

EMPOWERING APPLICATION WITH EASY TO INTEGRATE BLOCKCHAIN

Aakanksha Bomble¹, Nikhil Naidu², Prerana Padave³, Prof. Kushal Suvarna⁴

(EXTC, Viva Institute of Technology, India)

Abstract: Satoshi Nakamoto's development of Bitcoin in 2009 has regularly been hailed as an extreme advancement in cash and money, being the principal illustration of a computerized resource which at the similar time has no sponsorship or inherent worth and no unified guarantor or regulator. Nonetheless, another - seemingly more significant - portion of the Bitcoin test is the basic blockchain innovation as an apparatus of appropriated agreement, and consideration is quickly beginning to move to this other part of Bitcoin. So we are utilizing this innovation to make our own blockchain which is reasonable for some specialty areas which defeats the misfortunes of Bitcoin blockchain. The internet is undergoing a transformation: concentrated restrictive administrations are being supplanted with open, decentralised ones; believed parties supplanted with undeniable calculation; fragile area addresses supplanted with versatile substance addresses; wasteful solid administrations supplanted with shared algorithmic business sectors.

Bitcoin, Ethereum, and other blockchain networks have gained popularity in recent years. It has demonstrated the utility of decentralized exchange ledgers. We are building blockchain which can be easily integrated. We are using proof of work method in consensus layer.

Keywords –Blockchain, Decentralized system, Proof of work, Bitcoin, Proof of stake.

I. INTRODUCTION

The internet is undergoing a transformation, with centralised proprietary services being replaced by decentralised open services; brittle location addresses replaced with resilient content addresses; trusted parties replaced with verifiable computation Peer-to-peer algorithmic markets are replacing wasteful monolithic services. It is consisting of a series of blocks that contains information. It was first defined in 1991. A blockchain is a distributed ledger that it is totally accessible to anybody. Once data has been stored in a blockchain, changing it becomes extremely impossible. Each block contains some data, hash of block, & hash to previous block. The kind of blockchain determines the data that is kept within each block. For example, the bitcoin blockchain maintains transaction data such as sender, recipient, and coin amount. A hash is similar to a fingerprint in that it identifies a block and all of its contents and is always unique, just like a fingerprint. The hash of a block is determined after it is produced. The hash will change if something inside the block is changed. When you wish to identify changes to blocks, hashes come in handy. If a block's fingerprint changes, it's no longer in the same block. The previous block's hash is the third element. This essentially forms a chain of blocks, and it is this mechanism that ensures the security of a blockchain. Our solution is a decentralised network that transforms cloud storage into a market based on algorithm. A tangible asset (a home, car, cash, or land) or an intangible are two types of assets. As a member of a members-only network, you can trust that you will get accurate and timely data from blockchain, and that your sensitive blockchain records will be shared only with network members to whom you have expressly authorised access. These contracts are simple in nature that are stored on blockchain and can be put to use automatically exchange coins based on criteria.

II. LITERATURE SURVEY

2.1: bitcoin: a peer-to-peer electronics payment system The satoshi nakamoto published a paper entitled "bitcoin: a peer to peer electronic cash system" in that We have learned about the fundamental data structure of blockchain, consensus algorithm, proof of work Concept, mining and about networking. The technology stack

VIVA Institute of Technology

10th National Conference on Role of Engineers in Nation Building – 2022 (NCRENB-2022)
used in this paper are c++, python and c. This Paper comes under domain of blockchain technology,
cryptography and cryptocurrency.

2.2: ethereum: a platform for next-generation smart contracts and decentralized applications, the vitalik buterin published paper entitled " ethereum: a decentralized smart contract and application of the futurePlatform" in that we have learned about merkle tree, consensus algorithm, proof of work, decentralized Computing and networking. The technology stack used in this paper is go, c javascript. This paper comes under the domain of blockchain technology, cryptography, distributed computation and cryptocurrency.

2.3: solana: a high-performance blockchain architecture v0.8.13 The vitalik buterin published a paper entitled "Solana: a high-performance blockchain with a revolutionary architecture v0.8.13" in that we learned about network design consensus algorithm proof-of-stake decentralized computing networking. The technology stack used in this paper are rust, typescript. This paper comes under the domain of blockchain technology, cryptography, distributed computation and cryptocurrency. 2.4: a federated model for internet-level consensus: the stellar consensus protocol "The stellar consensus protocol: a federated model for internet-level consensus" was the topic of our study.". In this paper we learned about protocol design, benchmarking with other consensus algorithms, byzantine fault tolerance. The technology stack used in this paper are c, c++. This paper comes under domain of blockchain, cryptography, consensus protocol

2.5: hyperledger architecture, volume 1 we researched " hyperledger architecture, volume 1". In this paper we learned about protocol design use different consensus protocols in one Framework industrial use-case idea. The technology stack used in this paper is go. This paper comes under domain of blockchain, cryptography, consensus protocol

III. METHODOLOGY



Consensus Layer: It deals with the generation and verification of blocks. It's merely a way for a group to make decisions. Let me illustrate this with an example. Consider a group of 10 people who wish to decide on a project that will benefit them all. Each of them can propose a suggestion, but the majority will choose the one that will benefit them the most. Others must deal with this choice, whether they agree or disagree with it. Without consensus, blockchain is simply a way of storing encrypted/unencrypted data. Consensus allows it to be decentralised since all nodes in the network obey the same rules, ensuring consistency across all blockchain versions. As a result, any modification made in one blockchain is confirmed and adopted by another in the network. When we talk about consensus, we're referring to the collaborative process used by network nodes to agree on the validity of a transaction and to maintain the distributed ledger synced at all times. Because harmful (or fraudulent) transactions would have to occur (or be performed) across multiple places at the same time, or else the tampering would be detected relatively instantly by other nodes, these consensus techniques reduce the danger of malicious (or fraudulent) transactions. Before a transaction can be permanently recorded in the ledger,

VIVA Institute of Technology

10th National Conference on Role of Engineers in Nation Building – 2022 (NCRENB-2022)

the majority of the parties must agree that it is genuine..No one, not even the system administrator, can remove a transaction from the ledger after it has become permanent. The cost and time it takes to establish consensus are determined by the technique used and the number of nodes involved. The process of obtaining a high-level agreement includes the following steps, mining and propagation of blocks in the network defined by the consensus algorithm.

Protocol layer: Decides the methods of consensus and network participation with core elements and communication between peers. We need to have some rules to get each player of the team aligned towards the end goal (depending on the use-case / blockchain). For this we use a set of rules, which is as you know called the protocol layer. Here we decide what the truth is and build upon the core .Infrastructure elements are provided. Consensus can shift throughout the game, as the splits of Bitcoin Cash and Ethereum Classic have shown, but the infrastructure's essential pieces frequently remain the same. We have a common understanding if we know and comprehend the essential aspects, the method we interact within the team, and the regulations we must follow..This is a fantastic place to start when it comes to adding services and add-ons to your layers. This is also when you get more out of the back end and move towards the front end (away from the technical aspects and toward the user-facing aspects). Wallets for users and interface with the outside world of oracles appear here. Still a little techy, but greater involvement with the blockchain's outer reaches. This is the midfield in a sports comparison, a vital link between the back end and the front end.

Network layer: Blockchains are distributed across a peer-to-peer network. Peers communicate information about the network's current condition. The network layer includes privacy and security. While the blockchain technologies themselves are not novel, how they are used to build potentially decentralised and trustless networks is. As a result, extensive study and testing are required to properly comprehend the technology and its ramifications. Hopefully, this will serve as a starting point for organising the necessary research and development to fully fulfil the promise of this revolutionary new technology.

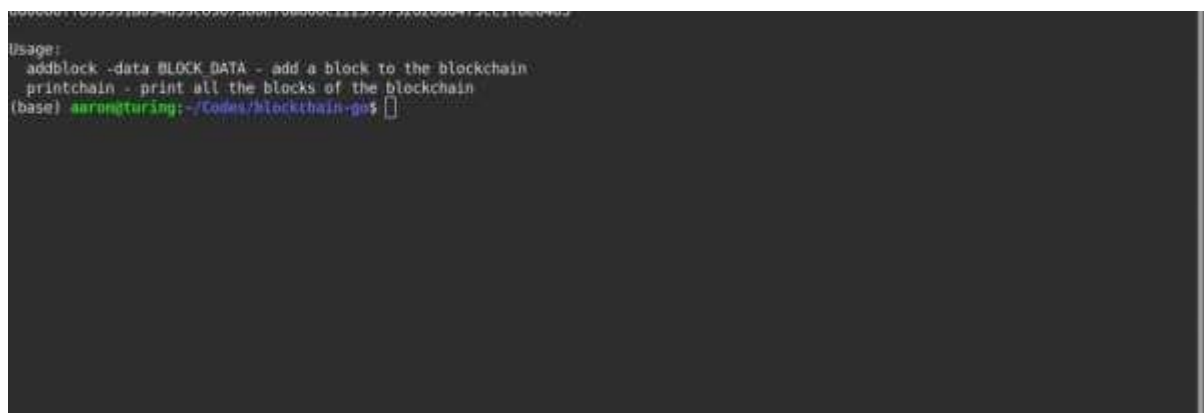
Data layer: Data structures of a blockchain are represented as a linked-list of blocks where transactions are ordered. The data structure of a block chain consists of two fundamental elements: pointers and a linked li. The genesis block i.e. the first block does not contain the pointer as it's the first in the chain.

Storage layer: LevelDB sorts data by key and saves keys and values in arbitrary byte arrays. Batch writes, forward and backward iteration, and data compression using Google's Snappy compression package are all supported. LevelDB isn't a relational database. It lacks a relational data schema and does not handle SQL queries, just as other NoSQL and dbm stores..It also doesn't support indexes. Because it lacks a server or command-line interface, applications utilise LevelDB as a library.

LevelDB is one of the supported backends for Risk and is used as the backend database for Google Chrome's IndexedDB..A LevelDB database is also used by Bitcoin Core and go-ethereum to hold blockchain metadata. For chunk and entity data storage, Minecraft Bedrock Edition utilises a modified version. Autodesk. LevelDB is also used in AutoCAD 2016.

IV. FIGURES AND TABLES

1.NO EXISTING BLOCKCHAIN



```
Usage:
  addblock -data BLOCK DATA - add a block to the blockchain
  printchain - print all the blocks of the blockchain
(base) aaron@turing:~/Codes/blockchain-go$
```

2.PRINT THE EXISTING BLOCKCHAIN

```
(base) aaron@turing:~/Codes/blockchain-go$ ./blockchain printchain
Prev. hash:
Data: Genesis Block
Hash: 000000ff899391a094b39c09075b0e70a60dc122373732626dd475cc1f8e6403
Pow: true

(base) aaron@turing:~/Codes/blockchain-go$
```

3.ADDING A BLOCK TO BLOCKCHAIN WITH DATA

```
Mining the block containing "nick send 2 btc to naddy"
000000fc52a0018d801e3b2500556f7853095be91914a7c9a93932740bda6603

Success!
(base) aaron@turing:~/Codes/blockchain-go$
```

4.PRINTING THE WHOLE CHAIN

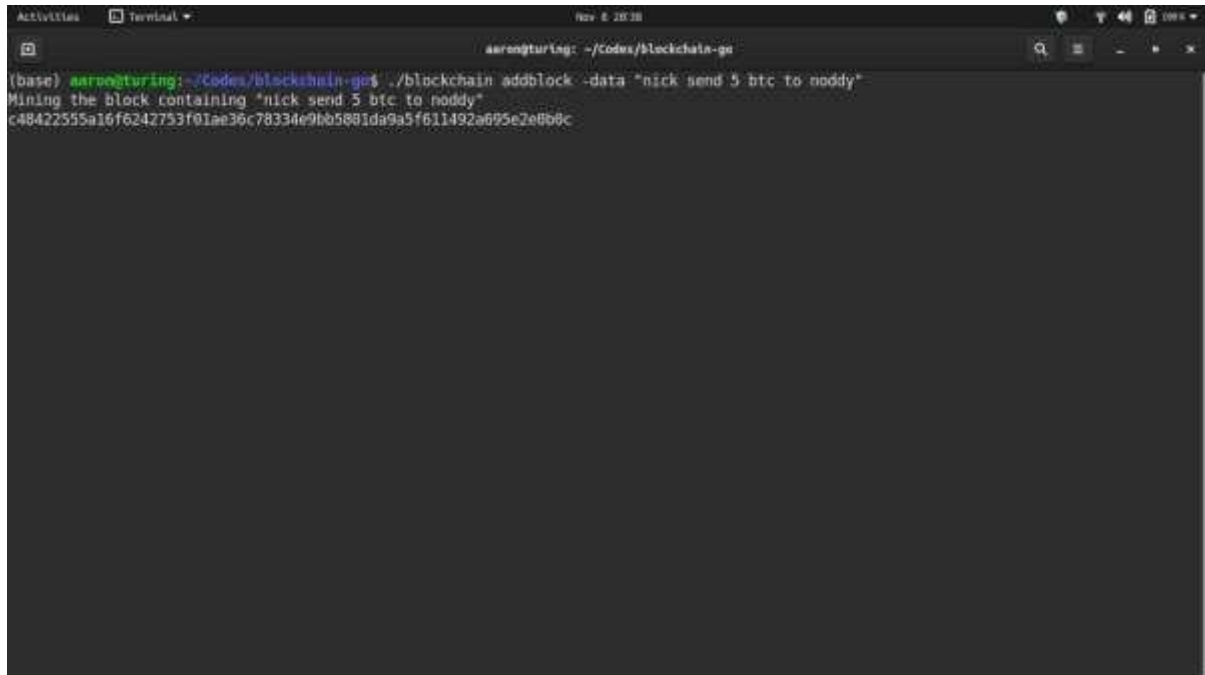
```
Activities Terminal Nov 8, 2022
aaron@turing: ~/Codes/blockchain-go

(base) aaron@turing:~/Codes/blockchain-go$ ./blockchain printchain
Prev. hash: 000000ff899391a094b39c09075b0e70a60dc122373732626dd475cc1f8e6403
Data: nick send 2 btc to naddy
Hash: 000000fc52a0018d801e3b2500556f7853095be91914a7c9a93932740bda6603
Pow: true

Prev. hash:
Data: Genesis Block
Hash: 000000ff899391a094b39c09075b0e70a60dc122373732626dd475cc1f8e6403
Pow: true

(base) aaron@turing:~/Codes/blockchain-go$
```

5.PROCESS OF MINING WHEN YOU ADD A NEW BLOCK



```
Activities Terminal Nov 8 20:38
aaron@turing: ~/Codes/blockchain-go
(base) aaron@turing:~/Codes/blockchain-go$ ./blockchain addblock -data "nick send 5 btc to noddy"
Mining the block containing "nick send 5 btc to noddy"
c48422555a16f6242753f01ae36c78334e9bb5881da9a5f611492a695e2e8b6c
```

V. CONCLUSION

We have presented an electronic transaction system that does not rely on trust. We started with the standard foundation of currencies generated from digital signatures, which allows for tight ownership control. By reviewing some of the papers about industrial-scale block chains and concepts we are going to come up with a design that is scalable, secured and easy to use for the masses with all the latest research from academia included. By reviewing and implementing some of the blockchains concepts we are going to come up with a design that is going to satisfy our objectives.

Acknowledgements

Presentation, Inspiration and motivation have always played a vital role in any field's growth. It gives me immense pleasure to express my gratitude to my guide Prof.Kushal Suvarna, Extc Department, Viva Institute of Technology, Virar, for his valuable guidance, encouragement and help for completing this work.

I would like to express my sincere thanks to you sir,, for giving us this opportunity to undertake this paper presentation. I would also like to thank our principal Dr. Arun Kumar to show us a support. I would also want to show my gratitude to Prof. Archana Ingle HOD (EXTC Engineering) for her support. I am also grateful to all my teachers for their constant support and right guidance.

I am immensely obliged to my team members for their elevating inspiration, encouraging guidance, support and valuable efforts in the completion of the paper.

REFERENCES

- [1] F. Restuccia, s. D'oro, s., s. Kanhere, t. Melodia and s., k. Das, "blockchain for the internet of things: present and future", iee internet of things journal, 2018.
- [2] K. Christidis and m. Devetsikiotis, "blockchains and smart contracts for the internet of things", iee access, 2016.
- [3] M.c.k. khalilov and a. Levi, "a survey on anonymity and privacy in bitcoin-like digital cash systems", iee communication surveys, 2018.

- [4] J. Kishigami, s. Fujimura, h. Watanabe, a. Nakadaira and a. Akutsu, "the blockchain-based digital content distribution system", in: 2015 iee fifth international conference on big data and cloud computing, 2015
- [5] W. Dai, "b-money," <http://www.weidai.com/bmoney.txt>, 1998.
- [6] H. Massias, x.s. avila, and j.-j. Quisquater, "design of a secure timestamping service with minimal trust requirements," in 20th symposium on information theory in the benelux, may 1999.
- [7] S. Haber, w.s. stornetta, "how to time-stamp a digital document," in journal of cryptology, vol 3, no 2, pages 99-111, 1991.
- [8] D. Bayer, s. Haber, w.s. stornetta, "improving the efficiency and reliability of digital time-stamping," in sequences ii: methods in communication, security and computer science, pages 329-334, 1993.
- [9] S. Haber, w.s. stornetta, "secure names for bit-strings," in proceedings of the 4th acm conference on computer and communications security, pages 28-35, april 1997.
- [10] A. Back, "hashcash - a denial of service counter-measure," <http://www.hashcash.org/papers/hashcash.pdf>, 2002.
- [11] R.c. merkle, "protocols for public key cryptosystems," in proc. 1980 symposium on security and privacy, iee computer society, pages 122-133, april 1980.
- [12] W. Feller, "an introduction to probability theory and its applications.