Analysis of blockchain process and data protection

[1]Megha P. Nagawade, [2]Prof. Aruna Verma

[#12]Department of Computer Engineering

Dhole Patil College of Engineering, Near EON IT Park,
Vitthal Nagar, Kharadi, Pune, Maharashtra 412207.

Abstract : Block chain is one of the emerging technologies which has higher scope for future applications. Block chain process is formulated based on blockchain thinking and formulating thinking. Blockchains allow us to have a distributed peer-to-peer network where non-trusting members can interact with each other without a trusted intermediary, in a veritable manner. The basic applications of blockchain provide vast chances to create more secured intelligence system. The feature of block chain with respect to sustainability is concluded with some of the major advantages and disadvantages of block chain.

Keywords: Blockchain; philosophy, thinking, utility, secured, intelligence system, use case

I. Introduction

Blockchain is based on distributed data structure which shares information among the members across the network. A blockchain is a database shared by every participant in a given system. The block chain stores the complete transaction history of a cryptocurrency or other record keeping system.

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger With a previous block hash contained in the block header, a block has only one parent block.[7] It is worth noting that uncle blocks (children of the blocks ancestors) hashes would also be stored in ethereum blockchain. The first block of a blockchain is called genesis block which has no parent block.

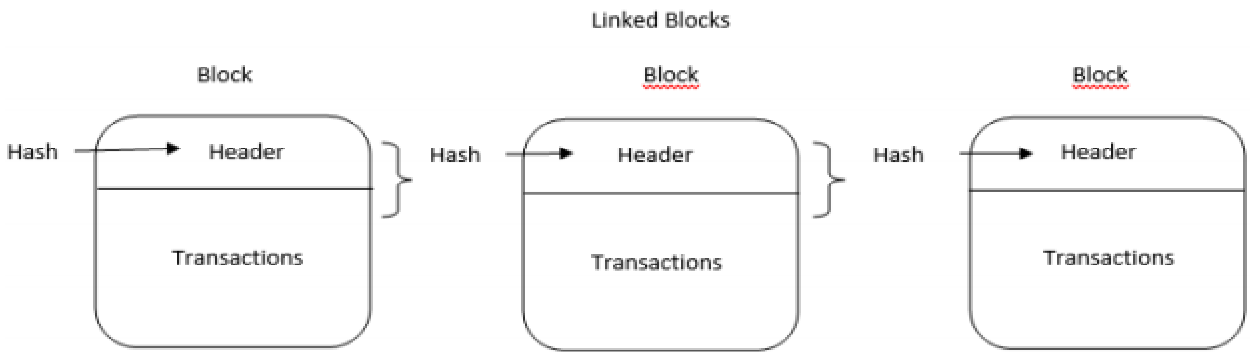

Figure 1: The transaction process of blockchain

Block: A block consists of the block header and the block body. In particular, the block header includes:

- Block version: indicates which set of block validation rules to follow.
- Merkle tree root hash: the hash value of all the transactions in the block.
- Timestamp: current time as seconds in universal time since Jan-uary 1, 1970.
- nBits: target threshold of a valid block hash.
- Nonce: an 4-byte eld, which usually starts with 0 and increases for every hash calculation
- Parent block hash: a 256-bit hash value that points to the previous block

Bit coin introduced the concept of blockchain basically to overcome the issue of double spending problem. A user requests for a transaction. A block is created representing the transaction. After that it is broadcasted to all the nodes of the network.

A. Blockchains: Private Vs. Public

A typical blockchain system consists of multiple nodes which do not fully trust each other. Some nodes exhibit Byzantine behavior, but the majority is honest. Together, the nodes maintain a set of shared, global states and perform transactions modifying the states. Blockchain is a special data structure which stores historical states and transac-tions. All nodes in the system agree on the transactions and their order. Figure 1 shows the blockchain data structure, in which each block is linked to its predecessor via a cryptographic pointer, all the way back to the first (genesis) block. Because of this, blockchain is often referred to as a distributed ledger.

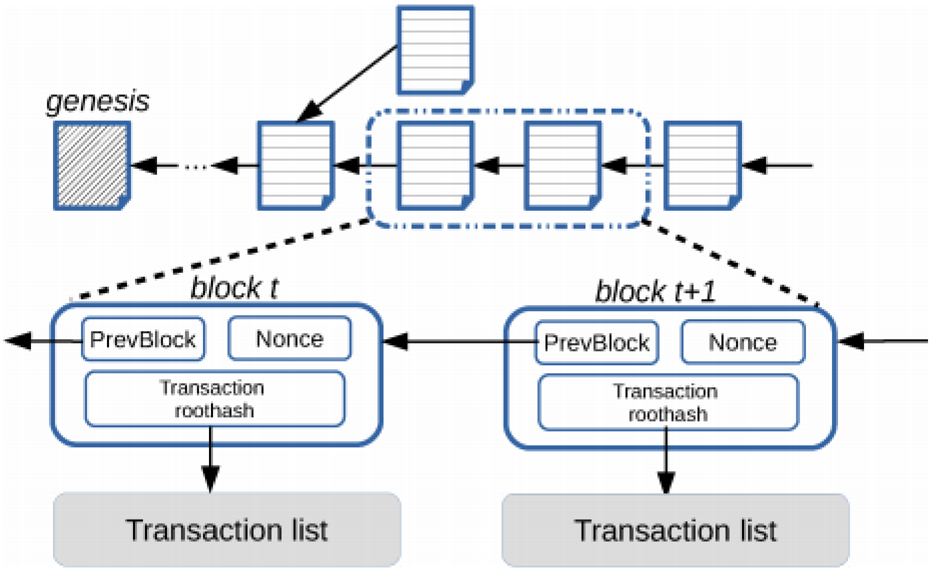

Fig. 2: Blockchain data structure. Transactions are packed into blocks which are linked to previous blocks.

II. CRYPTOGRAPHY CONCEPT

Blockchain systems make heavy use of cryptographic tech-niques to ensure integrity of the ledgers. Integrity here refers to the ability to detect tampering of the blockchain data. This property is vital in public settings where there is no pre-established trust. For example, public confidence in crypto-currencies like Bitcoin, which determines values of the currencies, is predicated upon the integrity of the ledger; that is the ledger must be able to detect double spending. Even in private blockchains, integrity is equally essential because the authenticated nodes can still act maliciously.

There are at least two levels of integrity protection.

First, the global states are protected by a hash (Merkle) tree whose root hash is stored in a block. Any state change results in a new root hash. The tree's leaves contain the states, the internal nodes contain the hashes of their children. For instance, Hyperledger v0.6 uses a bucket hash tree, in which states are grouped (by hashing) into a pre-defined number of buckets. Ethereum, on the other hand, employs a Patricia-Merkle tree which resembles a tries and whose leaves are key-value states.

Second, the block history is protected, that is the blocks are immutable once they are appended to the blockchain. The key technique is to link the blocks through a chain of cryptographic hash pointers: the content of block number n + 1 contains the hash of block number n. This way, any modification in block n immediately invalidates all the subsequent blocks. By combining Merkle tree and hash pointers, blockchain offers a secure and efficient data model that tracks all historical changes made to the global states.

III. METHODOLOGY

Evaluation Methods:
The evaluation is focused in two different aspects:

- **Macro benchmarks:**

It will give performance of the blockchains at the application layer, using YCSB and Smallbank benchmarks. We observe that in terms of throughput, Hyperledger outperforms the other two in both bench-marks. The gap between Hyperledger and Ethereum is due to the di erence in the consensus protocols: one is based on PBFT while the other is based on PoW. To put their performance in context, we compare the three blockchains against a popular in-memory database system, namely H-Store, using the YCSB and Smallbank workload. Blockchains and databases do not necessarily share the same design goal: the former are not designed for general data processing, nor do the latter protect data integrity against Byzantine failures.

- **Micro benchmarks:**

It will give the performance of the blockchains at the execution, data model and consensus layer. We deployed the CPU Heavy smart contract that is initialized with an integer array of a given size. The array is initialized in descending order. We invoked the contract to sort the array using quicksort algorithm, and measured the execution time and servers peak memory usage.

Algorithm: 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 trace-ability 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.

Steps of Traceability algorithms:

1. Identification and labeling of products to facilitate product identification.
2. Data capturing and recording: scanning capabilities with electronic information flow to optimize retrieval of data.
3. Linkages and communication to optimize data sharing between supply chain partners and protocols.

IV. BLOCKCHAIN BASED SECURED INTELLIGENCE SYSTEM

i. Blockchain

Thinking Blockchain in combination with AI works like a human brain. The memory is like a conventional neural network, but stored in multiple locations. This memory is retrieved whenever required for performing some computations. The neural network learns from external and stores in the Blockchain.

ii. Architecture

The architecture of Blockchain thinker is iput-process-output model. The input is various data obtained from external. This data is processed in distributed environment. The output is the actions taken based on the results of processing.

iii. Input

Various sensors are employed to collect data from external. For example, in a home automation system, sensors such as gas detector, power detector, smoke detector, cameras, fire detector, temperature sensors, water level detector, proximity sensor, pressure sensor, water quality sensor, IR sensor, motion detector, accelerometer sensor, gyroscope sensor, humidity sensor, optical sensor are used to collect data from external. This data is stored in Blockchain as a distributed file. These files are retrieved using internet from distributed locations. These sensors are recording the mind of a person and his mood also into digital files. The daily routine of a person is digitally stored along with the person's mood and the actions based on his mood.

iv. Processing

The data retrieved from distributed locations are analyzed using deep learning networks to take decisions. For example, there is a noise received from sound sensor, the noise is analyzed whether from a television set or from a cracker blast or from a toxic substance burst. The analysis is done by smart contracts running in different machines in a distributed way. A right decision is taken after the analysis. For example, in case of a fire accident, the owner of the house has to be alerted. A person's behavior is studied by the deep learning networks. The mind and mood patterns are analyzed to predict the sequence of next activities. For example, when one person is doing exercise, the next action can be taking bath.

v. Self mining system

When one sensor transfers data, another sensor is doing mining to validate the genuineness of data transferred. For example, when a camera detects the owner waiting for the door to open, the proximity sensor mounted in the door is doing mining work. The camera sensor data is validated and approved by proximity sensor to take next action such as opening the door.

vi. Proof of decision

The Blockchain thinker supports proof of decision by the participant nodes of the Blockchain. For example, in a home automation system, all sensors constitute a Blockchain. when camera sensor takes the decision to open the door, more than 50% of the sensors approve the decision to prove the genuineness of the decision. This avoids a malicious attack from external hacker to open the door illegally.

vii. Output

The output of a Blockchain thinker is an action or a feedback loop or a just notification. The actions are executed by smart contracts running on different participant nodes of the Blockchain. Feedback loops help to learn the environment. Notifications are used to update the states of the participant nodes. For example, actuators are used to perform actions such as opening the door, closing the door, switching on the geizer etc.

V. ADVANTAGES OF BLOCKCHAIN

Many of the real time issues can be fixed using blockchain. It can be also applicable for maintaining our financial life. It also has a lot of impact on industries. Some of the major advantages of block chain are

1. Decentralized

Banking sector shackle and handle customers in monopoly way. A huge amount of money is charged to verify the customers own particular assets. After being decentralized also blockchain is still applicable to a large number of users. It also retains some additional advantages such as no middle man scenario and most importantly the whole network is not in control of any one.

2. Distributed

In spite of having a centralized server, the network is still distributed. The data is spread to all over the user and nodes. Henceforth every user has control over the system. Blockchain networks are also compatible with IoTs. In realistic it is unbackable.

3. Immutable

Over time, the process of recovery and undoing gets tougher. So, in that sense, the technology can be said to be immutable. It’s a good and bad thing at the very same time. If you are a freelancer, once the client sends you the payment. Such a feature makes the tech more robust and sustainable and more trustworthy among the users.

4. Trustless

Users follow a common consensus algorithm that will verify every transaction and store it one the common ledger. Moreover, everyone can see the all the transactions made. And if any transaction violates this consensus algorithm, the transaction itself gets violated. So, even if the parties don't trust each other, it doesn't matter. The system is designed to ensure safety and common trust among the users.

VI. CONCLUSION

In this paper, we have conducted a comprehensive survey on blockchain technologies. We laid out four underpinning concepts behind blockchains and analyzed the state of the art using these concepts. We presented our benchmarking framework, BLOCKBENCH which is designed to evaluate performance of blockchains as data processing platforms. Finally, we discussed four potential research directions, inspired by database design principles, for improving block-chain performance. We hope that the survey and bench-marking framework would serve to guide the design and implementation of future blockchain systems that are not only secure, but scalable and usable in the real world.

REFERENCES

[1] J. Kelly and A. Williams. (2016). Forty Big Banks TestBlockchain-Based Bond Trading System.[Online]. Available:http://www.nytimes.com/reuters/2016/03/02/business/02reuters-bankingblockchain-bonds.html

[2] Kar. (2016). Estonian Citizens Will Soon Have the World's Most Hack-Proof Health-Care Records. [Online]. Available: http://qz. com/628889/this-eastern-european-country-is-moving-its-health-recordsto-the-blockchain/

[3] W. Suberg. (2015). Factom's Latest Partnership Takes on US Health-care. [Online]. Available: http://cointelegraph.com/news/factoms-latest-partnership-takes-on-us-healthcare

[4] S. Lacey. (2016). The Energy Blockchain: How Bitcoin Could be a Catalystfor the Distributed Grid. [Online]. Available: http://www.greentechmedia.com/articles/read/the-energy-blockchain-could-bitcoinbe-a-catalyst-for-the-distributed-grid [5] D. Oparah. (2016). 3 Ways That the Blockchain Will Change the RealEstate Market. [Online]. Available: http://techcrunch.com/2016/02/06/3-ways-that-blockchain-will-change-the-real-estatemarket/

[6] Mizrahi. (2015). A Blockchain-Based Property Ownership Recording System. [Online]. Available: http://chromaway.com/papers/A-blockchain-based-property-registry.pdf

[7] M. Walport, ``Distributed ledger technology: beyond block chain,'' U.K. Government Of ce Sci., London, U.K., Tech. Rep., Jan. 2016. [Online]. Available: https://www.gov.uk/government/publications/ distributed-ledger-technology-blackett-review

[8] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[9] Double-Spending Bitcoin WiKi, accessed on Mar. 15, 2016. [Online].Available: https://en.bitcoin.it/wiki/Double-spending

[10] Eris Industries Documentation Blockchains, accessed on Mar. 15,2016. [Online]. Available: https://docs.erisindustries.com/explainers/ blockchains/

[11] G. Greenspan. (2015). Ending the Bitcoin vs Blockchain Debate. [Online]. Available: http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/