EasyChair Preprint

№ 2943

A novel Integrated strict verification of smart contracts on Blockchain

B. Aarthi, Rahul Kumar, Abhishek and Rahul Kumar

March 12, 2020

A novel Integrated strict verification of smart contracts on Blockchain

B. Aarthi, Assistant professor,(SRMIST Ramapuram, Chennai),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 the 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.

Index Terms—Smart Contracts, Blockchain, Formal verification,BZT (Byzantine fault tolerance method)

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 the existing system, the blockchain security provides a secure execution environment. The secure data source provides the credible data to ensure the secure execution.

The contract made by contract participants needs to fully express the intention. of the makers and comply with the law. Then, implementing formal specification and formal verification on above established contract, which is an iterative 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 CONTRACT

Hash pointer:-

Hash pointer is a hash(key) of the data by cryptography, its point to the location in which data is stored. Hence by using hash pointer we can check whether the data has been tampered or not. A block chain is organized in such a way using hash pointers to link data blocks together. With the hash pointer which pointing to the pre block, each block indicates the address where the data of the pre block is stored.

Digital Signature:-

A digital signature establishes the validity of a set of data by using a cryptographic algorithm. It is also a scheme for regulating that data should not been tampered with. There are three core components that define a digital signature system. The first component is the key generation algorithm, which use to creates two keys, one of it is used to sign messages and to kept privately and called the private key, and the others are made easily available to the public system, thus called the public key, used to validate whether the message has the signature signed with the indicating the private key or not.

Vulnerability Scanning:-

Vulnerability scanning is the study of vulnerabilities which has been discovered, which aimed at avoiding the same mistakes. It use to discover potential vulnerabilities in the execution of contracts, which is important to maximize the level of security and credibility of contracts. Using vulnerability scanning method we can easily detect the possible vulnerabilities in contract while executing.

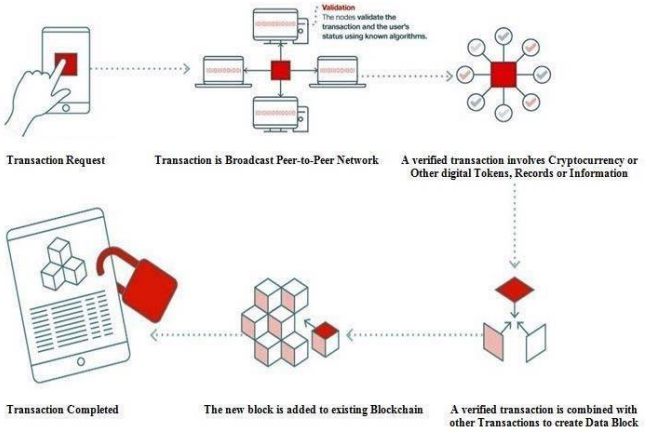
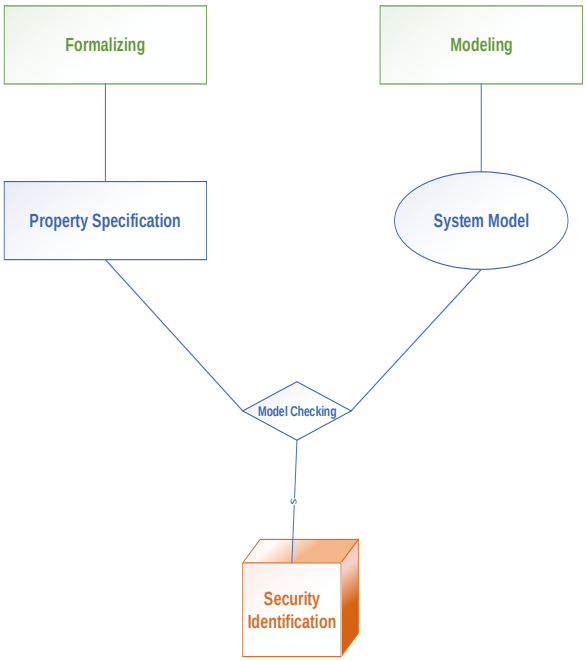


Fig. 1. How Blockchain Works

III. ADVANTAGES OF PROPOSED SYSTEM

- Less verification numbers and higher verification efficiency.
- Increases the speed of transaction verification
- Tool-aided formal verification is strong approach to check the correctness of code
- Joint optimization scheme are secure and efficient
- Achieved a nodal authentication and verification of the transmitted data

IV. ARCHITECTURE



V. TECHNOLOGY USED

Backend Technologies

- Python
- Postmen
- Spider
- Eclipse IDE

Frontend Technologies

- Web Technologies
- Bootstrap

VI. ADVANTAGES OF PROPOSED ALGORITHM

- It's highly scalable, making it suitable for a variety of applications.
- Higher speed – Transactions are processed faster compared to PoW ·
- Lesser energy consumption as there is no need for supercomputers

VII. FUTURE RESEARCH DIRECTIONS

Recently the smart contracts are emerging key feature of every decentralized application and playing prominent role to solve complex business logics but many research directions are vacant in future some of them are as follows.

- Resiliency against Hybrid Attacks
- Optimal Platform for IOT objects
- Security and Privacy Auditing Protocols
- Trust and Reliance Management in Social Networks
- Smart Energy-efficient Mining
- Innovation of Hybrid Consensus Protocols

VIII. CONCLUSION

The proposed system, actual verification of smart contracts running on distributed ledgers such as blockchain. Currently, the approaches can only handle simple smart contracts and simplified models,

and are not suitable for complex contracts. The proposed system facilitates the application of formal analysis and formal verification by considering technology layers and their security concerns. We picked three layers, implementation, protocol and language, as targets of applications of formal analysis. It proposes a framework to apply formal analysis to each layer by using existing standards and results.

REFERENCES

I. D. Vujičić, D. Jagodić, and S. Randić, ''Blockchain technology, bitcoin, ¯ and Ethereum: A brief overview,'' in Proc. 17th Int. Symp. INFOTEHJAHORINA (INFOTEH), Mar. 2018, pp. 21–23.

II. K. Finley. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Accessed: May. 18, 2019. [Online]. Available: https://www.wired.com/2016/06/50-million-hack-just-showed-daohuman/

III. Z. Zheng, S. Xie, H. Dai, and H. Wang, ''An overview of blockchain technology: Architecture, consensus, and future trends,'' in Proc. IEEE Int. Congr. Big Data, Big Data Congr., Honolulu, HI, USA, Jun. 2017, pp. 557–564

IV. N. Atzei, M. Bartoletti, and T. Cimoli, ''A survey of attacks on ethereum smart contracts (SoK),'' in Proc. Int. Conf. Princ. Secur. Trust, Apr. 2017, pp. 164–186. doi: 10.1007/978-3-662-54455-6_8.

V. M. Alharby and A. V. Moorsel, ''Blockchain-based smart contracts: A systematic mapping study,'' in Proc. Int. Conf. Artif. Intell. Soft Comput., Aug. 2017, pp. 125–140. doi: 10.5121/csit.2017.71011.