Blockchain technology

Akshay Tank, Kaushal gor

Student, Teacher
Master of computer application,
Parul University, Vadodara, India.

Abstract: Blockchain is a decentralized transaction and data management technology developed first for Bit coin cryptocurrency. The interest in Blockchain technology has been increasing since the idea was coined in 2008.[1]

The reason for the interest in Blockchain is its central attributes that provide security, anonymity and data integrity without any third party organization in control of the transactions, and therefore it creates interesting research areas, especially from the perspective of technical challenges and limitations. In this research, we have conducted a systematic mapping study with the goal of collecting all relevant research on Blockchain technology. Our objective is to understand the current research topics, challenges. And future directions regarding Blockchain technology from the technical perspective.[1]

We have extracted 41 primary papers from scientific databases. The results show that focus in over 80% of the papers is on Bitcoin system and less than 20% deals with other Blockchain applications including e.g. smart contracts and licensing. The majority of research is focusing on revealing and improving limitations of Blockchain from privacy and security perspectives, but many of the proposed solutions lack concrete evaluation on their effectiveness. Many other Blockchain scalability related challenges including throughput and latency have been left unstudied. On the basis of this study, recommendations on future research directions are provided for researchers.[1]

1. INTRODUCTION

Blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can perform transactions without the need for a central certifying authority. Potential applications include fund transfers, settling trades, voting and many others.

Nowadays cryptocurrency has become a buzzword in both industry and academia. As one of the most successful cryptocurrency, Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016 with a specially designed data storage structure, transactions in Bitcoin .Network could happen without any third party and the core technology to build Bitcoin is blockchain, which was first proposed in 2008 and implemented in 2009. Blockchain could be regarded as a public ledger and all committed transactions are stored in a list of blocks. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency. The blockchain technology generally has key characteristics of Decentralization, persistency, anonymity and auditability. With these traits, blockchain can greatly save the cost and improve the efficiency.[1][2]

Since it allows payment to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment. Additionally it can also be applied into other fields including smart contracts, public services, Internet of Things (IoT), reputation systems and security services.

Blockchain technology has great potential for the construction of the future Internet systems; it is facing a number of technical challenges. Blockchain is distributed and can avoid the single

Point of failure situation. As for smart contracts, miners could execute the contract automatically once the contract has been deployed on the blockchain. Blockchain technology works on blocks.[2][7]

Blocks means larger storage space and slower propagation in the network. This will lead to

Centralization gradually as less users would like to maintain such a large blockchain.[7]

2. APPLICATION AREAS

A. SECURE SHARING OF MEDICAL DATA

big data blockchain contracts help patients and doctors securely transfer sensitive medical information. The smart contracts establish the parameters of what data can be shared and even displays details of personalized health plans for each patient.[4]

B. MUSIC ROYALTIES' TRACKING

Media chain uses smart contracts to get musicians the money they deserve. By entering into a decentralized, transparent contract, artists can agree to higher royalties and actually get paid in full and on time. Streaming giant Spotify acquired Media chain in April 2017. Many of the current problems in media deal with data privacy, royalty payments and piracy of intellectual property. According to a study by Deloitte, the digitization of media has caused widespread sharing of content that infringes on copyrights.[4]

C. CROSS-BORDER PAYMENTS

Real estate marketplace with a decentralized title registry system. The online marketplace uses blockchain to make title issuance instantaneous and even offers properties that can be purchased using cryptocurrency. Blockchain is especially popular in finance for the money and time it can save financial companies of all sizes.[4]

D. REAL-TIME IOT OPERATING SYSTEMS

The Internet of Things (IoT) is the next logical boom in blockchain applications. IoT has millions of applications and many safety concerns, and an increase in IoT products means better chances for hackers to steal your data on everything from an Amazon Alexa to a smart thermostat.[4]

E. VOTING MECHANISM

Votz is a mobile voting platform that runs on blockchain. The encrypted biometric security system makes it secure to vote on a mobile device from anywhere in the world without fear of hacking or data corruption. West Virginia is one of the first states to use the company's platform to collect votes from eligible service people and travellers abroad during elections.[4]

F. SUPPLY CHAIN AND LOGISTICS MONITORING

A major complaint in the shipping industry is the lack of communication and transparency due to the large number of logistics companies crowding the space. A major complaint in the shipping industry is the lack of communication and transparency due to the large number of logistics companies crowding the space.[4]

G. PERSONAL IDENTITY SECURITY

By keeping social security numbers, birth certificates, birth dates and other sensitive information on a decentralized blockchain ledger, the government could see a drastic drop in identity theft claims. Here are a few blockchain-based enterprises at the forefront of identity security.[4]

3. METHODOLOGIES

Systematic mapping study was selected as the research methodology for this study. The goal of a systematic mapping study is to provide an over view of a research area, to establish if research evidence exists, and quantify the amount of evidence . In this study we follow the systematic mapping process described by Petersen et al. .We also use guidelines for a systematic literature review described by Kitchenham and Charters to search for relevant papers.[6]

A. RESEARCH TOPICS HAVE BEEN ADDRESSED IN CURRENT RESEARCH ON BLOCKCHAIN

The main research question of this mapping study is to understand the current research topics on Blockchain. By collecting all the relevant papers from scientific databases, we would be able to create an overall understanding of Blockchain research and map the current research areas. Mapping the current research done on Blockchain technology will help other researchers and practitioners to gain better understanding on the current research topics, which will help to take the research on Blockchain even further.[6]

B. APPLICATIONS HAVE BEEN DEVELOPED WITH AND FOR BLOCKCHAIN TECHNOLOGY

Blockchain is mostly known for its relation to Bitcoin cryptocurrency. Bitcoin uses Blockchain technology in currency transactions. However, Bitcoin cryptocurrency is not the only solution that uses Blockchain technology. Therefore, it is important to find the current applications developed by using Blockchain technology. Identifying other applications can help to understand other directions and ways to use Blockchain.[6]

C. FUTURE RESEARCH DIRECTIONS FOR BLOCKCHAIN

Understanding the potential future research directions for Blockchain technology is a consequence of RQ1-RQ3. Answering this research question is beneficial when deciding where the research on Blockchain technology should be directed and what issues need to be solved.[6]

4. ALGORITHMS

There are ton of compression algorithms out there. What you need here is a lossless compression algorithm. A lossless compression algorithm compresses data such that it can be decompressed to achieve exactly what was given before compression. The opposite would be a Lossy compression algorithm. Lossy compression can remove data from a file. [9]

Compression Algorithms Include:

1) CONSENSUS ALGORITHMS
2) MINING ALGORITHMS
3) TRACEABILITY CHAIN ALGORITHMS

A. CONSENSUS ALGORITHMS

Consensus algorithms are complex but help when purchasing coins or running a node. Consensus algorithms achieve reliability on networks involving multiple nodes, making sure all nodes conform to the said rule or action. Nodes define consensus in bitcoin, not miners. The chain with the most work defines consensus. If you fork and change the POW, you will not have the mining power to secure it. Nodes accept the transactions, validate the transactions, replicate the transactions, validate the blocks, replicate the blocks, serve the blockchain, and store the blockchain. Nodes even define the Proof-of-Work algorithm that miners have to employ. [9]

B. MINING ALGORITHMS

Classification is the analysis of a set of data and to generate a set of grouping rules, which can be used to classify future data. An association rule is a rule which implies specific association relationships among a set of objects in a database. Sequence analysis is the analysis of patterns that occur in sequence. There are many algorithms proposed to implement such aspects of data mining. [9]

In blockchain, miners use computers to repeatedly and very quickly guess answers to a puzzle until one of them wins. More specifically, miners will run the block's unique header metadata (including timestamp and software version) through a hash function which returns a fixed-length random string of numbers, while modifying the nonce value to impact the hash value.

C. TRACEABILITY CHAIN ALGORITHMS

Traceability proves the origin and practices behind a transaction while collecting additional data to improve internal process performances and planning activity of each node in a supply chain. Blockchain acts on big data analytics because transaction data is streaming data and high- dimensional data from distributed computing networks. The main goal with traceability chain algorithms is to reach traceability decisions quickly. Accordingly, such an operation produces irrelevant data problems and poorly optimizes traceability in blockchain. Therefore, artificial intelligence of a blockchain mining algorithm, like the traceability chain algorithm, runs faster than a consensus algorithm because of an inference mechanism. [9]

5. TECHNOLOGIES

1. REMIX IDE

Ethereum platform uses many tools for creating and deploying smart contracts on the blockchain. Remix is one of the easiest and browser-based tools to use for the creation and deployment of smart contracts. It can be used for writing, debugging, testing and deploying smart contracts using a programming language known as Solidity.[4][9]

2. TRUFFLE FRAMEWORK

Truffle is a framework for Ethereum that offers a development environment for building Ethereum based apps. It includes support for the library that provides custom deployments for coding new contracts and links Ethereum applications. It offers the ability to perform automated contract testing using Chai and Mocha.[4] [9]

3. SLC

Solidity is a loosely typed programming language with a syntax similar to ECMA script (JavaScript) used for the creation of smart contracts on the Ethereum platform. However, you need something to convert Solidity script into a format readable by EVM (Ethereum Virtual Machine). Solc (Solidity Compiler) serves this purpose. Solidity Compilers can be categorized in two ways, solc coded in C++ and solc-js that uses Emscripten for cross-compiling from solc C++ code to JS.[4] [9]

4. SOLIUM

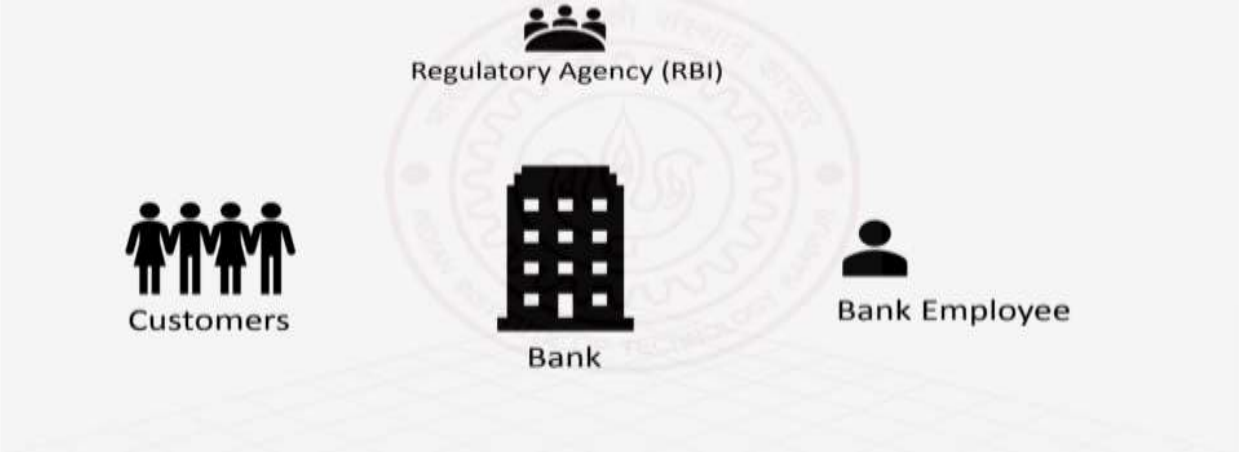
While developing a blockchain app, security plays a crucial role. It is essential to ensure that the Solidity Code is free from security holes. Solium tool is designed to format solidity code and resolve security issues in your code. It makes sure that the code is formatted and checks for vulnerability too. Use Solium by installing it with npm.[4] [9]

5. GETH

Geth is an Ethereum client used for running Ethereum nodes in the Go programming language. Geth is basically a program which works as a node for the Ethereum platform and can be used for mining ether tokens, create smart contracts, transfer tokens and explore the block history.[4] [9]

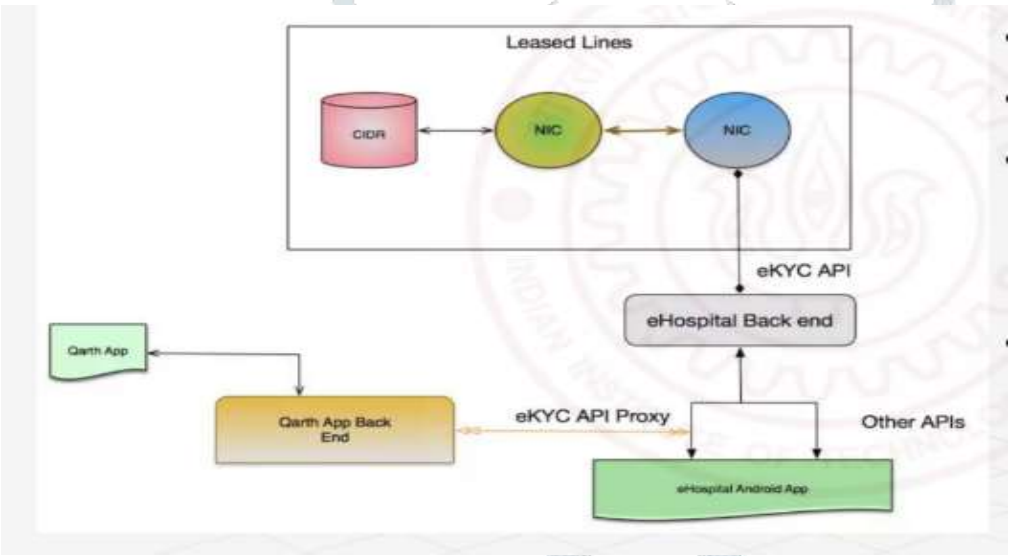
6. CURRENT R&D WORKS IN THE FIELD

1. BANKING SECTOR



Your write a check or do internet transaction to pay a payee
Bank checks if you have balance > transaction amount
• If yes, it debits your account by balance = balance - transaction amount
credit's payee's account by payee. Balance = payee. Balance + transaction amount
• If no, the transaction is invalid and rejected.
• You can check your transaction list online, or check the monthly
Statement. Bank maintain ledgers.
if Bank allows an invalid transaction go through
- Invalid = you did not authenticate the transaction
- Invalid = your balance was not sufficient but transaction was made[5]

2. IN AADHAAR CARD SYSTEM



- E-KYC logs
- Shown to you by UIDAI
- Different ID numbers
- A blockchain-based Aadhaar would help UIDAI to comply with the data protection and privacy stipulations outlined in the Right to Privacy judgment. It would allow information to be collected, held and utilized transparently with the consent of the individual whose information it is.[5]

7. 7. REFERENCES

- [1] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.[online] Available: https://bitcoin.org/bitcoin.pdf
- [2] S. Makridakis, A. Polemitis, G. Giaglis, and S. Louca, ``Blockchain: The next breakthrough in the rapid progress of AI," in Artificial Intelligence- Emerging Trends and Applications. London, U.K.: Intech Open, 2018.
- [3] K. Fanning and D. P. Centers, ``Blockchain and its coming impact on
- _nancial services," J. Corporate Accounting Finance, vol. 27, no. 5,
- pp. 53_57, 2016.
- [4] https://www.blockchain-council.org/blockchain/top-10-tools-for-blockchain-development/
- [5] https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477

- [6] https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.allerin.com%2Fblog%2Fwhat-is-the-it-market-clock-methodology&psig=AOvVaw3okYQid9T3qd4kkoo-qLdw&ust=1584122223502000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCID17orClegCFQAAAAAdAAAAABAD
- [7] https://en.wikipedia.org/wiki/Blockchain
- [8] https://blockgeeks.com/guides/blockchain-applications.
- [9]https://hackernoon.com/top-12-blockchain-development-tools-to-build-blockchain-ecosystem-371a1b587248]