International Scientific Journal of Engineering and Management
Volume: 03 Issue: 05 | May – 2024
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM01701

BLOCKCHAIN TECHNOLOGY: TRANSFORMING IOT AND FINANCE WITH PRIVACY AND SECURITY CONSIDERATIONS

Kumaran M, Uvashakthi E, Rajalakshmi R, Muralidharan B
Department of CSE
Jaya Engineering College
Thiruninravur – 602024, Chennai, India
kumaran.ma@gmail.com

Abstract— A Block chain, is a growing list of information, called blocks, which are linked using cryptography. A Block chain is a decentralized, distributed and a public digital ledger that is used to record transactions across many devices so that any involved record cannot be changed easily, without modifying all subsequent blocks, because of this, Block chain has found its use in wide-ranging fields. This system, therefore, describes the role of Block chain in IoT and financial applications, two fields which will be benefitted the most by it. Furthermore, this paper examines the privacy and security concerns related to it and shares some insights on how these problems can be tackled. In this paper, we have reviewed multiple such papers in which similar issues were addressed. Lastly, the public perception of block chain technology is taken to addresses how block chain is perceived in different segments of society

Keywords—framework; block chain; Scalable paymentVerification; Cryptographic hash function; Serial Communication; Transaction data.

1 INTRODUCTION

The purpose of a scalable payment verification for block chain transactions on IoT devices could be to enable fast, secure, and efficient payment processing on low-power devices with limited computational and storage capabilities. Such a protocol could help to address the challenges of scaling block chain technology to support a large number of connected devices in the emerging Internet of Things (IoT) ecosystem.

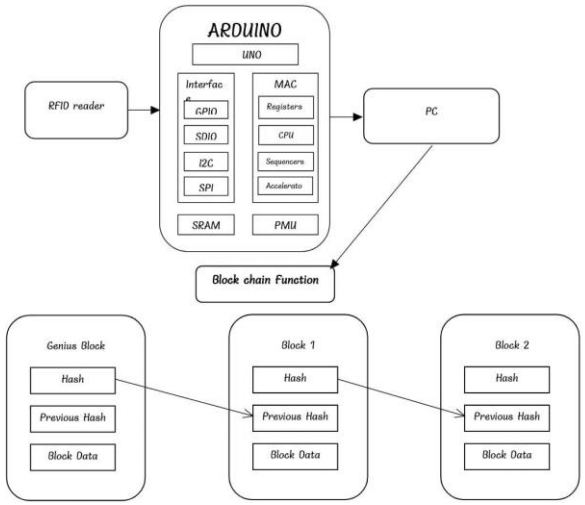
Reduce the processing time and energy consumption required to verify block chain transactions on IoT devices. Improve the security and privacy of payment transactions on IoT devices by reducing the risk of hacking or fraud.

It Enable micropayments and other low-value transactions on IoT devices that would not be practical with existing payment systems. Provide a standardized, interoperable payment protocol that can be used across different IoT platforms and devices.

Overall, a scalable payment verification for block chain transactions on IoT devices could help to unlock the full potential of block chain technology in the IoT ecosystem, facilitating new use cases and business models that were not previously possible.

International Scientific Journal of Engineering and Management
Volume: 03 Issue: 05 | May – 2024
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM01701

2 SYSTEM OVERVIEW



The Scalable Payment Verification (LPV) protocol is designed to enable IoT devices to verify block chain transactions in a resource-efficient manner. Here is an overview of the system:

Block chain Node: A block chain node is required to initiate and validate transactions. This node is responsible for creating a transaction and broadcasting it to the network.

IoT Device: The IoT device is the endpoint device that receives the transaction data from the block chain node. It must be capable of communicating with the block chain node through a secure channel.

SPV Protocol: The SPV protocol is a Scalable verification protocol that enables IoT devices to verify block chain transactions in a resource-efficient manner. The protocol allows IoT devices to request transaction data from the block chain node and verify it locally.

Transaction Verification: Once the IoT device receives the transaction data, it verifies the transaction by checking the digital signature, transaction amount, and transaction history. If the transaction is valid, the IoT device will accept it, and the transaction will be recorded on the block chain.

Resource Optimization: To optimize resource usage, SPV protocol uses techniques like simplified payment verification (SPV), Bloom filters, and Merkle trees to minimize the amount of data that the IoT device needs to receive and process.

3 METHODOLOGY

Scalable payment verification (SPV) is a technique that enables low-power IoT devices to verify block chain transactions without having to store the entire block chain on their device. Here is a methodology for implementing SPV for block chain transactions on IoT devices:

Transaction broadcasting: The IoT device broadcasts a transaction to the network. The transaction contains a hash of the previous transaction, the public key of the sender, the public key of the recipient, and the amount of cryptocurrency being transferred.

Simplified payment verification: Instead of downloading the entire block chain, the IoT device only downloads the block headers, which contain the Merkle root of the transactions in that block. The IoT device uses these block headers to verify the validity of the transaction.

International Scientific Journal of Engineering and Management
Volume: 03 Issue: 05 | May – 2024
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM01701

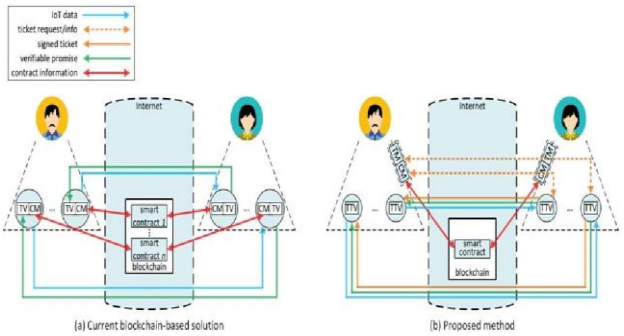
Proof-of-work validation: The IoT device validates the proof-of-work for each block header it downloads to ensure that the block was mined correctly.

Merkle proof verification: The IoT device checks the Merkle proof provided by the network to ensure that the transaction is included in a valid block. The Merkle proof is a cryptographic proof that shows that the transaction is included in the block without revealing the entire block.

Transaction validation: The IoT device validates the transaction by checking that the hash of the previous transaction matches the hash of the previous block and that the sender has enough funds to cover the transaction.

Transaction execution: Once the transaction has been validated, the IoT device can execute the transaction and update its local state.

By using SPV, IoT devices can participate in block chain transactions without having to store the entire blockchain on their device. This reduces the storage and processing requirements of IoT devices, making them more efficient and suitable for use in low-power, resource-constrained environments.



3.1 SHA-256 Algorithm

The SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that is commonly used in Bitcoin and many other block chain networks, including for Scalable payment verification (SPV) in IoT (Internet of Things) devices. Here's how SHA-256 is used in LPV for block chain transactions on IoT devices:

Transaction Hashing: When a transaction is initiated on an IoT device, the transaction data, including the sender's and recipient's addresses, transaction amount, and other relevant information, is hashed using the SHA-256 algorithm. This produces a fixed-size, 256-bit hash value that uniquely represents the transaction data. This transaction hash serves as a unique identifier for the transaction.

Merkle Tree Construction: In a block chain, transactions are typically grouped into blocks, and blocks are linked together using Merkletrees . A Merkle tree is a binary tree in which each leaf node represents a transaction hash, and each non-leaf node is the hash of the concatenation of its child nodes. This process continues until a single hash, called the Merkle root, is obtained at the top of the tree.

Block Header Hashing: The Merkle root, along with other information such as the previous block's hash, a timestamp, a nonce, and other parameter, is hashed using the SHA-256 algorithm to produce a block header hash. The block header hash is a fixed-size hash value that represents the entire block of transactions.

Proof-of-Work (Pow) Mining: In many block chain networks, including Bitcoin, miners compete to solve a Pow puzzle by finding a nonce (a random number) that, when hashed with the block header using SHA-256, produces

ISSN: 2583-6129
DOI: 10.55041/ISJEM01701

a hash value that meets a certain difficulty criterion. This process requires significant computational power and energy consumption. Once a miner finds a valid nonce, the block header hash, along with the nonce, is broadcasted to the network as proof of the miner's work.

SPV Verification: In SPV for IoT devices, instead of verifying the entire block chain, which may be resource-intensive, the IoT device only needs to verify the Merkle root and the block header hash using the SHA-256 algorithm. If the Merkle root and block header hash are valid, the IoT device can trust the transactions included in the block without needing to verify each transaction individually. This allows for more efficient and lightweight verification of block chain transactions on IoT devices.

3.2 UART Protocol

The UART (Universal Asynchronous Receiver/Transmitter) protocol is commonly used for serial communication between electronic devices. In the context of Scalable Payment Verification (SPV) protocol for blockchain transactions on IoT devices, UART can be used to transmit transaction data between the IoT device and a gateway device.

SPV protocol is a simplified version of the traditional blockchain verification process, which allows for faster and more efficient verification of transactions. In SPV, a so-called "header chain" is used to validate transactions, rather than the full blockchain. This allows for reduced bandwidth and storage requirements, which are critical for resource-constrained IoT devices.

To implement SPV on an IoT device, the device must be able to communicate with a gateway device that can perform the more computationally intensive verification process. The gateway device would typically have more resources available, such as processing power, memory, and storage.

UART can be used to establish a serial communication link between the IoT device and the gateway device. The LPV transaction data can then be transmitted using this link, allowing the gateway device to perform the necessary validation checks.

3.3 Here is a prototype of Scalable payment verification

Block header prototype:

The block header prototype used in LPV consists of a subset of the fields found in a full block header, such as the block version number, the previous block hash, the Merkle root hash, the block timestamp, and the difficulty target. By including only these essential fields, the LPV protocol reduces the size of the block header from hundreds of bytes to just a few dozen bytes. This makes it possible for IoT devices with limited storage and processing power to quickly download and verify the blockchain.

Merkle proof prototype:

To verify the validity of a specific transaction, the LPV protocol uses a compact Merkle proof prototype. A Merkle proof is a cryptographic proof that demonstrates that a specific transaction is included in a block in the blockchain without requiring the verifier to download and process the entire block.

The Merkle proof prototype used in LPV consists of a subset of the nodes in the Merkle tree that are required to verify the transaction. Specifically, the proof includes the transaction

ISSN: 2583-6129
DOI: 10.55041/ISJEM01701

hash, the hashes of the sibling nodes along the path from the transaction to the root of the Merkle tree, and the hashes of the intermediate nodes along that path.

By including only these essential nodes, the LPV protocol reduces the size of the Merkle proof from hundreds of bytes to just a few dozen bytes, making it possible for IoT devices to efficiently verify transactions

4 IMPLEMENTATION

The Scalable Payment Verification (SPV) protocol is a proposed protocol for enabling low-resource IoT devices to verify the validity of block chain transactions. While there is no one specific implementation of the SPV protocol, the following are the general steps that could be taken to implement the SPV protocol for block chain transactions on IoT devices:

Determine the hardware and software requirements of the IoT device: To implement SPV, it is important to determine the hardware and software requirements of the IoT device. The device should have sufficient processing power and memory to run the SPV node and download the necessary block chain data.

Choose a suitable block chain network: SPV can be used with any block chain network that supports the Proof of Stake (PoS) consensus algorithm. Choose a block chain network that meets the requirements of the IoT device and is compatible with the SPV protocol.

Install and configure the SPV node software: Install the necessary SPV node software on the IoT device. This may involve setting up a wallet, connecting to the block chain network, and downloading the necessary software libraries. Configuration steps will vary depending on the block chain network being used.

Use Simplified Payment Verification (SPV) to download block headers: To minimize storage and processing requirements, lightweight payment verification uses SPV to download only the block headers and a small portion of the block data. The SPV node should be configured to use SPV to download the necessary data from the block chain network.

Validate transactions using Proof of Stake (PoS): Once the necessary block chain data has been downloaded, the LPV node can use PoS to validate transactions and agree on the state of the block chain. This involves staking a certain number of tokens and participating in the consensus process to validate transactions and earn rewards.

Monitor the SPV node for new transactions: The SPV node on the IoT device should be constantly monitoring the block chain network for new transactions. When a new transaction is detected, the SPV node can validate the transaction using the steps described above and add it to the block chain if it is valid.

Handle any errors or exceptions: If any errors or exceptions occur during the SPV validation process, the SPV node should be configured to handle them in an appropriate manner. This may involve retrying the validation process or logging errors for later review.

Implement appropriate security measures: Since SPV involves staking tokens, it is important to implement appropriate security measures to protect the tokens and prevent unauthorized access to the SPV node. This may involve using secure hardware or software wallets, implementing multi-factor authentication, or other security measures.

ISSN: 2583-6129
DOI: 10.55041/ISJEM01701

Overall, implementing SPV for block chain transactions on IoT devices requires careful consideration of a variety of factors, including hardware and software requirements, performance optimization, security measures, and testing and validation. By following these steps and taking appropriate precautions, it is possible to create a lightweight and efficient SPV node on an IoT device that can validate the validity of block chain transactions

5 Results

The Scalable Payment Verification (SPV) protocol is designed to enable IoT devices to efficiently verify block chain transactions without the need for large amounts of computational resources or storage capacity. SPV allows for quick and secure verification of transactions by using simplified payment verification (SPV) techniques.

The SPV protocol is particularly useful for IoT devices, which often have limited computing power and memory, as it enables them to participate in block chain transactions without the need for significant resources. With SPV, IoT devices can validate transactions and ensure that they are legitimate, without having to download and store the entire block chain.

By using SPV, IoT devices can connect to lightweight nodes that can efficiently provide them with the information they need to validate transactions. This reduces the amount of bandwidth and storage space required by the devices, while also reducing the time and energy required for verification.

6 Conclusion

The cost of deployment and operation of IoT devices is the main impediment to widespread use of IoT-based solutions in different societal problems.

Horizontal integration of IoT devices is a promising approach to overcoming the cost barrier of such solutions.

Having a proper financial mechanism is the crucial first step in the horizontal integration of IoT devices. In this paper, we proposed a Ticket-Based Verification Protocol which is an extension of the current block chain-based financial mechanisms for IoT devices.

Unlike the current block chain based mechanisms, it does not require all the IoT devices to participate in complex interactions with the block chain itself and therefore this protocol can be used in various process.

References

[1] J. A. Stankovic, I. Lee, A. Mok, and R. Rajkumar, "Opportunities and obligations for physical computing systems," Computer, vol. 38, no. 11,pp. 23–31, Nov. 2005.

[2] W. Wolf, "Cyber-physical systems," Computer, vol. 42, no. 3, pp. 88–89,Mar. 2009.

[3] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: A new frontier," in Machine Learning in Cyber Trust, P. S. Yu and J. J. P. Tsai, Eds. Springer US, 2009, ch. 1, pp. 3–13.

[4] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in Proc. of the 47th Design Automation Conference (DAC), Anaheim, California, Jun. 2010, pp. 731–736.

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future

ISSN: 2583-6129
DOI: 10.55041/ISJEM01701

directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[6] T. Wolf and A. Nagurney, "A layered protocol architecture for scalable innovation and identification of network economic synergies in the internet of things," in Proc. of the First IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI), Berlin, Germany, Apr. 2016, pp. 141–151.