A Novel Integrated Strict Verification of Smart Contracts on Blockchain

B. Aarthi, Rahul Kumar, Abhishek, Rahul Kumar

Abstract: Blockchain is an evolving technology which helps in keeping records and process transactions in decentralized manner. Blockchain is considered as safest medium because of its decentralized nature and many protocols, algorithms which it follows to make sure that transaction are immutable. Blockchain concept basically uses BZT theorem, this is considered as one of secured algorithm to predict secure results. however formal verification approach for the smart contract is still the best way to perform verification. In our paper, we have depicted various algorithm according to which we can verify the smart contract in best possible way.

Keywords: Smart Contracts, Blockchain, Formal Verification, BZT (Byzantine Fault Tolerance).

I. INTRODUCTION

Smart contract is basically a way to interact between the different parties which agree on the code of smart contract. There may be the case that people may not trust each other but they can trust the machine which runs over the code. smart contract works basically like a code of agreement between two or more smart contract interacting parties. These are a set of self executable codes. the codes in smart contracts are immutable which means once party agrees to specific condition and the deal is locked through smart contract then none can make changes to that since the transaction block is proceed. In an existing system, blockchain security provides a safe haven. Secure data source provides reliable data to ensure secure execution. A contract made by contract participants needs to fully express the purpose. Thereafter, applying the formal reservations and formal guarantees to the above-mentioned contract, which is an analytical process. Through multiple behavioural modelling and smart Contract, we can validate whether the attributes meet the contract requirement or not.

II. MODULE INVOLVED IN SMART CONTRACTS

A. Hash Identifier

The Hash identifier is a hash (key) of data through cryptography, the point of which is where the data is stored. So by using the hash pointer we can check whether the data is reduced or not.

The block chain is organized in this way using hash pointers to link the blocks of data together. With the hash pointer pointing to the front block, each block displays the address where the original block data is stored.

B. Digital Signature

The digital signature establishes the authenticity of the data collection through the cryptographic algorithm. It is a control scheme that data should not be disturbed. There are three key components that define a digital signature system.

C. Risk Scan

Vulnerability scanning is a risk assessment that has been identified, which was intended to avoid similar errors. It uses to identify potential risks when contracting, which is important to increase the safety and reliability of contractors. Using a weak scanning method we can easily identify the risks to an agreement while performing it.

III. ADVANTAGES OF PROPOSED SYSTEM

- Less verification numbers and higher verification efficiency.
- Increases the speed of transaction verification
- Joint optimization scheme are secure and efficient
A Novel Integrated Strict Verification of Smart Contracts on Blockchain

- Achieved a nodal authentication and verification of the transmitted data

IV. TECHNOLOGY USED

- Backend Technologies
  - Python
  - Postmen
  - Spider
  - Eclipse IDE

- Frontend Technologies
  - Web Technologies
  - Bootstrap

V. ARCHITECTURE

VI. ADVANTAGES OF PROPOSED ALGORITHM

- It looks great, making it suitable for a variety of applications.
- High Speed - Actions are processed faster compared to PoW.
- Low power consumption as there is no need for supercomputers.

VII. FUTURE RESEARCH DIRECTIONS

Recently smart contracts have become an essential component of all applications and there is an important role to solve complex business issues but many research directions are futile some of which stand next. Resiliency against Hybrid Attacks.

- Suitable platform for IoT objects
- Security Privacy Policies
- Trust and Trust Management on Social Networks
- Ining Mines that work well with Smart Energy
- Establishment of Hybrid Consensus Protocol

VIII. RESULTS AND DISCUSSION

In our paper, we shed some light on the behavior of smart contracts when taken over by different blockchain platforms. We analyzed disability and various compliance policies. We also highlighted the positive contractual relationship between blockchain and IoT with an emphasis on opportunities and challenges. The discussion also focuses on future research directions. We found that the integration of Blockchain and IoT with the Smart contract could provide solid frameworks for new business communities and implement distributed systems (DApps).

However, as there are still many problems and limitations with smart languages and contracts. Many applications based on Blockchain-IoT technology are difficult to handle right now. We plan to take concrete for more research on smart contracts in the future.

IX. CONCLUSION

The proposed system, is the actual verification of smart contracts operating on distributed ledgers such as blockchain. Currently, methods can only handle simple smart contracts and simple models, and are not suitable for complex contracts. The proposed system facilitates the use of systematic analysis and formal validation by looking at the technical layers and their security issues. We have selected three layers, implementation, law and language, as targets for using systematic analysis. It proposes a framework for applying systematic analysis to each layer by applying existing levels and outcomes.

REFERENCES


AUTHORS PROFILE


Rahul Kumar, is doing his B.tech in CSE stream at SRM Ramapuram, Chennai. He has worked on multiple projects in various domains including web designing, and blockchain. He has published paper on “Chatbot embedded in android system” (ISSN:2349-5162) in JETIR in volume 5 Issue 10, page no.-853-857, October 2018.