Blockchain based Data Sharing

Srikar Gundla

Computer Science & Engineering
IIT Dharwad

Abstract: This report touches upon protecting information in the 5G network efficiently and securely. It further discusses upon a scheme based on blockchain technology to resolve the privacy issues in 5G networks. Illustration on how mutual trust is gained between content provider and user community by merging blockchain in data sharing is also explained.

Correspondence: ***180010016@iitdh.ac.in***

Introduction

The 5G networks represent the future phase of telecommunication, with recent developments and successful deployments around the world. The three major features of 5G networks are Ultra low latency, enhanced mobile broadband, massive machine type communication. The main issue with the 5G networks is security. The techniques used in 2G, 3G, 4G are not adequate for 5G as they are powerless to deal with data tampering, also security and privacy beyond protecting data integrity. There are many emerging 5G technologies such as SDN, D2D communications, further leading to increase in security and privacy challenges. 5G wireless networks are going to be decentralized which have importance for security requirements as well as privacy. In 5G, decentralization, immutability and transparency are the crucial factors which aid us in solving security issues. So, data sharing has become a major concern because of the security and privacy challenges in 5G networks. As the existing techniques are powerless to deal with the issues in 5G, we need to take this to a step further in order to tackle the challenges. Introducing blockchain could be the turning point in 5G and beyond networks.

The blockchain is a decentralized, immutable and transparent database. Blockchain proposes a solution for the challenges in 5G networks. Blockchain is based on peer-to-peer network architecture in which the information is managed by all the participants in the ledger unlike a centralized authority. Blockchain builds trust and security with its decentralization and immutability nature. As blockchain is capable of solving issues of security and privacy, we try combining them to solve the issues in data sharing.

Blockchain : Background and features of blockchain

Blockchain

Blockchain is mostly know for its cryptocurrency Bitcoin transactions. The basic idea underneath the technology is decentralization. Instead of storing the data at a single location, the data is copied and distributed among the participants in the ledger. Whenever there is a new transaction taking place or new block is added, the change is reflected in all the computers. The main advantage of blockchain is that there is no single-point failure. The blockchain is accessible for everyone but not controlled by any network entity. The concept behind working of blockchain is shown in Fig. 1. There are two kinds of chains, private and public. A public chain is accessible for everyone and anyone can participate and make transactions. Private blockchains are like invitation-only network. In this section wee discuss about the key features of blockchain.

-Data block: In simple words, a blockchain is a chain of blocks, a linear structure. The first block in the chain is called genesis block. Each block contains number of transactions and is linked to the previous block through hash. The hash of previous block is present in the current block. Each block has block header and block header contains group of transactions, hash of block for validation, a nonce value, time stamp. Nonce is a value that is generated by consensus protocol to produce hash.

-Distributed ledger: This is a database which is replicated and shared among the people in the network. Every person in the network has access to the block information.

-Consensus algorithm: As there is no centralized party to monitor the transactions, in order to regulate transaction rules and protect data from threats, we need to validate the block trustfulness. These are met using some protocols called consensus algorithm. In Bitcoin, Proof of Work algorithm is an enabling consensus mechanism run by miners to ensure security.

-Smart Contract: A smart contract is a program that runs on a blockchain network. Once the contract is deployed then any changes cannot be made. It's self-executing nature makes it smart. Let's consider transferring funds, these funds get transferred automatically over network. This will be recorded as a transaction and kept on blockchain which is immutable ledger.

-Immutability: It is the ability for ledger to keep the data tamper resistant. These are tamper-resistant because they are secured cryptographically by a hashing process. The blocks are linked, as the block contains the hash of previous block which makes the chain strongly unchangeable.

-Transparency: Everyone in the ledger has access to the information inside the block. In the public chains, everyone can view the information/ transaction details in the block. The same copy is shared across a large network for verification. Anyone can verify and track the transaction. This helps to maintain the integrity of the data.

-Decentralization: This means that it does not depend on a central point to manage transactions. This eliminates the risk

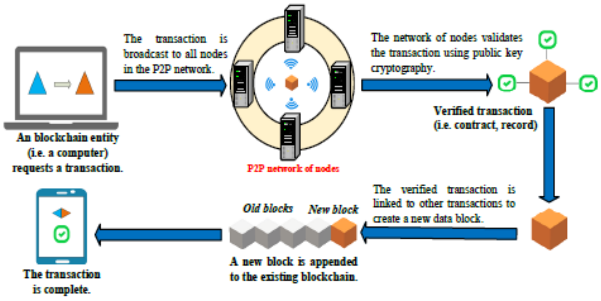
The transaction is broadcast to all nodes in the P2P network.
The network of nodes validates the transaction using public key cryptography.
Verified transaction (i.e. contract, record)
An blockchain entity (i.e. a computer) requests a transaction.
P2P network of nodes
The verified transaction is linked to other transactions to create a new data block.
Old blocks
New block
A new block is appended to the existing blockchain.
The transaction is complete.

Fig. 1. Concept used in blockchain.

of single point failure.
-Security: There are public and private keys which are inverse to each other. In simple words, it's like one key is multiplicative inverse of the other key (as in mathematics). If some data is shared then it can be signed with private key in order to maintain the data integrity and also provide privacy because the data can't be decoded without the public key of that user.

Problem Definition

Data sharing was quite a concern in 5G networks. For data sharing, we had to rely on third party cloud with no verification of data integrity. The main goal is to verify the data integrity and provide security and privacy for the data which is being shared. Verifying data integrity is a major problem. We integrate blockchain with 5G to solve the issues related to privacy and security in data sharing. Thanks to immutability and tamper-resistant nature of blockchain which helps us in maintaining security, privacy and data integrity.

The content provider, user community and cloud storage are linked via smart contract which communicates with all the three. Content provider uploads a data to cloud and whenever the user downloads the data from cloud, we must ensure data integrity. Only if the data is not tampered then only the user should be able to get the data from cloud. By doing this we can tackle the problems of data integrity.

Also, we need to ensure that no malicious user tries to access and manipulate the data. So, only if the user satisfies the control policy which is set by the content provider then the user will be able to download the data. Introducing access control policy removes the risk of data being leaked to some users whom the content provider do not wish to share with. We ensure the data integrity using blockchain data. Whenever a content provider uploads data to cloud, a transaction is taken place which is done automatically by the smart contract and a new block is added to the chain. Only a miner can add blocks to the chain. In order to get the ownership of block, a miner must solve a puzzle and if he succeeds in solving then he gets the authority to add the block. The block has the hash value of data and as well as the hash of previous block. Whenever a user tries to download the data, the integrity is verified by comparing the hash value of data in the block and the calculated hash value of data obtained from cloud.

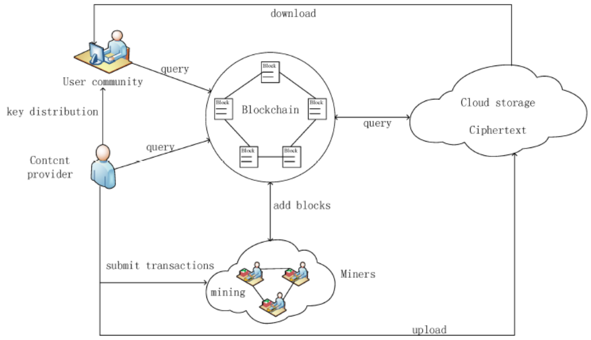

Fig. 2. System Architecture.

Approach towards implementing

As for the initial implementation, I studied how voice calls happen in 4G networks which is similar to data sharing. The study of voice calls in 4G helps to gain the knowledge about the network architecture. With the knowledge of system architecture a blockchain based architecture can be designed to tackle the problem statement. The architecture on which we are going to implement the above discussed solution is shown in Fig. 2

One way of approach towards solving the problem is following the above proposed solution locally and test it. We can deploy contracts for testing purpose using Truffle and Remix. As we locally implement the above proposed solution, we need four interfaces each for cloud storage, content provider, user community, smart contract. So, we need to make files for each of them and make them communicate with each other using Truffle IDE. In order to communicate with each other, the files needs the address of the contracts deployed. Each deployed contract has a unique address which gives access to the functions and variables present in it. We are well aware of the fact that once these contracts are deployed then we cannot make any changes. So, before deploying any contract we must ensure that the contract has no errors and works properly. The best way to deal with errors is using Remix IDE. Always test before you deploy.

We have to make sure that content provider, user community, cloud storage must be connected via smart contract where miner is invoked and addition of block takes place(only when content provider uploads a data to cloud). The main asset of blockchain is hashing. The data integrity is verified when hash of data which is in the block and the hash of data in the cloud match. The main hashing algorithms are Keccak256 and Sha256. The most important thing to know is that Sha256 and Keccak256 are not same. We get different hashes for the same data given. Ethereum uses Keccak256 but due to compiler version constraints (0.4.18), we use Sha256. Keccak256 function works well for solidity version 0.5.0 or higher.

As this is not a real network scenario, the mining takes place automatically in truffle. So, if a function which changes the variables in the contract is called, then the Truffle IDE makes a transaction. Unlike this, in the real network scenario there are actual miners who mine only after data is uploaded to the cloud. The user gets to download the data only if the data is unaltered. This is checked by the smart contract and allows the user to download only if the data in not tampered.

Results and Details

The above proposed solution was efficient in providing data integrity. For simple illustration, one content provider and two users were considered and was successful in implementing the above solution for data integrity related issue. As mentioned earlier, the user gets to download the data only if the data is unaltered. To illustrate this locally, we alter data in cloud storage and check if the data is being downloaded or not. To confirm if the altered data is downloaded by user or not, the user downloads a message 'ERROR' instead of empty string.

Attack to cloud storage: If any malicious user wants to access the data from cloud storage then he must decrypt the data from cloud storage which is encrypted with the private key of the content provider. To access it he must have the decryption key and without it the data becomes useless for the attacker.

Security & Privacy: As the data stored in the cloud is encrypted, the data is safe. As explained earlier, the data without the decryption key is useless for any attacker. This nullifies the existence of security issues. The content provider designs the access control policy for the users and only if the user satisfies the policy then he/she will be able to download the data. The access control policy rules out the question of privacy from content provider point of view.

Conclusions

Blockchain tackles most of the security and privacy related issues. With the help of blockchain and smart contract, we tackled our primary issues of data sharing in 5G networks. For the future generation networks, blockchain is capable of contributing a lot towards security, privacy and also to ensure data integrity. When compared to other existing technologies, blockchain has a lot more to contribute to the networks. Similar to the new technologies, blockchain has the ability to outperform the existing security and privacy related technologies.

ACKNOWLEDGEMENTS

I would like to express my special thanks of gratitude to Prof. Siba Narayana Swain of Computer Science department, IIT Dharwad for guiding me through tough times, encouraging me in learning and providing me tremendous opportunity to work under him for this project.

1. *A Survey of Blockchain for 5G and Beyond Networks*.
2.*Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G*.
3. https://www.youtube.com/watch?v=YxU87o4U5iw&t=612s
4. https://www.youtube.com/watch?v=qlvj8eEsBr8&list=PLbbtODcOYIoGfbrnfxgwva0Fktju0L449&index=2