Distributed Architecture for Secure, Attack-Resilient Crypto Currency Transactions for the Classified Temporal and Text Data

Challa Narasimham

Abstract: ***In the digital world, the crypto currency has to do with the use of tokens based on the distributed ledger technology in a secure manner. Crypto currency can be a resource on a block chain network or can be seen as a tool to perform the transactions ensuring the privacy and security. Data may be available in temporal or text format. This paper describes about the distributed architecture for secure and attack-resilient bit coin-based crypto currency transactions for classified temporal and text data. The temporal data may be voice, sound or graphical information basing on the time series. If the data available is temporal this work describes about how it can be classified into a processed form. In this context, this paper describes the process of converting temporal data into text data. Further, the paper describes about the process of ensuring the security. This paper describes about the methodologies of cryptography-based hashing, attack-resilient nonce generation and verifiable encryption techniques for the construction of resilient transactions against stealthy data-integrity attack.***

Keywords: *Classification, Crypto currency, Hashing, Nonce, Temporal Data, Transactions, Verifiable encryption.*

I. INTRODUCTION

Now a day's majority of the applications like e- transactions performing over internet. Billions of operations that are taking place over digital systems. At the same time threats are also increasing in enormous way. One side technology is growing the other side it is enviable to come up with security measures to ensure the transactions over internet. In the digital system crypto-currency a specially designed data structure and transactions.

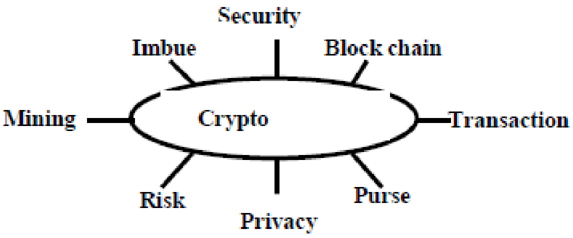


Fig. 1. Crypto currency data structure

Data can be text data, temporal data. Data available in the form of text from other sources, on the other hand it can be temporal. Temporal data refers to data changes over time. It can be represented by its general form

td = fun(time));

and for a discrete time stamps ts, this can be in the form

$td_i = fun(ts_i);$

Data can be classified to identify, manage and protect the information by representing as a layered security to protect itself against advanced persistent Threats from the outside world.

II. EXISTING SYSTEM

The block chain is the distributed registry of bit coin entities. It is recurrently developing as miner and appends new blocks to document the updated negotiations. These blocks are updated to the block chain in a linked list manner. The pass around blocks linked to the Bit coin network.

Block chain technology has been used for the bit coin as a digital currency. The block chain is the name of the technology behind of Bit coin. Technically the block chain is similar to a database, except that interactions with them differ. A public distributed ledger of all block chain transactions or digital events that have been executed and shared among the participating parties across peer-to-peer networks. The bit coin system transactions by them in groups called blocks and then linking these blocks. The transactions in a single block are considered to have happened at the same time. These blocks are linked to each other (like a chain) in a linear, chronological order, with every block containing the hash of the previous block.

III. PROPOSED PROCEDURE

The following is proposed to orvide distributed architecture for secure, attack-resilient transcations.

a. Classify the temporal data into text file
b. Temporal to text data conversion using classifier
c. Data Conversion using SHA256
d. Nonce generation
e. Verifiable Encryption
f. Mining

A. Architectural Design

The work proposes to integrate the transaction and security as well as to protect from threats and disturbances by using block chain Technology. The project focuses on adaptive featured dynamic hash algorithms for the cyber-secure data transactions in the Block-chain models. It is proposed to demonstrate the efficacy of security and privacy of crypto currency data transactions for the Bit coin application.

Revised Manuscript Received on August 05, 2019.

Challa Narasimham , CSE, Vignan's Institute of Information Technology,

Step1: Conversion of Temporal data to text data

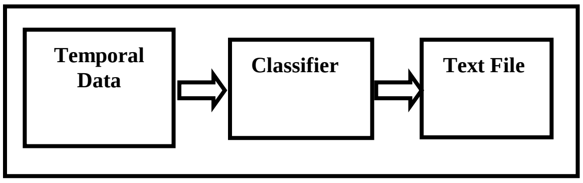


Fig. 2.a. Conversion of temporal data to text data

Step2: Temporal Data to Text

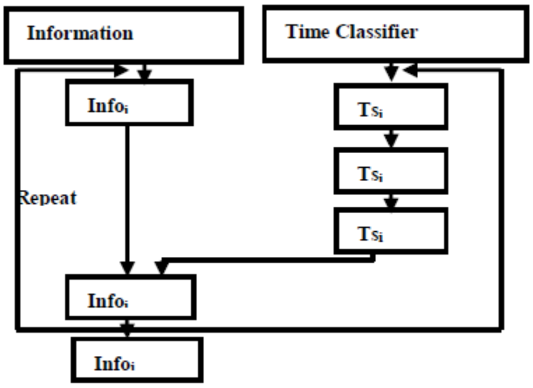


Fig. 2. b. Conversion of temporal data to text data

Step3: Generating crypto currency

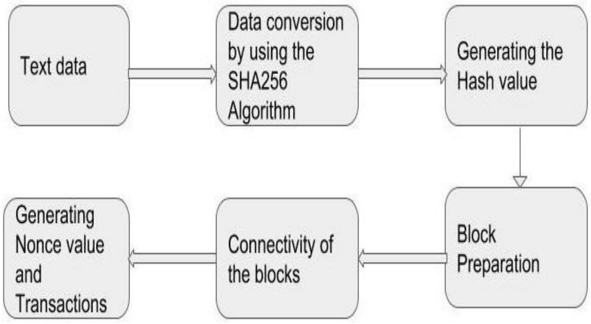
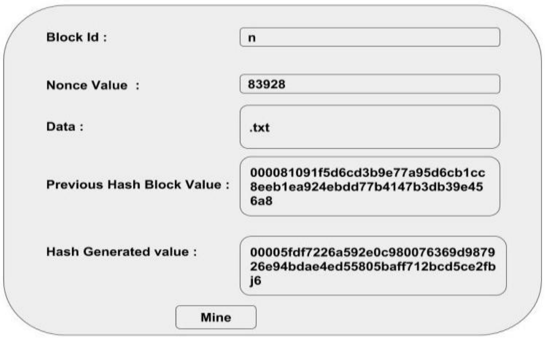

Text data
Data conversion by using the SHA256 Algorithm
Generating the Hash value
Block Preparation
Connectivity of the blocks
Generating Nonce value and Transactions

Fig. 3. a. Crypto currency transactions

Step 4: Transactions


Block Id : n

Nonce Value : 83928

Data : .txt

Previous Hash Block Value : 000081091f5d6cd3b9e77a95d6cb1cc8eeb1ea924ebdd77b4147b3db39e456a8

Hash Generated value : 00005fdf7226a592e0c980076369d987926e94bdae4ed55805baff712bcd5ce2fbj6

Fig. 3. b. Crypto currency transactions

Step 5: Data Conversion to generate Hash value

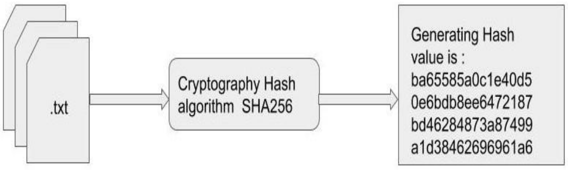

.txt
Cryptography Hash algorithm SHA256
Generating Hash value is : ba65585a0c1e40d50e6bdb8ee6472187bd46284873a87499a1d38462696961a6

Fig. 4. Generating Hash value

IV. BLOCK PREPARATION

A block stores the transactions that have not yet entered any prior blocks. Each and every block contains the Block no, Nonce, Data – Transaction, Previous Hash value and generated hash value. The block chain facilitates a highly distributed ledger for accessing transactions, attributing them to a specific node in a network, and ordering them in time. Data is permanently recorded in the network system through files called blocks. A block is a record of some or all of the most recent transactions that have yet to be recorded in prior blocks.

The log book of predecessor is known as block chain. A block consists of block body and block header. The block header contain of three sets of block metadata. First, there is a link to a predecessor block hash value. Second set of metadata, namely the difficulty, nonce, in the case of bit coin, relate to the mining competition. The last piece of metadata is the Markel tree root, a data structure used to efficiently specify all the transactions in the block, which contains a set of transactions divided into I/O.

A. Connectivity of blocks

It is a collection of encrypted annals. The block connected the hidden hash of the earlier block and transactional data. Transactions are set together in blocks and then included in the block chain. It is a data structure containing linked blocks of transactions, and it can be stored as a simple database. The block having the selection of predecessor block to generate a chain that connects the propagation block to the present block. It is identified by the hash of its header, which is generated using Cryptographic algorithm.

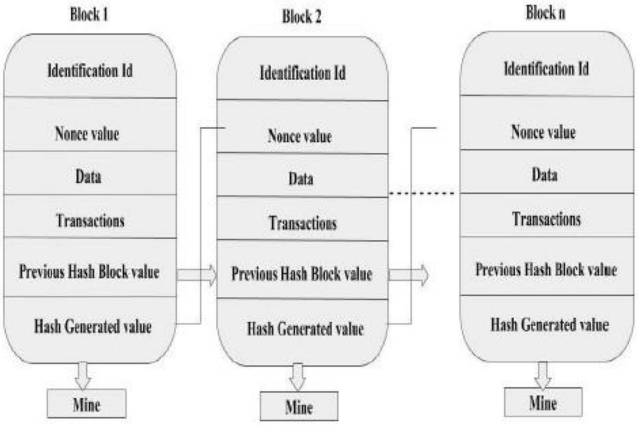


Fig. 5. Block Chaining

V.VERIFIABLE ENCRYPTION

PROVER

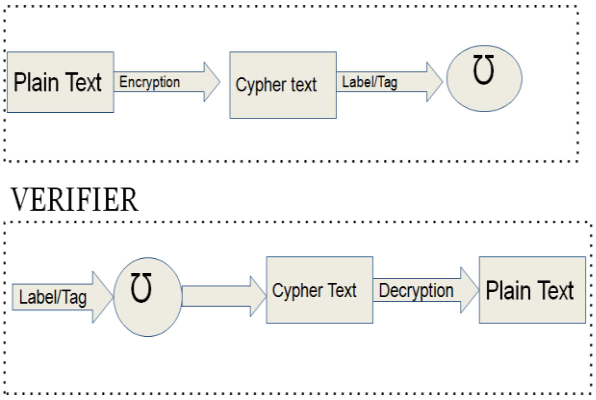


Fig. 6. Verifiable Encryption for transaction

VI. TRANSACTION IMPLEMENTATION

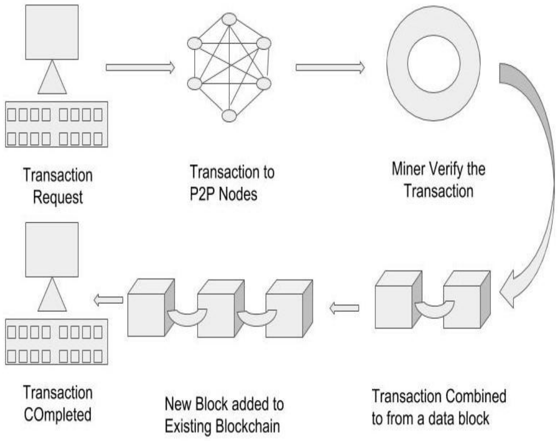

Transaction Request
Transaction to P2P Nodes
Miner Verify the Transaction
Transaction COmpleted
New Block added to Existing Blockchain
Transaction Combined to from a data block

Fig. 7. Secure, attack-resilient transaction

VII. CONCLUSION

The paper described the process of classifying the temporal data, privacy and security of transactions. With the practical implementation of the verifiable encryption it was found that the better security could be achieved by this adopted methodology. The security and privacy process implemented was by generating the Nonce value and the hash value.

Nonce generated value would be used to add an extra layer of security to transactional data which is converting in to the hash value. It would be implemented using verifiable encryption. Further, the bit coin transaction process has been implemented by the public and private key that is through verified signature and mining process.

REFERENCES

1. Camenisch, J. and I. Damgård (2000) “Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes”.
2. 2. Camenisch, J. and V. Shoup (2003). “Practical verifiable encryption and decryption of discrete logarithms.” pp 126–144.
3. C. Cachin, K. Kursawe, V. Shoup, Practical Asynchronous Byzantine Agreement Using Cryptography, 1999.
4. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Block chain Technology: Architecture, Consensus and Future Trends".
5. M. Sato, S. Matsuo "Long-Term Public Block chain: Resilience against Compromise of Underlying Cryptography".
6. H. Halpin, M. Piekarska, "Introduction to Security and Privacy on the Block chain".
7. 7. P. Geurts, “Pattern extraction for time series classification”, 2001.
8. M. S. C. Kadous “Classification of multivariate time series and structured data using constructive induction,” Machine Learning, vol. 58, no. 2-3, p. 179–216, 2005.

AUTHORS PROFILE

Challa Narasimham, Professor of Computer Science Engineering & Dean IQAC and Former Principal of Vignan’s Institute of Information Technology have been working in the field of Teaching and Research for the last 24 years. The Author received Ph D in Computer Science in the year 2009. Guided three Ph D scholars and guiding four research scholars. Published 79 research articles in various National and International journals. At present, registered for Post-Doctoral work leading to D. Sc with UoS Panama and doing work in the area of verifiable encryption, cryptography and security.