OVERVIEW OF SMART CONTRACT IN BLOCKCHAIN TECHNOLOGY

JIGNESH PATIL [1], Dr. Varsha Namdeo[2], Dr. Dinesh Kumar Sahu [3]

[1] M.TECH in Computer Science, SRK UNIVERSITY BHOPAL
[2] [3] SRK university MP, Bhopal

***

Abstract — The rapid growth of blockchain technology and cryptocurrencies has altered the financial industry in recent years, resulting in the creation of a new crypto-economy. Then, thanks to the appearance of smart contracts, which are computer protocols designed to facilitate, verify, and enforce automatically the negotiation and agreement among multiple untrustworthy parties, next-generation decentralised applications without involving a trusted third-party have emerged. Despite the positive aspects of smart contracts, security threats, weaknesses, and legal concerns continue to stymie their implementation. We'll look at smart contract architecture and data authentication in blockchain in this chapter. We'll learn about smart contract components and the smart contract's future scope.

INTRODUCTION

A block in a blockchain is a collection of digital documents or transactions that have been encrypted. Each block is then "chained" to the following block in a linear, chronological order using a cryptographic signature. Blockchain is an innovative and one-of-a-kind method of safeguarding and disseminating data. In a dispersed network, the lack of a central instance implies a significant shift away from intermediary services and toward direct contacts amongst non-intermediaries.

Smart contracts are executable codes that run on top of the block chain and are used to facilitate, execute, and enforce agreements between untrustworthy parties without the need for a trusted third party. Network automation and the capacity to convert paper contracts into digital contracts were made possible by smart contracts.. Smart contracts, as opposed to traditional contracts, allowed users to formalise their agreements and trust relationships through automated transactions that were not supervised by a central authority. Smart contracts are copied to each node of the blockchain network to prevent contract manipulation. Human error could be eliminated by allowing computers to execute tasks and using services supplied by blockchain platforms to avoid contract disputes. We perform a comprehensive survey to better understand existing smart contract subjects, with the goal of better identifying and mapping research areas that require additional investigation. The goal of this survey is to look at smart contracts from both a technical (e.g., codifying, security, and performance) and a user perspective (e.g., smart contract applications in finance, healthcare, etc).

On the blockchain, a smart contract is a computer programme that runs. Between non-trusting participants, a smart contract might be thought of as a trusted third party. A contract storage, a balance, and programme code make up smart contracts. Simply by adding a transaction to the blockchain, it can be generated and made available for usage by any node in the network.

Once a smart contract is added to the blockchain, its software code is locked and cannot be changed. Smart contracts are managed by a network of miners who are in charge of keeping the blockchain up to date. Miners agree on the smart contract's execution conclusion and update the blockchain accordingly. Each smart contract is given a 160-bit address after it is deployed, and it is run anytime a transaction is created using this address. It's possible that the smart contract's storage will be updated while it's being executed (i.e., reading from or writing to the storage).

A smart contract can also be used to swap bitcoin between users. Furthermore, by publishing a message that is not recorded in the blockchain, a smart contract can activate and establish another smart contract. Smart contracts utilise this message to either create a new smart contract or to call functions in other smart contracts. Ethereum is a permission sless blockchain and money, similar to Bitcoin. It allows you to design and run complicated apps based on smart contracts on the blockchain, in addition to transferring money. Ether is Ethereum's native currency. The account is the Ethereum system's fundamental unit. Externally owned accounts and contract accounts are the two types of accounts in Ethereum. The former maintains a balance by being controlled by the owner's private key. It can also be used to make money transfers or to start a smart contract. The latter has balance, storage, and state and is managed by smart contract code logic. The Ethereum virtual machine, which executes smart contracts, lies at the heart of Ethereum. A smart contract's source code is compiled into bytecode, which the Ethereum virtual machine can understand. To facilitate the execution of smart contracts and maintain blockchain consensus, each Ethereum node executes the identical instructions. Many Turing-complete languages, such as Solidity, can be used to create Ethereum smart contracts. As part of a blockchain transaction, a smart contract is installed or performed on the system.

LITERATURE REVIEW

Maher Alharby, Amjad Aldweesh [1] studies Smart contracts, which are based on the blockchain, are computer programmes that codify an agreement between non-trusting parties. If specific criteria are met, smart contracts are performed on a blockchain system without the need for a trusted third party. In recent years, blockchains and smart contracts have gotten a lot of interest, including from academics. We conduct a comprehensive mapping assessment of all peer-reviewed technology-oriented smart contract research. Our goal is to give a review of the scientific literature as well as to detect academic research trends and adoption. We exclusively look at peer-reviewed scientific articles to see how academics have embraced smart contract technology and produced established scientific outcomes. We gathered all research papers from the major scientific databases and identified 188 that were relevant utilising the systematic mapping method. Security, privacy, software engineering, application, performance & scalability, and other smart contract-related subjects were divided into six areas. The majority of the articles (approximately 64 percent) and software engineering (21 percent) come into the application and software engineering categories, respectively. We found that the number of relevant papers has increased by nearly eightfold since our 2017 study and that the focus has changed significantly toward smart contract applications.

ARCHITECTURE

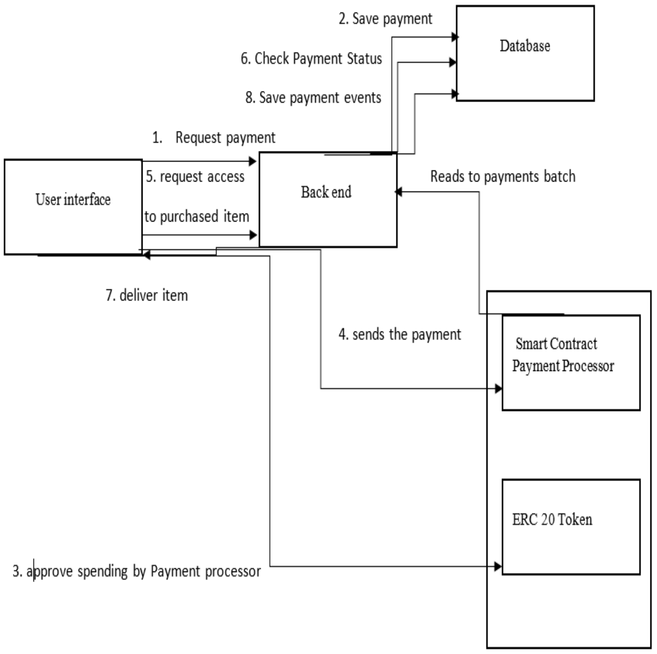


Figure 1: Smart architecture

1. User interface: The website is built using React, which allows developers to create a user interface (UI) that adheres to module standards. For example, there are two websites with a text form that perform the same function but have distinct features. Due to the changes in the text forms, when the customer clicks a link and visits another page, the page will still re-render the text form. If the development team creates a UI module standard and then picks the text form from the module to apply to various pages, the text form will not be re-rendered since React will identify that the two forms are identical and will not alter them. In short, React not only revolutionises front-end programming, but it also establishes a new standard in user interface design and development.

2. Database: Data is stored in the blockchain container using mongodb. MongoDB is a web-based database management system. It's a NoSQL database that's built on documents. The data model and persistence mechanisms are designed for high read and write throughput, as well as easy scaling and failover. MongoDB's document data model makes it simple to build on because it supports unstructured data out of the box and does not necessitate costly and time-consuming migrations when application requirements change. BSON is a JSON-like format used by MongoDB to store documents. BSON is a lightweight, quick, and traversable language that is a perfect fit for modern object-oriented programming approaches MongoDB's document network transfer format is BSON. BSON appears to be similar to BLOB at first glance, but there is one key difference: the MongoDB database understands BSON internals. This means that MongoDB can use dot notation to reach inside BSON objects, including nested ones. MongoDB may use this to create indexes and match objects to query expressions on both top-level and nested BSON keys. MongoDB also supports full indexes and rich queries. This distinguishes it from other document databases that handle complicated queries through a separate server layer. Automatic sharding, replication, and convenient storage are among its other characteristics. The growing popularity of MongoDB, as well as the vast amounts of sensitive user data kept in these databases, raises questions about the data's confidentiality and privacy, as well as the security provided by these systems. When MongoDB was first created, security was not a top priority for its creators.
3. Backend: Node.js paved the way for Full Stack Developers, who can now manage both the server and client sides independently. Due to its event-

driven, non-blocking, and asynchronous techniques, Node.js is quick and dependable for huge files and heavy network demand applications. Developers can also maintain whole projects in single pages (SPA) and utilise it for IoT. The study's findings are based on a survey and a literature evaluation of Node.js implementation areas and obstacles. Finally, I'll offer suggestions on how to improve in order to overcome the obstacles.

4. Tether: Coins that are stable The exact definition of a stablecoin, like e-money in the 1990s, is now in the eye of the beholder, owing to the lack of established rules and standards governing stablecoins today. Stablecoins are "digital units of value that differ from existing forms of currencies (e.g. deposits, e-money, etc.) and rely on a set of stabilisation methods to limit swings in their price against a currency, or basket thereof," according to the European Central Bank (ECB). 15 The ECB, like many others, believes that the word used to represent this digital payment innovation is imprecise and even deceptive. In actuality, the Financial Action Task Force (FATF) believes that "the term'stablecoin' is essentially a marketing phrase used by advocates of such currencies, rather than a defined legal or technical category." 16 Monetary authorities, such as the BIS, now use the term "so-called stable coins" to mistakenly accept these claims.

5. Solidity (Truffle): It is an Ethereum Blokchain Development Environment, Testing Framework, and Asset Pipeline. It has the following features: Smart contract compilation, linking, deployment, and binary management are all built-in. Framework for deployment and migrations that is scriptable and flexible. For deployment to any number of public and private networks, network administration is required. Contract testing that is automated for speedy development.

Steps for smart contract:

1. The payment id is generated by the UI using the API.

2. The payment id is saved in the mongo db database by backends.

3. The UI approves the request by sending it to the ERC 20.

4. The payment is sent to the smart contract.

5. It reads and configures the events after getting the payment id, then updates the events in the Mongo db.

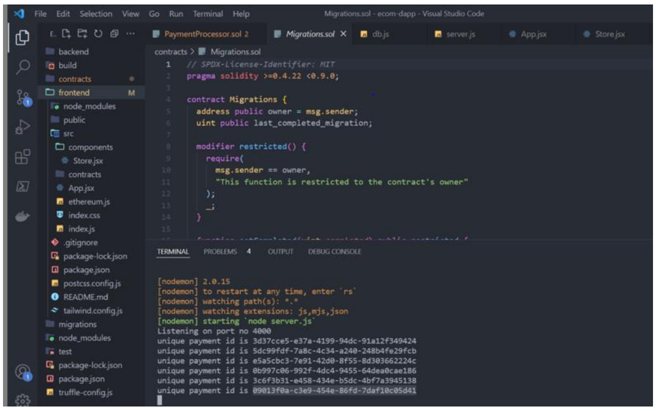
6. Make API requests to the back end for the item, then configure the back end with the MongoDB database.

7. They deliver the thing to the consumer once the item and payment id are matched.

8. Finally, keep the payment id for future reference.

9. We can see that data authentication is done by configuring the payment id. Without the payment id, the web cannot access any item requests.

RESULTS



```
// SPDX-License-Identifier: MIT
pragma solidity >=0.4.22 <0.9.0;

contract Migrations {
  address public owner = msg.sender;
  uint public last_completed_migration;

  modifier restricted() {
    require(
      msg.sender == owner,
      "This function is restricted to the contract's owner"
    );
    _;
  }

```

```
[nodemon] 2.0.15
[nodemon] to restart at any time, enter `rs`
[nodemon] watching path(s): *.*
[nodemon] watching extensions: js,mjs,json
[nodemon] starting `node server.js`
Listening on port no 4000
unique payment id is 3d37cce5-e37a-4199-94dc-91a12f349424
unique payment id is 5dc99fdf-7a8c-4c34-a240-248b4fe29fcb
unique payment id is e5a5cbc3-7e91-42d0-8f55-8d303662224c
unique payment id is 0b997c06-992f-4dc4-9455-64dea0cae186
unique payment id is 3c6f3b31-e458-434e-b5dc-4bf7a3945138
unique payment id is 09013f0a-c3e9-454e-86fd-7daf10c05d41
```

Figure 2: Unique payment id generation.

In the Figure 1(architecture) we have seen that payment id block and how payment id is generated . In above figure (screenshoot of the unique id generation while transaction made by the user) we can use these for the purpose of the data authentication which is verified in the (mongodb)database and with user transaction.

For example: Payment is made initiated by the user, it will open the wallet to pay and after payment is successful done it will send the payment id to the mongodb. Then mongodb (transaction or payment id) is read by the admin, hence they will send the product or message that (your product is available for you or thank you for donation).

CONCLUSION

We conclude that we have seen numerous sorts of block chain mining in the paper, and we can understand that mining is required for the block chain to secure transactions by discussing various scenarios in the article. There are now three mining companies working on implementing and solving the mathematical puzzle. Future work will be based on the presented model, which states that AI mining is a novel concept that will be more efficient and successful than the other three mining methods.

REFERENCES

[1] Mining Process in Cryptocurrency Using Blockchain Technology: Bitcoin as a Case Study Ahmad Abdullah Aljabr1, Avinash Sharma2, Kailash Kumar1 Journal of Computational and Theoretical Nanoscience Vol. 16, 4293–4298, 2019.

[2] An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang 2017 IEEE 6th International Congress on Big Data.

[3] David Easley, D., O'Hara, M. and Basu, S., 2019. From mining to markets: The evolution of bitcoin transaction fees. Journal of Financial Economics, 134(1), pp.91–109.

[4] A Generalised logical architecture for blockchain technology, Jared Newell*, Quazi Mamun*, Sabih ur Rehman* and Md Zahidul Islam* *School of Computing, Mathematics and Engineering, Charles Sturt University Australia, A preprint October 20, 2021.

[5] Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research Article in IEEE March 2021 DOI: 10.1109/ACCESS.2021.3068178.

[6] Blockchain technology forecasting by patent analytics and text mining Seyed Mojtaba, Hosseini Bamakan a,b, , Alireza Babaei Bondarti , Parinaz Babaei Bondarti, Qiang Qu, //doi.org/10.1016/j.bcra.2021.100019; 20 June 2021 2096-7209/,2021, Elsevier B.V. on behalf of Zhejiang University Press.

[7] Blockchain-enableddecentralized identity management: The case of self-sovereign identity in public transportation, Lukas Stockburger, Georgios Kokosioulis, Alivelu Mukkamala, Raghava Rao Mukkamala,Michel Avital, /10.1016/j.bcra. 2021.; Accepted 7 May 2021 2096-7209/ 2021 Elsevier B.V. on behalf of Zhejiang University.

[8] Blockchain: Research and Applications Magda Foti * , ManolisVavalis, doi.org/10.1016/j.bcra.2021.100008 February 2021 2096-7209/© 2021, Elsevier B.V. on behalf of Zhejiang University Press.

[9] BlockHDFS: Blockchain-integrated Hadoop distributed file system for secure provenance traceability Viraaji Mothukuri a , Sai S. Cheerla, Reza M. Parizi , Qi Zhang ,Kim-Kwang-RaymondChoo, https://doi.org/10.1016/j.bcra.2021.100032,October 2021

[10] ABCDE—agile block chain DApp engineering Lodovica Marchesi, Michele Marchesi, Roberto Tonell, https://doi.org/10.1016/j.bcra.2020.100002,26 November 2020 2096-7209/© 2020, Elsevier B.V. on behalf of Zhejiang University Press.

[11] Research – A blockchain of knowledge, Jens Ducree,

https://doi.org/10.1016/j.bcra.2020.100005, December 2020