International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2173101

A Secure E-wallet System Using Block Chain

Kartik Sarwan, Sanket Thore, Niranjan Satav, Pruthviraj Kamble, Dibyo Mandal
Marathwada Mitra Mandal's College of Engineering Pune, Maharashtra, India

Article Info
Volume 7, Issue 3
Page Number: 454-466

Publication Issue :
May-June-2021

Article History
Accepted : 25 May 2021
Published : 31 May 2021

ABSTRACT

In 2016, the Indian government, diode by Prime Minister Narendra Singh Modi, academic degree announced that the nations two highest-denomination bank notes would stop to be legal tenders. At the time, the two denominations accounted for roughly eighty 600 of cash in circulation in India. those that possessed the banknotes were to deposit them among the bank. With the move, the Indian government aimed to penalize tax evaders wanting back. The logic was that people with hoards of black money would have to be compelled to answer queries if they tried to deposit the demonetized banknotes. Banking and technology unit really closely associated and innovations have changed banking drastically over the number of it slow. The digital innovations among the banking sector started with the introduction of money that replaced the barter system then the gradual replacement of wax seal with digital signatures. One such troubled innovation that's dynamic the banking sector globally is Block chain Technology (BCT).

Block chain is shared distributed ledger that stores business group action to a permanent unbreakable chain which may be viewed by the parties during a group action. Block chain technology has the potential to disrupt the nancial business applications because it provides permanent and tamper proof recording of transactions during a distributed network.

Keywords - Cashless Economy, Security, Distributed Database, Visual Cryptography, Hash Algorithm

I. INTRODUCTION

Today block chain is that the buzz word within the IT market. Simply put, Block chain is that the decentralized systematically evolving public ledger of the digital records. it's well-liked as a result of, it brings trust to peer-to-peer networks and offers real privacy protection. Evolution within the block chain technology has detached new opportunities for block chain developers, in numerous domains. Block chain has the potential to disrupt major industries just like the monetary services, real state, Health care and lots of a lot of.

A. Overview of Block chain Objectives:
Describe the block chain dealing method Generate a public key and a digital signature

Generate a nowadays, a hash code, and a block chain block.
Work with a distributed system and perform transactions.

B. Block chain & its importance
Block is very important as a result of it brings trust to peer-to-peer networks solutions. A primary reason that banks had been inexistence for many years is that the act because it trustworthy third party for transactions. Block chain will operate in a very peer-to-peer fashion with zero intervention from third parties. so it eliminates the requirement of trust whereas conducting business.

C. Block Chain Definition
Block chain could be a decentralized ledger of all transactions across a peer-to-peer network. it's a technology that permits Bit coin and is additionally applied to several business processes. so bit coin is

simply one application that runs on block chain. It not solely performs transactions however additionally ensures namelessness and security of the users.

Block chains is just a series of blocks once victimization the words "Block" and "Chain" within the context mentioned higher than we tend to square measure pertaining to the digital info that is that the block keep within the public info that is that the chain.

D. History of Block chain
1990: The conception of Distributed ledgers has been around since 1990.

2009: Satoshi Nakamoto created Bit coin and introduced the conception of Block chain.
2011-2012: Crypto currency preparation in applications.
2012-2013: Currency transfer and digital payment system.
2013-2014: monetary markets and applications victimization block chain on the far side money transactions.
2014-2015: Evolution of good contracts.
2015-2016: Permission block chain network resolution.
2016-2017: Market development and exploration across industries.

II. Block Chain in Banking System

A. Current Banking System
The dealing created within the current banking system escort the no. of problems and disadvantages. contemplate associate degree example of 2 individuals do a cross- border payment.

One person, John is based in the US & John's Friend Kat is based in India. Now John wants to transfer $1000 to Kat in India. Currently the way this process works is that John will go to his bank in US and will give them a $1000 with the instructions to transfer them to Kat in India. Once the John has done the needful both John and Kat have to wait in after about 2-5 days and the amount of $1000 will reflect in Kat's bank account in India. Now let's look at some issues with this process.

B. Issues in Banking System
Apart from the time, that the process is taking, it has lot of other issues.
The presence of intermediate makes the process very expensive. Apart from the fees that is charged by every

intermediate, banks must also anchor cost for hedging to counter the volatility of currencies.

In fact, the global cross-border remains is estimated to be 20 billion dollars every year. This amount is more than the GDP of some other smaller countries in the world.

Moreover, there are innumerable cases registered were of hackers and fraudsters took over the control of the banks online systems to cipher out funds with millions of dollars, resulting in net frauds in account hacking.
Lastly situation like financial crisis puts the money at risk if it's helped by a third party organization like a bank.

C. Block chain solution for the issues

Block chain can overcome a number of these issues: Let's see how?
We already saw the how the transaction between John and Kat gets executed due to traditional banking channels.
Let's now understand how the same transaction will take place if John & Kat were using Bit coin a crypto currency powered by Block chain.

- John uses his Bit coin wallet to initiate a transaction. The amount is then send to Kat's public address which is the approval in of the bank account number in the Bit coin world.
- The amount thus gets credited almost instantaneously in Kat's wallet as supposed to take 2-5 days like a bank does.
- In the banking system, we saw that every bank maintains its own ledger and thus the bank's need to update them independently and reconcile periodically.
- The block chain on a contrary comprises of a single ledger shared among all participants. Thus no separate messaging protocol is required.
- Thus block chain is tackling the issues in traditional banking world with some of its features like Decentralized ledger, Distributed ledger, Incentives of validation, Consensus algorithm, Cryptography algorithm.

Thus banks and other financial institutions have started looking into the block chain as they want to better understand and implement this technology for various other use cases.

D. Block chain Transaction Process

- The transaction process begin with an initiation of a new transaction request which can arise from any node in a network.
- This transaction request then broadcasted throughout the network and gets picked up by various miners who are part of the network.
- Each miner picks up the transaction and runs some computations in order to validate the transaction.
- Once validated, this transaction gets added to the block and a new block is created which in turn gets added to the block chain. This is how a new transaction is completed.

III. Steps of block chain transaction

Each block chain transaction is a combination of four key features

- Cryptography Algorithm
- Decentralized Network
- Consensus Algorithm
- Distributed Ledger

A. Transaction Initiation Features of Block chain

• Cryptography Algorithm
It is an algorithm that is used to alter data from plain text readable format to cipher text protected format and that to plain text.

We all use cryptography on day-to-day basis without realizing.
Well known messaging apps use encryption. Cryptography forms one of the core aspects in block chain technology.

There are two kinds of cryptography

• Asymmetric key Cryptography
It uses two kinds of keys the public key and the private key. At any point one key is used for encryption of the message while the other is used for decryption.

• Symmetric key Cryptography
It uses only 1 key that is that the secret key used for each cryptography and decoding. The Bit coin block chain uses a biracial key cryptography so as to leverage the general public key and personal key of users to free digital signatures for initiating a dealings that is eventually propagated through the network. This digital signature provides authentication and validation to the dealings. It ensures the protection and integrity of information recorded.

B. Digital Signatures
A digital signature provides authentication and validation like traditional signatures. It ensures the

protection and integrity of information recorded on the block chain.
It uses uneven cryptography during which data may be shared employing a public key.

Primary keys square measure coupled to users providing digital signatures a top quality of non repudiation.

C. Digital Signature Creation
The signer takes the data to be transmitted and runs a Hash formula so as to come up with thirty two or sixty four bit Hash worth. This Hash worth is then encrypted victimization the signer's personal key. The result's a digitally signed document that is broadcasted into a network. Once the booster receives the digitally signed document. He decrypts constant victimization the signer's public key.

The Hash worth created when decoding is then compared with a another Hash worth regionally generated by the booster victimization constant Hash formula because the one employed by the signer.

If the Hash values square measure equal then the signature is taken into account valid and booster will then use the document.

IV. Transaction Broadcast

A redistributed network could be a system wherever play a vital role within the validation of dealings going down.

A. Types of network
• Decentralized Network

• Block chain is build upon a redistributed network which might be known by peer-to-peer connections of miners, United Nations agency play a vital role within the validation of each dealings.

• It eliminates the necessity for central authorities to control the network.

• Instead the whole management is within the hands of individual users.
• Decentralization makes the whole system truthful and secure.

• Centralized Network

Centralized network may be known by a compulsory centralized purpose which might be no heritable by a hub or a bit of hardware

through that all knowledge on a network should passed.

The current structure of net is that the best example of centralized network.

B. Consensus and its features

A accord formula is outlined as a plan from engineering that is employed to recent agreement on a particular knowledge worth once the system is distributed.

Thus accord algorithms give irresponsibleness in a very network comprising of unreliable nodes.

C. Consensus Protocol

It is a fault tolerant protocol that's wont to accomplish the required agreement on one knowledge worth or one state of network.

Fault tolerance is outlined because the ability of a system to continue operational usually within the event once a number of its parts fail.

Consensus could be a set of rules that decides on the contribution of the varied participants of the block chain.

It ensures that each one transactions occurring on the network square measure real and every one participants agree on the accord of the ledger.

D. Block chain protocols

The block chain protocol is associate degree underlying platform that holds transformative power of the bit coin.

Today block chain protocol could be a similar organic process stage wherever TCP/IP, HTTP, SMTP and numerous different protocols were be a part of their infancy.

However a significant advantage with bit coin protocol is that contrary to the first days of the first days of the net with solely a number of individuals used computers.

Today everyone has one. so the adoption of technology and disruption of the business economy and society is occurring at the breath taking speeds.

E. Features of consensus protocols

• Efficient

Efficiency that the consensus protocols offers consensus makes exchanges quicker and simpler as no third party is required.

• Security

Security is the second key feature of consensus protocol, which is ensured by not having a single point of failure.

For the hacker that hacked the block chain, he/she will need to attack countless devices at the same time in order to collect little pieces of data and put them together. This is neither practically possible nor is the advantages for the perspective of the return of investment.

• Real time

Use a peer-to-peer consensus protocols as supposed to central third party or manual offline reconciliation processes enables real time transactions.

• Reliable

Consensus protocols also makes the block chain reliable because it is impossible to tamper with the consensus of the block without being noticed including the date stamp.

This provides a non reputable statement binding or work to a point in time.

• Functional

Consensus protocol is making the bock chain more functional due to its adoption in various industries for development of new applications.
For instance, its moving the document authentication opulence by removing a step in a functional process.

V. Miners

Role of Miner in block chain

Miners are integral part of the bit coin ecosystem who ensures fairness and keep the network stable, safe and secure by improving transactions.
When a node is use an new transaction it is broadcasted to the miners in the network who validate the same.
Once validated and processed the transaction is confirmed there by allowing the recipient to receive the bit coins self to him by the initiator of the transaction.
Miners use special software to solve mathematical problems under issued.
New free headed coins in reward along with the transaction fee payed by the sender. This provides a good way to issue a new currency and create an incentive for more people to become miners.
Miners have to provide a solution to complex mathematical problems which is called proof of work.

VI. Proof of Work

It is a consensus algorithm in a block chain algorithm that is used to confirm transactions and produce new blocks to the chain.
Proof of work system requires users to perform some kind of work in order to participate. The work is such that it is easily verifiable by the network but difficult for the miner.

In, Bit coin proof of work exists such as miner compete to solve a block which contains a set of transactions and have that block accepted to the global block chain of the system.
The only way to have the block accepted is by correctly guessing the special value with a certain amount of mine.
If the miner does not guess the value before another he must start over in attempt guessing a new value that solves the puzzle.

A. Three Main characters of proof of work

• Nonce (Number used once)
It is a random number whose value is set so that the hash of the block will contain a run of leading zeroes.

• Hash code
It is basically a numeric value which is sys in identifying an object at the time of the quality testing.

It also serves as an index for the object.
The main purpose of hash code is to assist with the efficient look up and insertion in data collections that are contingent on a hash table.

The code generated by taking an input and converting into cryptographic output using a mathematical algorithm is hash code.

H(x) is the hash of x.

Thus hash code is an algorithm that converts a sequence of characters into a string of 64 letters or numbers.

• Transaction
Miners have a lot of transactions to processed and they want to be the first one to do so in order to receive the mining rewards.

Every miner knows the hash of the previous block as a public information available on the block chain.
Thus a miner becomes with the previous block hash to start creating a new block of text.

• Hash pointer

Hash pointer is a pointer to the location where information or hash of that information is stored.

If we retrieve information that the pointer points at, we can get the hash of the information and confirm it to be unchanged.
It requires information from previous field.
Thus a regular pointer provides the user a way to retrieve information. However, a Hash pointer will allow us to get the information and also verify that the information hasn't been tampered. Thus a hash pointer informs us where something is and what its value is.
It also saves the hash of the value which they compared data had when we last retrieved it.
Consensus algorithm:

B. Proof of Stake
Proof of stake is a low cost, low energy consuming algorithm which states that a person can mine and validate transaction based on how many coins he or she holds.

In proof of stakes

• Anyone who holds the base crypto currency can become a validator, although sometimes a locked-up deposit is required.
• A validator's chance of mining a block is based on how much stake (or crypto currency) they have.

For example: If you owned 1% of the crypto currency, you would be able to mine 1% of all its transactions.

• The PoS protocol will randomly assign the right to create a block between selected validators based upon the value of their stakes.

The chosen validator is rewarded with a part or the whole of the transaction fee.

C. Proof of Elapsed Time
Proof of elapsed time is a consensus algorithm which prevents high energy consumption and resource utilization by following a lottery system.
Each participant within the network is needed to attend for a every which way chosen time
period. The one who completes the designated waited time wins the new block. Each node within the block chain network generates a random time for which it waits and goes to sleep.
The one who wakes up first commits a new block to the block chain in broadcast the information to the network.

PBFT (Practical Byzantine Fault Tolerance):
It improves the robustness and performance of transaction by directing peer-to-peer messages with minimal latency.

In PBFT, the block chain operator configures and operates the consensus network. To this network

smart contracts are deployed and executed on pure nodes.
The applications are then used to invoke the smart contracts. Though the exact network depends on the consensus mechanism.
PBFT has a leader, validation and non validating peers.
Consensus messages flow between the appropriate peers to ensure that the block chain SC transactions are kept in order.

VII. Block Creation

A. Block Chain Block Structure Block comprises of 3 parts

• Header

Contains version information, nonce, previous block id and timestamp.

• Merkle It is a hash built from the block's transactions identifiers.

• List of records

It is an identification of hashes that were included into the block's Merkle tree.

Every block of a block chain follows a forum structure such that each field predetermined size which is followed throughout the block chain.

B. Block Chain Identifiers:

• Block Header

Primary identifier of a block chain.

Digital finger print, twice the size of a block header.

Unique identification of a block of 32-byte hash.

• Block Height

Position of the block in block chain. The first block is of height 0

Each node dynamically identifies a block.

• Block Chain Merkle tree

Data structure used for summarizing and substantiating the integrity of huge sets of knowledge.

It is conjointly referred to as Binary Hash Tree.

C. Distributed Ledgers

Block chain stores the records of each transaction in the distributed ledger.

A distributed ledger can be defined as a consensus of shared replicated and synchronize data in digital format, which is geographically spread across the globe.

It has no central administrator or single data storage point.

D. Evolution of ledgers Distributed ledgers

Distributed ledgers stores the copy of transactions that have taken place.

Every single person of the network includes a copy of the ledger.

VIII. Types of Block Chain

A. Public Block Chain

Ledgers are publically available to verify or add blocks to the block chain.

Some of the public block chains are: Bit coin

Ethereum Dash Factom

B. Private Block Chain

Only licensed users will add or verify the blocks, however anyone will read it.

A private block chain is a closed network that offers its participants the benefit of the technology.

Some of the Private block chains are: Multi chain

Block Stack

C. Consortium

Only a predefined set of nodes has permission to write the block, since it is a semi-centralized block chain.

Some of them Consortium are:

Hyper ledger 1.0 R3

Ripple

Block chain platforms:

• Ethereum: largest crypto currency after Bit coin.

• R2 : Distributed ledger-based platform.

• Ripple: Cross- border payments.

• Chain : Block chain based cloud infrastructure.

• Hyper ledger: Consortium network for enterprise block chain application.
• IOTA : Backs nano payments.
• Open Chain: Open source, enterprise ready block chain platform.
• Quorum: Majority voting consensus mechanisms.

IX. Challenges in Block Chain

A. Initial cost

Miners use giants computers rigs with several servers to keep the network taking over and that consume a lot of electricity which is not affordable.

B. Energy Consumption
Proof of work consensus mechanisms is very wasteful as a computing algorithm. The year 2017, saw a significant increase in Bit coin network activity and estimated show a combined yearly energy consumption rate of 70 terawatt hrs for bit coin.

C. Security
A block chain pose is security profits from the decentralized nature of its nodes that verify transactions on the block chain.
But owing to the design of block chain technology all public block chains are exposed to SI% of tax.

D. Privacy
It a block chain is public, anyone can look at the transaction recorded on the block chain.
The information available in the public domain runs against long standing norms especially in health care, legal and financial sectors which have the typical privacy requirements.

$$\text{SHA-256}: \begin{array}{ccc} B^1 \cup \ldots \cup B^{2^{64}} & \to & B^{256} \\ M & \mapsto & H \end{array}$$

E. Public Perception:
The biggest disadvantage of block chain has been the perception ate holes in the eyes of the people. People not see it as a part of conventional functioning. Most didn't believe that block chain technology will last for long.

F. Integration with legal systems:
The integration barrier with the legacy systems is also a main issue with adopting block chain.
All the traditional systems would be using different data formats and models for storing data and would be working in isolation.

Most of the systems are take the pact and would have less models of integration with the block chain.

X. Hashing with SHA-256

Hash functions remodel impulsive giant bit strings known as messages, into small, fixed-length bit strings known as message digests, such digests determine the messages that made them with a awfully high likelihood. Digests area unit in this sense fingerprints: a operate of the message, simple, nevertheless complicated enough that they permit identification of their message, with a awfully low likelihood that totally different messages can share identical digests.

In SHA-256, messages up to 2^{64} bit (2.3 Exabyte's, or 2.3 billion gigabytes) area unit remodeled into digests of size

where P = 1 0..0 L
and L is M's length *l* in bit notation

256 bits (32 bytes). For perspective, this implies that associate degree object seven times the scale of Face book's knowledge warehouse in 2014 passed to SHA-256 would manufacture a piece of information the scale of a 32-letter string of American Standard Code

for Information Interchange characters, which string would the object's terribly special fingerprint

FIGURE 1: SHA -256

If we tend to note B^n the set of all bit strings of length strictly n, then we are able to outline SHA- 256 as a perform from the union of bit strings sets B^1 to $B^{2\wedge 64}$, i.e. taking as input any message M of length but 2^{64}, mapping to the bit string set B^{256}, i.e. outputting digests H of length strictly 256.

A distinguished use case of hashing is knowledge integrity verification of huge files, that depends on the comparison of actual and expected message digests, or checksums. Another is hashing as a part of the encryption/decryption journey.

Before a message will be encrypted with associate algorithmic program like RSA, it has to be hashed. within the remainder of this text, we tend to explore what hashing will to a message, with a read to later develop a higher understanding of RSA.

Step by step hashing algorithm with SHA-256:

Pre-processing

• Padding:

If we tend to note M the message to be hashed, and l its length in bits wherever $l < 2^{64}$, then as a primary step we tend to produce the cushiony message M', that is message M and a right cushioning, specified M' is of length l', a multiple of 512. Specifically, we tend to use a cushioning P specified M' is:

FIGURE 2 : Padding

The new message M' =M‖ P is of length l', a multiple of 512. The inclusion of L in artifact P helps avoid trivial collisions (i.e. messages "00" and"000" would turn out identical cushiony messages within the absence of L). the first message will be extracted by reading the last sixty four for bits for length, and so attractive the message from left to right, of length l

• Blocks.

M' is parsed into N blocks of size 512 bits, M^1 to M^N, and each block is expressed as 16 input blocks of size 32 bits, M_0 to M_{15}.

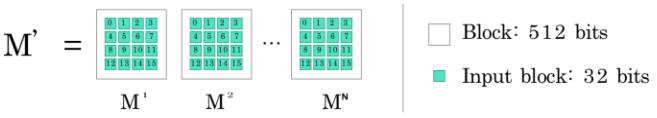


FIGURE 3: Blocks

• Hash initialization.

The initial hash value H^0 of length 256 bits (8 input blocks of 32 bits) is set by taking the first 32 bits of

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ \sigma_1^{\{256\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{256\}}(W_{t-15}) + W_{t-16} & 16 \le t \le 63 \end{cases}$$

$$\sigma_0^{\{256\}}(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x)$$
$$\sigma_1^{\{256\}}(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$$

the fractional parts of the square roots of the first eight prime numbers:

$$H_0^{(0)} = 6a09e667$$
$$H_1^{(0)} = bb67ae85$$
$$H_2^{(0)} = 3c6ef372$$
$$H_3^{(0)} = a54ff53a$$
$$H_4^{(0)} = 510e527f$$
$$H_5^{(0)} = 9b05688c$$
$$H_6^{(0)} = 1f83d9ab$$
$$H_7^{(0)} = 5be0cd19$$

FIGURE 4: Hash initialization

XI.AES ALGORITHM

A. Background

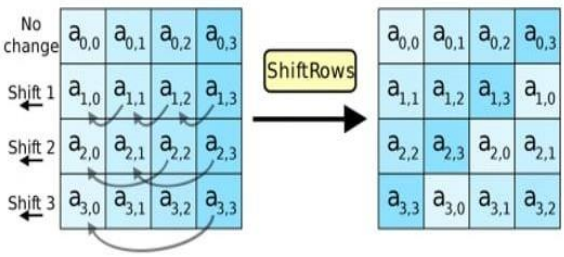
In the 1990s, DES was rendered insecure due to its relatively small 56-bit key size. So, in 1997, the Advanced Encryption Standard (AES) was proposed in response to a public call for proposals by the National Institute of Standards and Technology (NIST). The table below shows how AES compares to its predecessor.

TABLE 1: Comparison of AES and DES

	DES	AES
Developed	1977	2000
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block size	64 bits	128 bits
Key length	56 bits	128/192/256 bits
Security	Rendered insecure	Considered secure

B. What is the AES algorithm?

The AES formula (also referred to as the Rijndael formula) could be a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits



and converts them to cipher text exploitation keys of 128, 192, and 256 bits. Since the AES formula is taken into account secure, it's within the worldwide normal.

C. How does AES work?

The AES formula uses a substitution-permutation, or SP network, with multiple rounds to supply cipher text. the quantity of rounds depends on the key size being employed. A 128-bit key size dictates 10 rounds, a 192-bit key size dictates twelve rounds, and a 258-bit key size has fourteen rounds. every one of those spherical needs around key, however since just one key's inputted into the formula, this key must be swollen to urge keys for every spherical, together with spherical zero.

• Steps in each round

Each round in the algorithm consists of four steps.

• Substitution of the bytes

In the first step, the bytes of the block text are substituted based on rules dictated by predefined S-boxes (short for substitution boxes).

• Adding the round key

In the final step, the message is XORed with the respective round key.

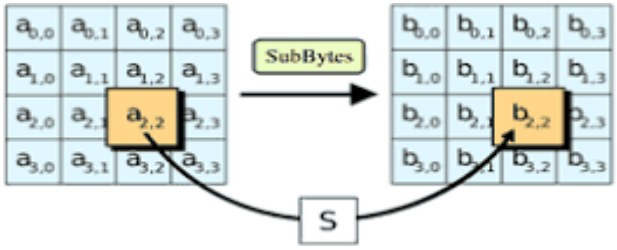


FIGURE 5: Substitution of Bytes

• Shifting the rows:

Next comes the permutation step. In this step, all rows except the first are shifted by one, as shown below.

FIGURE 6: Shifting of Rows

• Mixing the columns:

In the third step, the Hill cipher is employed to jumble up the message a lot of by combining the block's columns.

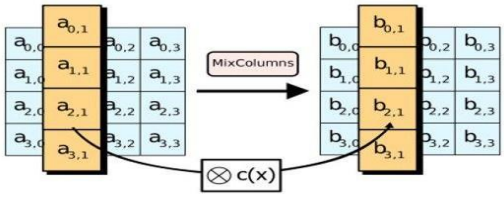


FIGURE 7: Mixing of Columns

Adding the round key
In the final step, the message is XORed with the respective round key.

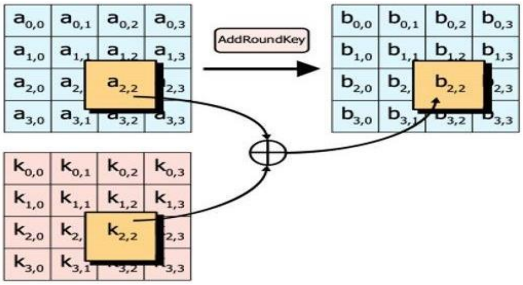


FIGURE 8: Adding the Round Key

XII. APPLICATIONS

• Enterprises
• Government Organizations
• Banking Sector
• Secure sharing of medical data
• NFT marketplaces
• Music royalties tracking
• Cross-border payments
• Real-time IoT operating system
• Anti-money laundering tracking system
• Supply chain and logistics monitoring
• Voting mechanism
• Advertising insights
• Original content creation
• Crypto currency exchange
• Real estate processing platform
• Personal identity secure

XIII. CONCLUSION & FUTURE WORK

Thus we are going to implement a prototype web based software application in Java for application of BCT for cashless economy . We will implement blockchain features such as:

• Decentralization
• Visual Cryptography
• Hash Algorithm
• Encrypted Database.

Thus it is possible to track every transaction in cashless system using BCT. Also thesystem can be transparent using BCT.

The future of block chain technology will continue to drive crypto currency wallet application development. This technology adds security, transparency, and convenience to many financial transactions. Plus, it's applications continue to expand.
Bit coin is a crypto currency that can be used for any online retailer through Crypto pay, a Bit coin debit card. Plus, many online retailers accept Bit coin for payment.

As the number of digital wallet apps continues to rise, users will continue to utilize these apps to cut out intermediate financial arbiters and quickly receive and send digital currency with ease. This reality alone is groundbreaking, notably for users that don't utilize banks, and for several international

transactions that might be tough while not the use of a digital wallet.

There is no doubt that block chain technology is an innovative tool that will make it much easier to navigate the world of crypto currency.

XIV. REFERENCES

[1]. F. Lv and S. Chen, ”Research on Establishing a Traceability System of Quality and Safety of Agricultural Products Based on Block chain Technology,” Rural Finance Research, vol. 12, pp. 22-26, 2016.

[2]. Y. Yang and Z. Jia, ”Application and Challenge of Block chain Technology in the Field of Agricultural Internet of Things, Information Technology, vol. 258,pp. 24-26, 2017.

[3]. S. Nakamoto, ”Bit coin: A peer-to-peer electronic cash system, Consulted, 2008.

[4]. Y. Yuan and F. Y. Wang, ”Block chain: The State of the Art and Future Trends,” Acta Automatica Sinica, 2016.

[5]. Y. Yuan, T. Zhou, A. Y. Zhou, Y. C. Duan, and F. Y. Wang, ”Block chain Tech- nology: From Data Intelligence toKnowledge Automation,” Zidonghua Xue- bao/acta Automatica Sinica, vol. 43, pp 1485-1490, 2017.

[6]. Y.-b. Zhang, ”The New Ecosystem of Cross-border E-commerce between EU and China based on Block chain,” China Business And Market, vol. 32, pp. 66-72, 2018.

[7]. T. Hong, ”Accelerating the Application of Block chain in the Field of Agricultural Products E - commerce in China,” Journal of Agricultural Information, pp. 18-20, 2016.

[8]. Y. Yuan and F.-Y. Wang, ”Parallel Block chain: Concept, Methods and Issues,” IEEE Acta Automatica Sinica, vol. 43, pp. 1703-1712, 2017

[9]. Andreas M A. Mastering Bit coin: Unlocking Digital Crypto currencies. O’ReillyMedia, 2014

[10]. Jerry B, Andrea C. Bit coin: A Primer for Policymakers. Mercatus Center, George Mason University, 2013.

Cite this article as :

Kartik Sarwan, Sanket Thore, Niranjan Satav, Pruthviraj Kamble, Dibyo Mandal, "A Secure E-wallet System Using Block Chain", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 3, pp. 454-466, May-June 2021. Available at doi : https://doi.org/10.32628/CSEIT2173101
Journal URL : https://ijsrcseit.com/CSEIT2173101