Conference Proceeding Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Internet of Things Revolutionary Real Time Implementation Enhancement: A Review

[1]R. Mahalakshmi and [2] Dr. D. Selvanayagi,
[1]Research Scholar, PG and Research Department of Computer Science, Vellalar College for women (Autonomous), Thindal, Erode, India
[2]Department of Computer Applications, Vellalar College for women (Autonomous), Thindal, Erode, India

Abstract: Currently, the world is experiencing a strong rush towards modern technology, while specialized companies are living a terrible rush in the information technology towards the so-called Internet of things IoT or Internet of objects,Blockchain, the foundation of Bitcoin, has received extensive attentions recently. Block chain serves as an immutable ledger which allows transactions take place in a decentralized manner. Block chain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. However, there are still many challenges of block chain technology such as scalability and security problems waiting to be overcome. This paper presents a comprehensive overview on block chain technology. We provide an overview of block chainarchitecture firstly and compare some typical consensus algorithms used in different block chains. Furthermore, technical challenges and recent advances are briefly listed. We also lay out possible future trends for block chain.

Keywords: *Internet of things (IoT), Smart Communication, Sensors, Actuators, System integration, Smart house/city, Network interface Block chain, decentralization, consensus, scalability*

I. INTRODUCTION

Nowadays cryptocurrency has become a buzzword in both industry and academia. As one of the most successful cryptocurrency, Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016 [1]. With a specially designed data storage structure, transactions in Bitcoin network could happen without any third party and the core technology to build Bitcoin is block chain, which was first proposed in 2008 and implemented in 2009 [2]. Block chain could be regarded as a public ledger and all committed transactions are stored in a list of blocks. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency.

The block chain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, block chain can greatly save the cost and improve the efficiency. Since it allows payment to be finished without any bank or any intermediary, block chain can be used in various financial services such as digital assets, remittance and online payment [3], [4]. Additionally, it can also be applied into other fields including smart contracts [5], public services [6], Internet of Things (IoT) [7], reputation systems [8] and security services [9]. Those fields favor block chain in multiple ways. First of all, block chain is immutable. Transaction cannot be tampered once it is packed into the block chain. Businesses that require high reliability and honesty can use block chain to attract customers. Besides, block chain is distributed and can avoid the single point of failure situation. As for smart contracts, the contract could be executed by miners automatically once the contract has been deployed on the block chain.

Although the block chain technology has great potential for the construction of the future Internet systems, it is facing a number of technical challenges. Firstly, scalability is a huge concern. Bitcoin block size is limited to 1 MB now while a block is mined about every ten minutes. Subsequently, the Bitcoin network is restricted to a rate of 7 transactions per second, which is incapable of dealing with high frequency trading. However, larger blocks mean larger storage space and slower propagation in the network. This will lead to centralization gradually as less users would like to maintain such a large block chain. Therefore the tradeoff between block size and security has been a tough challenge. Secondly, it has been proved that miners could achieve larger revenue than their fair share through selfish mining strategy [10]. Miners hide their mined blocks for more revenue in the future. In that way, branches could take place frequently, which hinders block chaindevelopment. Hence some solutions need to be put forward to fix this problem. Moreover, it has been shown that privacy leakage could also happen in block chain even users only make transactions with their public key and private key [11]. Furthermore, current consensus algorithms like proof of work or proof of stake are facing some serious problems. For example, proof of work wastes too much electricity energy while the phenomenon that the rich get richer could appear in the proof of stake consensus process.

II. BLOCKCHAIN ARCHITECTURE

Block chain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger [14]. Figure 1 illustrates an example of a block chain. With a previous block hash contained in the block header, a block has only one parent block. It is worth noting that uncle blocks (children of the block's ancestors) hashes would also be stored in etherealblock chain [15]. The first block of a block chain is called genesis block which has no parent block. We then explain the internals of block chain in details.

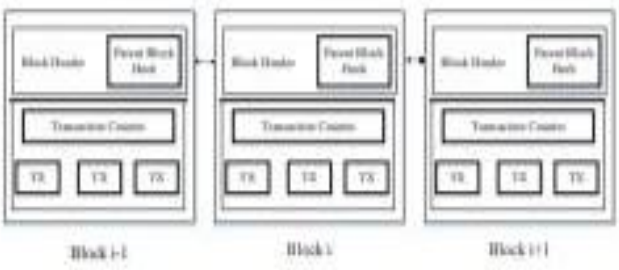
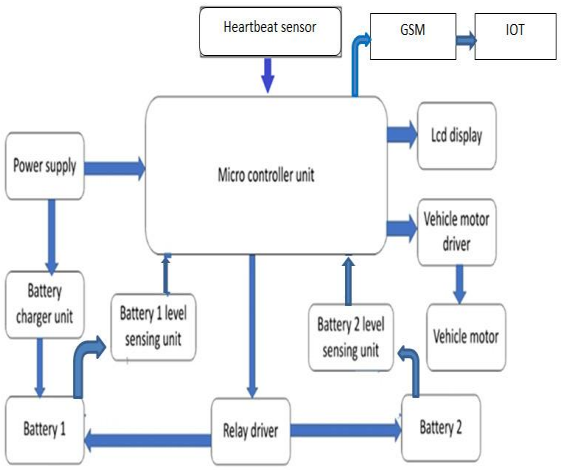


Fig 1 Sequence of blocks of block chain

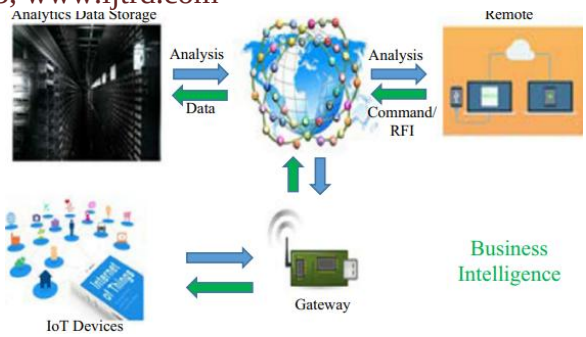
Fig 2 Block Structure

A. Block

A block consists of the block header and the block body as shown in Figure 2. In particular, the block header includes: (i) Block version: indicates which set of block validation rules to follow. (ii) Merkle tree root hash: the hash value of all the transactions in the block. (iii) Timestamp: current time as seconds in universal time since January 1, 1970. (iv) nBits: target threshold of a valid block hash. (v) Nonce: an 4-byte field, which usually starts with 0 and increases for every hash calculation (will be explained in details in Section III). (vi) Parent block hash: a 256-bit hash value that points to the previous block. The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Block chain uses an asymmetric cryptography mechanism to validate the authentication of transactions [13]. Digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature.



Here in this project about Block diagram we can explain that the microcontroller unit process that I have two batteries battery 1 and battery 2. These two batteries are none other than Lithium-Ion batteries. Here we connect this battery using relay driver and from the microcontroller we connect LCD display and a vehicle motor driver and through vehicle motor. In LCD display to the driver it shows the all the information like, How much the charge available in the battery. We connect the power supply with the microcontroller and the battery charger unit then we have externally connect the dynamo for the rotation of speed converted into energy that actually mechanic rotation of speed mechanical energy and it Converts into electrical energy. Then we have used to internally the Heartbeat sensor in the seat belt of the driver seat for the emergency purpose of the drive.



B. Digital Signature

Each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is used to sign the transactions. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is involved with two phases: signing phase and verification phase. For instance, an user Alice wants to send another user Bob a message. (1) In the signing phase, Alice encrypts her data with her private key and sends Bob the encrypted result and original data. (2) In the verification phase, Bob validates the value with Alice's public key. In that way, Bob could easily check if the data has been tampered or not. The typical digital signature algorithm used in block chains is the elliptic curve digital signature algorithm (ECDSA) [16].

C. Key Characteristics of Block chain

In summary, block chain has following key characteristics.

- Decentralization.

In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting to the cost and the performance bottlenecks at the central servers. Contrast to the centralized mode, third party is no longer needed in block chain. Consensus algorithms in block chain are used to maintain data consistency in distributed network.

- Persistency.

Transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the block chain. Blocks that contain invalid transactions could be discovered immediately.

- Anonymity.

Each user can interact with the block chain with a generated address, which does not reveal the real identity of the user. Note that block chain cannot guarantee the perfect privacy preservation due to the intrinsic constraint (details will be discussed in section IV).

- Auditability.

Bitcoin block chain stores data about user balances based on the Unspent Transaction Output (UTXO) model [2]: Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the block chain, the state of those referred unspent transactions switch from unspent to spent. So transactions could be easily verified and tracked.

D. Taxonomy of block chain systems

Current block chain systems are categorized roughly into three types: public block chain, private block chain and consortium block chain [17]. In public block chain, all records are visible

to the public and everyone could take part in the consensus process. Differently, only a group of pre-selected nodes would participate in the consensus process of a consortium block chain. As for private block chain, only those nodes that come from one specific organization would be allowed to join the consensus process. A private block chain is regarded as a centralized network since it is fully controlled by one organization. The consortium block chain constructed by several organizations is partially decentralized since only a small portion of nodes would be selected to determine the consensus.

- Consensus determination.

In public block chain, each node could take part in the consensus process. And only a selected set of nodes are responsible for validating the block in consortium block chain. As for private chain, it is fully controlled by one organization and the organization could determine the final consensus.

- Read permission.

Transactions in a public block chain are visible to the public while it depends when it comes to a private block chain or a consortium block chain.

- Immutability.

Since records are stored on a large number of participants, it is nearly impossible to tamper transactions in a public block chain. Differently, transactions in a private block chain or a consortium block chain could be tampered easily as there are only limited number of participants.

- Efficiency.

It takes plenty of time to propagate transactions and blocks as there are a large number of nodes on public block chain network. As a result, transaction throughput is limited and the latency is high. With fewer validators, consortium block chain and private block chain could be more efficient.

- Centralized.

The main difference among the three types of block chains is that public block chain is decentralized, consortium block chain is partially centralized and private block chain is fully centralized as it is controlled by a single group.

III. WORKING OF THE SYSTEM

When the power from battery 1 starts draining, the battery 2 power will be used. This can be done by using a relay which will indicate the status of battery 1 and then it will automatically swap the battery power from battery 1 to battery 2. . Also the power drained battery 1 can be charged using the Dynamo which is fitted on the wheels. Dynamo is a device which is capable of changing mechanical energy into electrical energy .Hence by using this character of the dynamo the problem can be solved. The description of this technique is that by placing one dynamo in each wheel so that each dynamo will produce a charge through the rotary motion given by the wheels of the EV car and these charges is stored in a separate swapping battery and that can be used for the emergency purpose and this process is cyclic. When car losses its charge while running on the charge produced by the dynamo, the dynamo will not stops its work, it again produce a charge so that you can go for a longer distance.

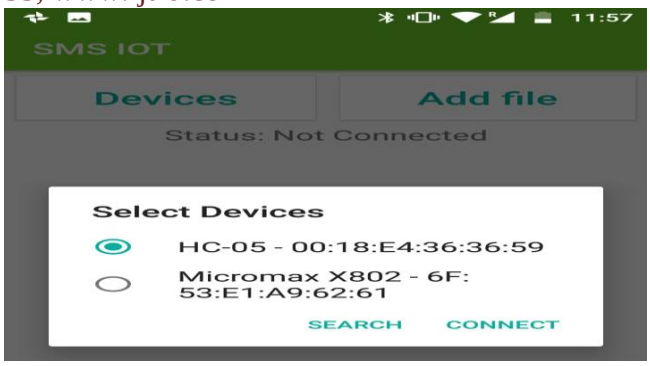


Fig 2 : Connect Page To The IOT

• Consensus process.

Everyone in the world could join the consensus process of the public block chain. Different from public block chain, both consortium block chain and private block chain are permissioned. Since public block chain is open to the world, it can attract many users and communities are active. Many public block chains emerge day by day. As for consortium block chain, it could be applied into many business applications. Currently Hyper ledger [18] is developing business consortium block chain frameworks. Ethereum also has provided tools for building consortium block chains .

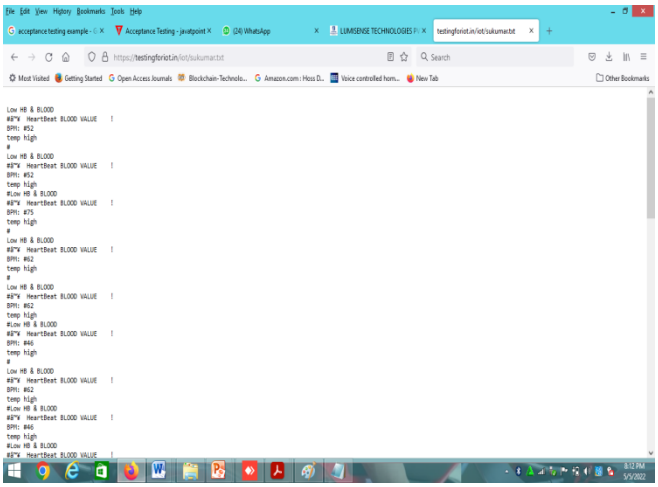


Fig 3 : Real Time IOT based monitoring

The implemented system was tested efficiently and tested for proper working. The swapping of Batteries using Microcontroller and store energy by producing the Dynamo. Then we monitoring the Health Condition of Driver and intimate that message through IOT. The initialization of the IOT and working of the sensors were verified. Messages were obtained after each alert and corresponding data uploaded on to the cloud storage. The buzzer and sprinkler also worked efficiently.

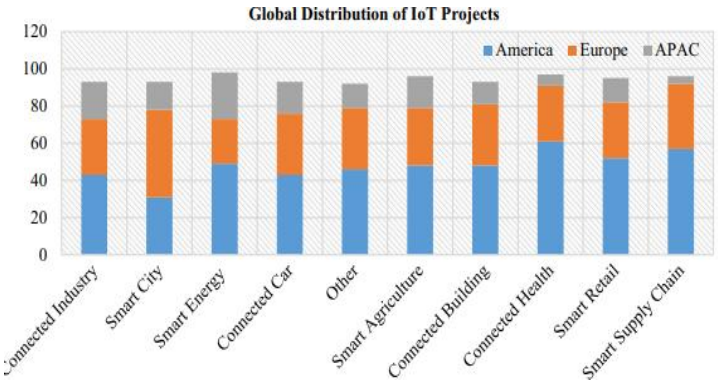


Fig 4: Implementation tiny os tool

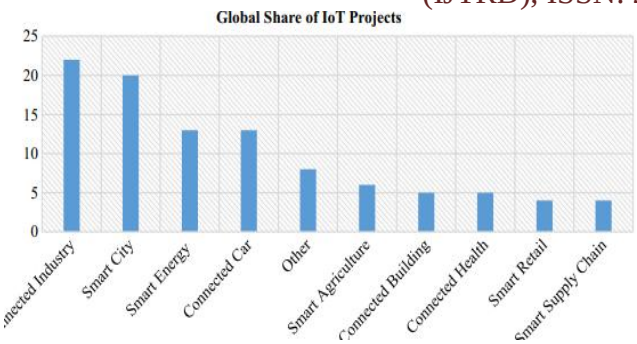


Fig 5: Implememtation sense sim tool

Smart city is one of the trendy application areas of IoT that incorporates smart homes as well. Smart home consists of IoT enabled home appliances, air-conditioning/heating system, television, audio/video streaming devices, and security systems which are communicating with each other in order to provide best comfort, security and reduced energy consumption.

CONCLUSION

Block chain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability. In this paper, we present a comprehensive overview on block chain. We first give an overview of block chain technologies including block chain architecture and key characteristics of block chain. Nowadays block chain based applications are springing up and we plan to conduct in-depth investigations on block chain-based applications in the future.

FUTURE SCOPE

The system has been tested for various operating conditions and results analysed rigorously. The developed battery management system is effectively charge the batteries as well as protects the battery from overcharging and over discharging. The developed maximum power point algorithm also performed well with maximum power point tracking IOT. The based battery management system is better system for dynamo charging of battery in electric vehicle application..

References

[1] [1] "State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/ state-of-blockchain-q1-2016/

[2] [2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] [3] G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective," 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn. 2646618

[4] [4] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," 2015.

[5] [5] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.

[6] [6] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online]. Available: https://ssrn.com/abstract=2394738

[7] [7] Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.

[8] [8] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.

[9] [9] C. Noyes, "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning," arXiv preprint arXiv:1601.01405, 2016.

[10] [10] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436–454.

[11] [11] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29.

[12] [12] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[13] [13] NRI, "Survey on blockchain technologies and related services," Tech. Rep., 2015. [Online]. Available: http://www.meti.go.jp/english/press/ 2016/pdf/0531 01f.pdf

[14] [14] D. Lee KuoChuen, Ed., Handbook of Digital Currency, 1st ed. Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc: eee:monogr:9780128021170

[15] [15] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, 2014.

[16] [16] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.

[17] [17] V. Buterin, "On public and private blockchains," 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains/

[18] [18] "Hyperledger project," 2015. [Online]. Available: https://www. hyperledger.org/

[19] [19] "Consortium chain development." [Online]. Available: https://github. com/ethereum/wiki/wiki/Consortium-Chain-Development