**CRYPTO CURRENCY BASED BANKING SYSTEM WITH BLOCKCHAIN**

Karuppasamy.K 1, Muniyappan.R 2, Murugesan.K 3, ShanthiPriya.D 4

1 Research Student , Computer Science And Engineering, N.S.N College Of Engineering & Technology, Karur ,Tamilnadu, India

2 Research Student , Computer Science And Engineering, ,N.S.N College Of Enggineering & Technology, Karur, Tamilnadu, India

3 Research Student , Computer Science And Engineering, ,N.S.N College Of Enggineering & Technology, Karur, Tamilnadu, India

4 Assistant professor , Computer Science And Engineering, ,N.S.N College Of Enggineering & Technology, Karur, Tamilnadu, India

**ABSTRACT**

 Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. So in this project we can implement Bit Coin based banking system can be implemented using Block chain technology to create hash functions. In a Bit coin transaction, block chain will create an interconnection between all users connected to network and every time when entering a transaction to the network after validating it will broadcast to other users and also network will have a copy of every transaction. Instead of saving any transaction in the block chain, the network will bundle transaction information into a block and it will broadcast into the network. Each and every block link to the previous block this chain will trace to the first block which is called genesis block

**Keywords:** Crypto, Blockchain, Transaction, Chain, Hash

**1. INTRODUCTION**

 A block chain is a distributed database that is shared among the nodes of a computer network. As a database, a block chain stores information electronically in digital format. Block chains are best known for their crucial role in cryptocurrency systems, such as maintaining a secure and decentralized record of transactions. The innovation with a block chain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party. One key difference between a typical database and a block chain is how the data is structured. A block chain collects information together in groups, known as that hold sets of information. Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the block chain. All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled. A database usually structures its data into tables, whereas a block chain, like its name implies, structures its data into chunks (blocks) that are strung together. This data structure inherently makes an irreversible time line of data when implemented in a decentralized nature. When a block is filled, it is set in stone and becomes a part of this time line. Each block in the chain is given an exact time stamp when it is added to the chain.

**2. METHODOLOGY**

**2.1 EXISTING SYSTEM**

A credit network models trust between agents in a distributed environment and enables payments between arbitrary pairs of agents. With their flexible design and robustness against intrusion, credit networks form the basis of several Sybil-tolerant social networks, spam-resistant communication protocols, and payment systems. Existing systems, however, expose agents’ trust links as well as the existence and volumes of payment transactions, which is considered sensitive information in social environments or in the financial world. This raises a challenging privacy concern, which has largely been ignored by the research on credit networks so far. Privacy preserving standards have been created recently because sensitive information is now frequently stored on computers that are attached to the Internet. Also many tasks that were once done by hand are carried out by computer; therefore there is a need for Information Assurance (IA) and security. Privacy preserving is an important in order to guard against identity theft. Businesses also need security because they need to protect their trade secrets and proprietary information. Cyber-terrorism is one of the major terrorist threats posed to our nation today. As we have mentioned earlier, this threat is exacerbated by the vast quantities of information now available electronically and on the web. Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher text and obtain an encrypted result which decrypted matches the result of operations performed on the plaintext. For instance, one person could add two encrypted numbers and then another person could decrypt the result, without either of them being able to find the value of the individual numbers.

**2.2 DISADVANTAGES**

* Unauthorized person can view the details easily. So security was less
* Maintain the details in single server
* Need large amount of storage space for store the encrypted data.
* Easily hack the details.

**2.3 PROPOSED SYSTEM**

With the advent of communications techniques, e-commerce as well as online payment transactions are increasing day by day. Along with this financial frauds associated with these transactions are also intensifying which result in loss of billions of dollars every year globally. Also the various types of benefits like cash back, reward points, interest-free credit, discount offers on purchases made at selected stores, and so forth tempt the customers to use credit card instead of cash for their purchases. The major problem for e-commerce business today is that fraudulent transactions appear more and more like legitimate ones and simple pattern matching techniques are not efficient to detect fraud.  Using a public ledger, bit coin is transacted as crypto currency in this decentralized system. Here implement hybrid keyboard method is implementing to address the problem of shoulder-surfing attacks on authentication schemes. This is a PIN-based authentication method that operates on touch screen devices. Hybrid keypad uses the technique to blend two keypads with different digit orderings in such a way, that the user who is close to the device is seeing one keypad to enter the PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad. In the bit coin, blockchain establishes a decentralized consensus about the order of transactions among a large number of members who need not to know or trust anyone. Furthermore, each block references the hash of the previous block. This establishes a link between these blocks, thus, it creates a blockchain.

Then, by combining peer-to-peer network, cryptographic algorithm, distributed data storage and a decentralized consensus mechanism, blockchain technology provides a way for people that record in a secure and verifiable manner, and it can prevent double spending effectively. Bit coin is a crypto currency, which is not backed by any country's central bank or government. Design the system for banking system with improved security. Implement block chain technology to split the details in the form of blocks. All transactions are done with help of crypto currency format.

**2.4 ADVANTAGES**

* Unauthorized person difficult to hack the details
* Maintain the details in multiple blocks
* Reduce amount of storage needed
* No one can use or guess the details

**3. MODELLING AND ANALYSES**

A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.

****

**Figure 1:** System Architecture

**4. RESULTS AND DISCUSSION**

The proposed framework implemented in Python Framework as web application in banking sectors. The currency and Block chain storage as shown in below figure. Today Banking environment faced with issues like rising cost of operations, fraudulent attacks on centralized servers and ensuring transparency of the transactions. Most of the banking transactions depend on manual processing and documentation, involve with intermediaries and time consuming. Blockchain provides solutions for banks as it helps to eliminate intermediaries’ transactions and facilitates real-time cryptography transactions. So most of the banks adopted this technology and increased their profit. Following evaluation factors such as block generation time state process of creating blocks with in efficient manner. It also shows the performance of proposed blockchain technology.

**5. CONCLUSION**

As the crypto currency market continues to expand, secure and stable key management is becoming more and more important. This article focuses on designing a decentralized crypto currency key management scheme. Compared with local management and central management, decentralized management can avoid risk aggregation and make use of the whole network storage resources. The primary goal of data privacy is the protection of personally identifiable information. In general, information is considered personally identifiable if it can be linked, directly or indirectly, to an individual person. Thus, when personal data are subjected to mining, the attribute values associated with individuals are private and must be protected from disclosure. Miners are then able to learn from global models rather than from the characteristics of a particular individual. In this project, we can conclude that the proposed system provided net banking interface to access the all transactions in crypto currency format and secure the transactions using Block chain technology.

**6. REFERENCES**

[1] Taleb, Nasser. "Prospective applications of blockchain and bitcoin cryptocurrency technology." TEM Journal 8, no. 1 (2019): 48-55.

[2] Verma, Manish. "Emerging applications of blockchain technology." International Research Journal of Modernization in Engineering Technology and Science 3, no. 4 (2021): 1258-1260.

[3] Sin, Edwin, and Lipo Wang. "Bitcoin price prediction using ensembles of neural networks." In 2017 13th International conference on natural computation, fuzzy systems and knowledge discovery (ICNC-FSKD), pp. 666-671. IEEE, 2017.

[4] Atsalakis, George S., Ioanna G. Atsalaki, Fotios Pasiouras, and Constantin Zopounidis. "Bitcoin price forecasting with neuro-fuzzy techniques." European Journal of Operational Research 276, no. 2 (2019): 770-780.

[5] Lin, Yu-Jing, Po-Wei Wu, Cheng-Han Hsu, I-Ping Tu, and Shih-wei Liao. "An evaluation of bitcoin address classification based on transaction history summarization." In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 302-310. IEEE, 2019.

[6] Lin, Chao, Debiao He, Xinyi Huang, Xiang Xie, and Kim-Kwang Raymond Choo. "Ppchain: A privacy-preserving permissioned blockchain architecture for cryptocurrency and other regulated applications." IEEE Systems Journal 15, no. 3 (2020): 4367-4378.

[7] Lin, Chao, Debiao He, Xinyi Huang, and Kim-Kwang Raymond Choo. "OBFP: Optimized blockchain-based fair payment for outsourcing computations in cloud computing." IEEE Transactions on Information Forensics and Security 16 (2021): 3241-3253.