BLOCKCHAIN TECHNOLOGY

[1]NISHANT PAREKH
IV year, B.E. Department of CSE BMS College of Engineering

[2]PRADEEP SADANAND
Assistant Professor, Department of CSE BMS College of Engineering

[3]SANYAM JAIN
IV year, B.E. , Department of CSE BMS College of Engineering

ABSTRACT: A blockchain is an electronic ledger of digital records, events, or transactions that are cryptographically hashed, authenticated, and maintained through a "distributed" or "shared network of participants using a group consensus protocol, following the most disruptive aspect of eliminating the need for third-party intermediaries in transactions.

---

1. INTRODUCTION

This is a literature review of the current landscape in the field of BlockChain technology and analyse prior literature. By understanding the concepts and going deeper into the use of blockchain as a technical platform for future applications and software, thus providing platform which provides capability of four basic functions: *financial system, registry structure, smart contract and "smart laws".* Eliminates the need for multiple intermediaries, regulatory authorities, and document circulation. It's aim is to take decentralization even further, by adding every civil, economical and financial service onto the BlockChain.

2. DEFINITIONS

2.1 BLOCKCHAIN

The Blockchain technology is defined as "[…] the technology underlying bitcoin and other cryptocurrencies—is a shared digital ledger, or a continually updated list of all transactions". This definition agrees with the one used throughout the paper and is thus to be taken into consideration as the general consensus that is used in this paper.

2.2 PLATFORMS

For platforms, this paper uses the definition presented by Techopedia that defines a platform as "[…] a group of technologies that are used as a base upon which other applications, processes or technologies are developed.".

3. TRADITIONAL SYSTEM:

Talking about transaction then the existing system is centralized, slow, inefficient, unreliable, more costly and talking about money it doesn't work well for cross border payments. Government can manipulate and print the currency. The value of the currency doesn't remains the same throughout the globe hence isn't providing a constant market approach.

Also in the approach of traditional government system, traditional physical contracts, such as those created by legal professionals today, contain legal language on a vast amount of printed documents and heavily rely on third parties for enforcement. This type of enforcement not only consumes a lot of time, but also turns out to be very ambiguous. If things go astray, contract parties that are participating often must rely on the present public judicial system to correct the situation,that turns out to be very costly and also consumes a lot of time.

4. GARTNER HYPE CYCLE:

Garter's Information Technology Hype Cycle is a way to represent emergence, adoption, maturity and impact on applications of specific technologies. In the graph,the X- axis denotes expectations and Y- axis denotes time factors. BlockChain technologies that are currently at rank 6 and has been identified as one of the upcoming technologies as noted in Gartner's IT Hype Cycle. The graph and the research depicts that it will take around 6-10 years for market to adopt.

5. BACKGROUND

Following the theoretical introduction, this paper aims to further explain on the theoretical ground in order to provide a brief summary of research done earlier and additionally to highlight areas of work where potential lies.

A literature review can be described as a summary of summaries that allows identification of research areas within a given subject field within the field of research, a literature review is concept-centric and determine the further framework of the review.

Boundaries of a paper are important along with the scope. Economic and other use cases of the technology (e.g. Bitcoin) are focused and reviewed solely on the technology behind, the Blockchain.

5.1 TECHNOLOGICAL BACKGROUND

Blockchain, a decentralized node structure, where each node contains the copy of all the distributed nodes and if in case of changes in data contained by the node takes place it affects to all the nodes in the chain. The most favourite domain of BlockChain, Bitcoin (where most of the research is working around) has demonstrated in the financial space that trusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger, a decentralized personal data management system that ensures users own and control their data.

Taking the case of Bitcoin ,an order of transaction is maintained by a lottery system over a math problem that, which transaction is to be processed next in the chain. After the changes are done at a node then the transactions are broadcast to the network using software applications such as Gossip algorithms.[5] The gossip protocol enables communication between nodes. Its basic flow control is taken care by UDP along with this there is a protocol level connection management. A Token Bucket method of implementation is used to put a limit on the average message

transmission rate. A Token Bucket implementation is used to limit the average rate of message transmission. Peers in the gossip network are called Nodes. Nodes exchange Messages. Message handling upon arrival is dispatched via Event Handlers associated with the journal. There are different type of algorithms used such as teknek-gossip(UDP, java) and gossip-python(TCP).[5]

The transactions are validated by the mining nodes, time stamping schemes are also used along with Proof-of-Work[9], which is a consensus protocol used to serialize changes, combining established primitives for managing ownership through public key cryptography with a consensus algorithm for keeping track of who owns , known as "proof of work."

In the case of bitcoin where a newly generated block is created at the time of transactions, miners make their calculations to turn the transactions message into something far shorter, in which a random sequence of letters and numbers that is called as Digest. Presently there are lot of crypto currencies popular in the market which uses different cryptographic hash generation algorithms such as Bitcoin uses SHA256 [10], Litecoin uses Scrypt, Peer coin uses pow/pos and Quark uses M7.

Different digital signature schemes are used some are namely RSA, DSA, ECDSA. [9]

The block interval defines the latency at which it is written to the blockchain. The smaller the block interval is, the faster a transaction is confirmed and the higher is the probability of stale blocks(Waste Blocks). The block interval adjustment directly relates to the difficulty change of the underlying PoW mechanism. [3]

5.2 TECHNOLOGICAL FEATURES

5.2.1 SECURITY

Evaluating the soundness of BlockChain technology is akin to evaluating the efficacy of a lock. Just as the security lock is taken into consideration , if everyone in the town has a copy of the key, the safety of the BlockChain is heavily dependent on its current working protocols– how it verifies transactions between parties, what encryption algorithms is it using in the Blockchain, and more.

The recent increase in reported incidents of surveillance and security breaches compromising user's privacy call into question the current model, in which third-parties collect and control massive amounts of personal data .[2]

5.2.2 INTEGRITY

But integrity which is the main concern of the chain is maintained and hence if any change happens at any block and hash is changed inside the block then any block getting added up later into the chain will be out of the whack. Thus miners play a very important role in keeping the chain intact and preventing the data getting compromised. [11]

A lower difficulty results in a larger number of blocks in the network, while a higher difficulty results in less blocks within the same timeframe.

Blockchain Technology has also some technical challenges and limitations that have been identified: Throughput (Transactions per seconds), Latency, Size and Bandwidth, 51% attacks, Wasted resources, Usability, Versioning, Multiple chains. [8]

5.2.3 PERFORMANCE

This is an important feature to overpower the existing systems and upgrade the functionalities of BlockChain technologies. But The performance of PoW based blockchains cannot be enhanced without affecting its security. The framework that is used in the paper [13] , here the framework has two main key elements, a blockchain instance and a blockchain security model.

6. APPLICATIONS

In this digital world where everything is getting on the go, but still there are some problems which are yet to be solved i.e speed, efficiency, security, integrity and third party involvement.Blockchain technology still being in it's infancy is incapable to provide solutions to all the problems of the world , but it can provide solutions for most of them. Some applications where this technology can be used are Finance , Health, Logistics, Real Estate, FIR/Law and more.

6.1 BANKING SECTOR

In a Blockchain, participants share a system of record, everybody participating is permitted to see the complete transaction lifecycle and everybody's involvement.

Indeed, blockchain represents a powerful technological tool along with the existing technologies like databases, transaction processing systems, and enterprise messaging. People must believe in cryptography than the present system. Verifiability and certainty can be achieved with blockchain.

The blocking factors like regulation, legal constraints and even vested interests will almost certainly be resolved in time. Standards are to be set, just like internet . It also needs to have access rights. Blockchain proposition needs interoperability to function. Privacy is the main concern for transactions and identity, and it needs to be tuneable, so that counter parties can see only the transactions for which they are permissioned.[6]

6.2 HEALTH SECTOR

In the healthcare industry there are various possibilities i.e in health management, in the pharmaceutical sector, in medical research or in consumer-oriented healthcare. A decentralized database which is consistently held up to date presents many advantages to the health care industry.It become interesting when many different parties need access to the same information . Many of the parties involved (e.g., general practitioners,medical specialists, hospitals, etc.) and the media disruptions involved during the treatment of a patient can result in a time consuming and resource-intensive authentication and information processes for all medical stakeholders. Thus different healthcare specialists can access this shared network infrastructure .

Also provides the medical stakeholders to the latest treatment information. It permits medical experts involved to track the interactions between the patient and reports of all the check- ups done till date.It has also got uses in drug conflicting i.e whole top to down information of related to drug and where it came from.[1]

6.3 SMART CONTRACT

An important use of BlockChain is in smart contracts, these are the full-fledged programs working on BlockChain and has its execution governed and enforced by a consensus protocol. A smart contract is identified by an address, transactions are sent to this address to invoke the code.Sometimes A smart contract calls another contract by address to perform its main function. A contract behaviour can be changed by voting over working of the contract on a certain way by following the majority and calls the contract by the address stored in the mutable part of the database , a contract also has set of members, public key addresses which are used for voting to execute main function stored on a different contract.

6.4 IOT

A blockchain network of devices has a convenient *billing layer* and paves the way for a *marketplace of services between* all hardware sharing a copy ,which is charged at certainty to maintain the infrastructure cost . A Smart electronic lock-Slock that can be unlocked with a device that carries the appropriate token bought on the Ethereum blockchain.One of the application is if an owner of Slock that has got something to rent or sell sets a price and the later party identify the Slock and pay the amount in ethers to unlock it, billing can be maintained by having all Slocks operate on the same Blockchain.[12] Konstantinos and michael in their paper describes that IOT devices use BLE radio to do transaction whenever in proximity.

6.5 FRAUD MANAGEMENT

Chain is made to store risk intelligence the ledgers that trace and store information about the risk involved to reduce the fraud costs down the line. History of the supply chain is made to do the verification of the products and goods or fraud transaction, can even work on similar advanced elements such as digital rights management and proof of authenticity to counter fraud.[14]

7. CONCLUSIONS

This technology will definitely be a disruptor for many fields, as well as an enabler for technological ecosystems built on the blockchain technology. However, concluding that the technology in its current state still has some way to go before the technology will reach a state where it will be considered sufficient enough for solving major problems and adopted as mainstream .

8. REFERENCES

[1] Blockchain Technology in Healthcare The Revolution Starts Here Matthias Mettler M.A. HSG Boydak Strategy Consulting AG Freienbach, Switzerland mettler.matthias@bluewin.ch

[2] The Fintech 2.0 Paper:rebooting financial services

[3] Arthur Gervais, Ghassan O. Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, Srdjan Capkun : On the Security and Performance of Proof of Work Blockchains

[4] https://en.bitcoin.it/wiki/Weaknesses

[5] Stephen Boyd ,Arpita Ghosh, Balaji prabhakar, Devarat shah https://web.standard.edu/~boyd/papers/gossip_infocom.pdf

[6] https://www.finextra.com/finextra-downloads/surveys/documents/32e19ab4-2d9c-4862-8416-d3be94161c6d/banking%20on%20blockchain.pdf

[7] http://www.gartner.com/newsroom/id/3412017

[8] Jesse Yli-Huumo1, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander: RESEARCH ARTICLE Where Is Current Research on Blockchain Technology?

[9] https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-proof-of-work

[10] Florian Mendel, Norbert Pramstaller, Christian Rechberger and Vincent Rijmen Institute for Applied Information Processing and Communications (IAIK) Graz University of Technology, Austria: Analysis of Step-Reduced SHA-256www.iaik.tugraz.at/research/krypto

[11] www.blockchaintechnologies.com

[12] Blockchains and Smart Contracts for the Internet of Things KONSTANTINOS CHRISTIDIS, (Graduate Student Member, IEEE),AND MICHAEL DEVETSIKIOTIS, (Fellow, IEEE)Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606, USA

[13] On the Security and Performance of Proof of Work Blockchains ,Arthur Gervais ETH Zurich, Switzerland,Ghassan O. Karame NEC Laboratories, Europe , Karl Wüst ETH Zurich, Switzerland ,Vasileios Glykantzis ETH Zurich, Switzerland ,Hubert Ritzdorf ETH Zurich, Switzerland ,Srdjan C˘ apkun ETH Zurich, Switzerland

[14] Data Exchange Platform to fight Insurance Fraud on Blockchain Indranil Nath11Vice President, Insurance Industry Solution, IBM, United Kingdom indranil.nath@uk.ibm.com