the major encouragements in difference to bad behaviour.

3.4 Practical byzantine fault tolerance (PBFT)

In PBFT, a new block is resolute in a round where in each round, the most important will be selected according to some rules. PBFT needs that every single node is known to the system. PBFT consensus method does not need any hashing algorithm to agree interactions in a blockchain, which suggests there is no obligation for high energy consumption and the risk of centralization is lesser than in equally of blockchain mechanisms. PBFT is currently being used by the Hyperledger venture, which allows developers to construct their own particular digital resources on a disseminated ledger.

3.5. Tendermint

Tendermint is used by the developers for securely and consistently replicate the applications written in whatever programming language and advance setting is right for them. By strongly, we mean that Tendermint works even if up to 1/3 of equipment fail in accidentally and every non-faulty machine realizes the identical transaction log and calculates the same state. Tendermint consists of two chief procedural workings: a blockchain consensus engine and a generic purpose edge. The consensus engine, named Tendermint Core, authorizes that the same business are documented on every machine in chronological order. The application interface, otherwise known as the Application BlockChain Interface (ABCI), allows the transactions to be managed in any programming language.

4. Smart Contract

A smart contract is a computer code running on top of a blockchain comprising a set of rules under which the parties approve to cooperate with each other. It is a decentralized automation relating two or more parties and digital assets, where assets are deposited by the parties into the smart contract and the resources automatically get reallocated with the parties based on a formula and based on certain data, which is not identified at the time of contract initiation. It enables safety and permits no third party to intervene to avoid fraud or criminal acts. All transactions performed in smart contracts are permanent and trackable. A smart contract describes penalties and rules and also imposes the responsibilities in the agreement automatically.

4.1 Ethereum's

Ethereum is an open-sourced immutable blockchain-based platform that permits smart-contracts and has a Turing-complete programming language for launching distributed applications. It can run all blockchains and protocols. All the nodes in the Ethereum network runs the Ethereum VM for smart contract execution in a distributed execution. Ethereum is an efficient protocol for application development to design smart contracts. The distributed ecosystem of Ethereum, includes components like "Ethereum-Swarm" - a decentralized file-serving method, "Ethereum-Whisper" - a P2P procedures and syntax for cryptographic messaging system to diminish risk between agents in trustless networks.

4.2 DApps

DApps stands for decentralized applications that cannot execute on a centralized machine. Dapp runs on a distributed network nodes It protects participant information. Smart contracts allow DApps to connect to blockchain technology for conducting pre-programmed operations. A smart contract or DApp is well-defined in a Ethereum as a transaction protocol to accomplish group of contracts on a cryptographic blockchain. Examples of DApps are OpenBazzar, LaZooz, Twister, Gems etc.,

4.3 DAOs and DACs

Decentralized autonomous organizations / corporations are more complex form of a decentralized application. They are notions derived from AI. In a DAO/DAC, smart contracts are

running on blockchains that perform ranges of predefined tasks based on conditions. and changing events. Smart contracts operating on the blockchain can perform the functions of real world as well as can instantiate the model to an autonomous corporation.

5. Blockchain Technology In Banking

Blockchain is a dispersed ledger of transactions, a multi-tiered technology that potentially organize the behavior of customers and their assets based on a mode of transaction ledgers. Registering the electronic transactions in a global insurance blockchain makes transaction scam not possible. Authentication of the transaction accuracy is instant and can be performed by anyone at anywhere. The blockchain may moderate the processing costs appreciably by storing the information in blocks. All major banks can exercise blockchain which could be used for transfer the money, maintain the records and additional back-end tasks. The function of blockchain can replace the paper-based global trade business procedure to an electronic decentralized ledger that offers all the participating entity, including banks, the competence to access a single source of information. It also permits them to pursue all documentation and authorizes ownership of assets digitally, as an irreversible ledger in real time.

5.1. Crowd funding

It is a method of raising the capital for a big project such as scientific projects, space research etc., from large amount of people where each one can contribute a small amount of data. In a traditional approach the amount donated by the crowd will be collected by a single organisation where malpractices, fraud, information asymmetry may arise during the fund raising activities. Blockchain is an emerging technology where companies can make and verify financial transactions on a network directly without a central authority. Each transaction made in the blockchain needs to be approved and preserved in the ledger maintained by all the nodes.

5.2 KYC (Know Your Customer):

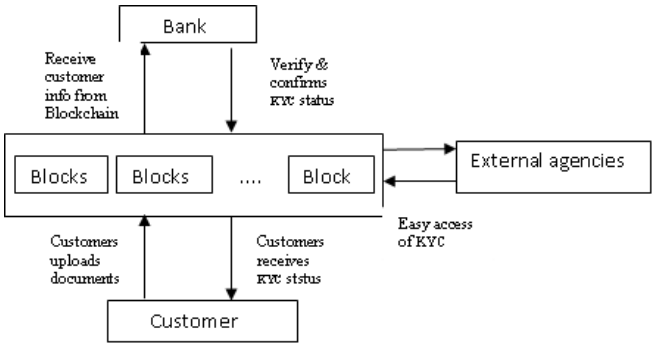

Fig.2. KYC Verification in Blockchain

KYC is a major aspect in the battle against financial scam and money laundering. KYC check is the compulsory process of identifying and verifying the individuality of the client when opening an account. KYC procedure comprise ID card authentication, face authentication, document proof such as utility bills such as address proof, and biometric verification. However, in traditional approach KYC is a repetitive process done by individual organization and stored in their database.

5.3 Trading Platform

The blockchain skill offers a possible new intermediate to exchange assets with no centralized trusts or mediators and without the risk of spending twice the cost. Blockchain can reduce the risk or the threat of fraud in all areas of banking, and this could equally apply to a trading platform. For each high value property a digital token will be issued to the owner, stating the "certificate of authenticity". The token will be moved every time the product is sold or brought and the new ownership will be created and stored in the blockchain. The advantage of the digital token is the final recipient or the current owner of the product can be verified from the chain of protection to all the way back to point of creation. By this way bank can use blockchain as a secured trading platform.

5.4 Payment process

Electronic payment is the fast and easy way to perform the transactions. But in today's payment processing service the "beneficial ownership" rules makes the transaction time much higher. Ripple is a "real-time gross settlement system" (RTGS), money exchange and allowance network with no chargeback. However it is a proprietary blockchain system and did not connect with other system. It is

much better to have a global blockchain system to connect varies organizations throughout the world so that transactions can be performed very easily without fraud.

5.5 Fraud Detection

Most banking systems in the world, built on a centralized record are more at risk to cyber attack. Blockchain is being accepted as the circulated technology that would reduce fraud. In traditional banking environment is based on paper transaction and electronic payments such as Paytm, Google pay, PayU, etc., and the malfunctions in these transactions can be intentional or unintentional. Private and immutable ledger that enables transactions between the cross banks in a transparent and secure manner.

6. Issues in Blockchain Technology

- **Scalability**

Blockchains are having trouble in effect with supporting a large number of users on the network. Scaling methods have to be verified before implementation into the ledgers.

- **Privacy**

The Bitcoin blockchain is considered to be freely visible. All the information pertaining to a transaction is available for anyone to view. For example, private patient data, government data or financial data should not be available for all as is the case with proprietary industry data.

- **Costs**

Blockchain is an effective tool for reducing costs. It reduces the fees related with transferring the value and can update operational processes. However, because it is a relatively new innovation, it is difficult to combine it with legacy systems. Such a process is likely to be an expensive issue that many corporations and governments will be unwilling to undertake.

7. Future Enhancement and Conclusion

Blockchain has likely for transforming traditional business with its key characteristics: decentralization, persistency, ambiguity and auditability. Blockchain refers to a tamper-proof circulated ledger which solves the problems in centralized model. However efforts spent for integration of blockchain to business processes are still at infantacy. Sharding, Editable-blockchain, IoT-specific consensus are some of the key area needs future enhancement. Blockchain can well be combined with Bigdata technology where data management can be handled in a circulated environment and transactions on blockchain can be used for analytics to obtain model. Now a days blockchain based applications are emerging rapidly and we plan to conduct in-depth investigations in banking applications.

References

Journals

[1] Vida J. Morkunas, et. al., “How blockchain technologies impact your industry model,” Paper of trade Information incorporation, vol.13. pp. 32-39, 2019.

[2] I. Ahmed, Shilpi, and M. Amjad, “Blockchain Technology A Literature Survey,” Oct 2018 Volume: 05 Issue: 10 International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056

Book

[3] wan,Blockchain: Design for a innovative Economy (2015), OReilly, First Edition.

[4] Blockchain For Dummies® Published by: John Wiley & Sons, Inc., River Street, Hoboken, NJ 07030-5774, www.wiley.com Copyright © 2017 by John Wiley & Sons, Inc., Hoboken, New Jersey.

[5] Bikramaditya Singhal, "Beginning Blockchain - A Beginner’s Guide to Building Blockchain Solutions", ISBN-13 (electronic): 978-1-4842-3444-0 https://doi.org/10.1007/978-1-4842-3444-0 Retrieved Mar 15, 2019

Conference Proceedings

[6] A. Stanciu, Blockchain based circulated manage system for Edge Computing, in: 21st International Conference on Control Systems and Computer Science Blockchain, 2017, pp. 667–671.

[7] Zibin Zheng, et. al. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", available

athttps://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends. Retrieved Mar 15, 2019

[8] F. Stroud, Blockchain, [Online]. Available:https://www.webopedia.com/TERM/B/blockchain.html. Accessed 15 October 2019.

[9] Blockchain discussion group for Beginners: Learn Blockchain Technology, https://www.guru99.com/blockchain-tutorial.html

[10] Blockchain Challenges and Opportunities: A Survey Zibin Zheng https://pdfs.semanticscholar.org/305e/dd92f237f8e0c583a809504dcec7e204d632.pdf

[11] Famous Blockchain Consensus Mechanisms and their Benefits, https://www.newgenapps.com/blog/8-blockchain-consensus-mechanisms-and-benefits Retrieved Mar 15, 2019

[12] Delegated Proof of Stake:Features & Tradeoffs https://multicoin.capital/wp-content/uploads/2018/03/DPoS_-Features-and-Tradeoffs.pdf Retrieved Mar 15, 2019

[13] what is Tendermint available at : https://tendermint.com/docs/introduction/introduction.html Retrieved Mar 15, 2019

[14] Smart Contracts - https://blockchainhub.net/smart-contracts/ Retrieved Mar 15, 2019

[15] What Are Smart Contracts And dApps—A Beginners Guide https://blog.coinswitch.co/what-are-smart-contracts-and-dapps-a-beginners-guide-b369d44ec4a5 Retrieved Mar 15, 2019

[16] Blockchain IoT use cases - https://www.leewayhertz.com/blockchain-iot-use-cases-real-world-products/ Retrieved Mar 15, 2019

[17] Using Blockchain to Enable Supply Chain Transparency https://www.iotforall.com/blockchain-supply-chain-transparency/ Retrieved Mar 15, 2019

[18] Blockchain Technology in Banking & Finance https://www.nelito.com/blog/blockchain-technology-in-banking-and-finance.html Retrieved Mar 15, 2019

[19] Blockchain technology as a platform for digitization Implications for the insurance industry available at: https://www.ey.com/Publication/vwLUAssets/EY-blockchain-technology-as-a-platform-for-digitization/%24FILE/EY-blockchain-technology-as-a-platform-for-digitization.pdf Retrieved Mar 15, 2019