Proof-of-Authentication: IoT-Friendly Blockchain

By Deepak Puthal and Saraju P. Mohanty

We have discussed details of Blockchain technology with its various pros and cons, and application in two articles in IEEE Consumer Electronics magazine. This is the 3rd article on this topic to present some perspectives on consensus algorithms used in Blockchain which is a resource intensive as well as computational intensive step of a traditional Blockchain. Specifically, this article introduced the concept of proof-of-authentication for lightweight implementation of blockchain in Internet of Things (IoT). The proof-of-authentication (PoAh) can replace existing consensus algorithms such as proof-of-work (PoW), proof-of-stake (PoS) and proof-of-activity (PoA) for resource and energy constrained infrastructure such as IoT.

Blockchain in IoT – The Challenges

The IoT is based on the vision to connect of physical devices to Internet and access remote data to control distanced physical world. The IoT things are objects or embedded devices building block of the IoT by connecting devices to the Internet. IoT includes sensing, computation, communication, identification, and semantics. A critical requirement of IoT is that the things in the network must be inter-connected. Implementing blockchain in IoT to secure the infrastructure in distributed manner is a big challenge (Figure 1). Considering the resource constrain devices of IoT, blockchain implementation looks impossible due to the energy requirement for proof-of-work. However, proof-of-work is the backbone for blockchain and without which blockchain cannot a have distributed form. Thus, the current blockchain technology cannot be applied to IoT. Due to the wide range of applications of IoT in modern world and blockchain as only distributed security architecture, we cannot ignore intersection of these technologies. IoT applications focus on energy efficient computing and real-time decision making. This motivates us to explore lightweight consensus algorithm for blockchain transaction verification and validation method for IoT.

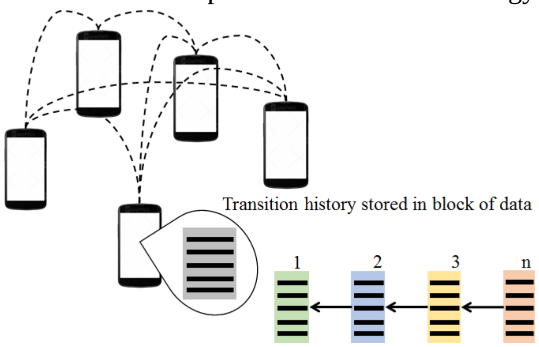

Figure 1. The blockchain transactions network.

Proof-of-Work

Miners within a bitcoin network must maintain and record on the same distributed ledger to secure and consistent bitcoin. However, with millions of decentralized nodes and no central server to maintain the network, the question is how this can be done? Bitcoin's solution to this problem is proof-of-work. In tradition transaction method, a trusted third part always involved to maintain a transaction record to maintain the balance. On the other hand, the decentralised trust-less consensus maintains the transaction without help of third party services. With the concept of bitcoin or digital currencies, individual users in the network hold the distributed ledgers i.e. the blockchain (Figure 2). The users can track the transaction information without the help of trusted third party. They do not need an authenticated by third part to validate their transactions.

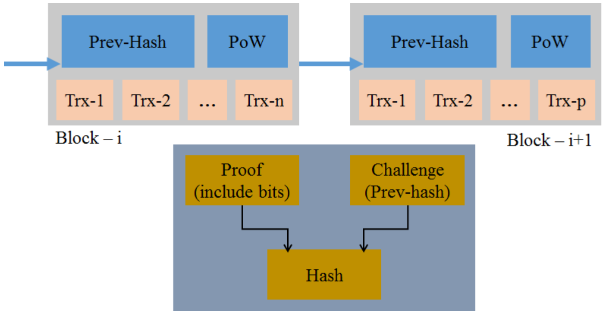

Figure 2. Proof-of-work transactions.

The distributed ledgers required an expensive computational calculation to solve mathematical puzzles to validate the trustless transactions. The expensive computational calculation also known as miner and the process of validating the transactions called as proof-of-work. Miner has two important roles: (1) validate the transactions by avoiding potential network threats, and (2) calculate reword points. Block contains numbers of transactions, where miner apply proof-of-work to evaluate individual transactions as shown in Figure 2. Followed by, miner got a reward point, who have solved the block at first. In order to achieve the reward points, all the miners compete with each other to solve the mathematical problem. After finding solution, miner broadcast to all the network to update the blockchain and receive reward i.e. cryptocurrency. In a real world problem, the mining process is essentially an inverse to hash function. In the standard blockchain, the parameters update fortnightly and new block generate in every 10 minutes.

In proof-of-work, it works with distributed consensus based, where miner needs lots of energy. In a bitcoin transaction, electricity consumption is equivalent to 1.5 household electricity for one day in USA. The bitcoin transactions consume close to the electricity in Denmark by 2020. The concept proof-of-work is not only used for bitcoin but also for several other applications including ethereum. Due to the computational and economical hardness of proof-of-work, several applications use slide modification of proof-of-work to use blockchain. One of the common term is proof-of-stake for ethereum.

Proof-of-Stake

The basic concept of proof-of-stake is proof the ownership of digital currency from proof-of-work. Coin age did not play a crucial role for bitcoin, whereas this concept is originated for bitcoin to help prioritize the transactions. Proof-of-stake gives same level of confidentiality as this is the most critical requirement of monetary transactions.

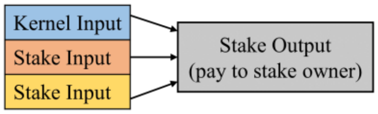

Figure 3. Structure of proof-of-stake (coinstake) transaction.

The transaction of proof-of-stake gives also known as coinstake, introduce a new type of block (Figure 3). The term kernel is the first input of coinstake and is required to meet target hash protocol and apply stochastic process to generate proof-of-stake blocks. Specifically, coinstake follows limited search space to compute hash value instead of unlimited search space like proof-of-work. As a result, proof-of-stake is energy efficient compared to proof-of-work. The hash targets that stake kernel must meet is a target per unit coin age consumed in the kernel. This system ensures that miners who have not been able to provide a solution to the cryptographic puzzle will have a higher chance of creating a block as the coinage of their currency increases.

Proof-of-Activity

In the proof-of-stake scheme, coins would continue to grow in coinage even if the participant is offline. This creates a problem where miners would go online every several weeks, create blocks and then go offline afterwards. This significantly reduces the numbers of concurrently online nodes, reducing the security of the coin. Another problem with this schematic is that it discourages the exchange of the coin as each exchange would reset the coinage, leading of hoarding of the currency.

Proof-of-activity was designed to reduce the impact of these issues. The idea is to reward a fraction of the proof-of-work reward to active peers, where having higher stake in the currency increases the chances of “winning” the reward. A miner who solves a proof-of-work puzzle broadcasts the solution to the network. Every node receiving the block is able to derive a number of “ticket numbers” from the solution. If a peer who owns the coin corresponding to the “ticket” will put their signature onto the block and be able to receive a part of the reward. A peer who is offline will not be able to sign the block and therefore will not receive the reward. The proof-of-activity scheme aims to incentivize peers to remain on the blockchain, whereby improving its security by using this award mechanism. This scheme also makes spending of the currency less punishing, as holding onto currency for long periods of time does not improve the probability of receiving a reward.

Proof-of-Authentication for IoT

The consensus algorithms like proof-of-work, proof-of-stake and proof-of-activity for blockchain are introduced for bitcoin kind applications. The presented proof-of-authentication follows traditional blockchain working model with lightweight block verification.

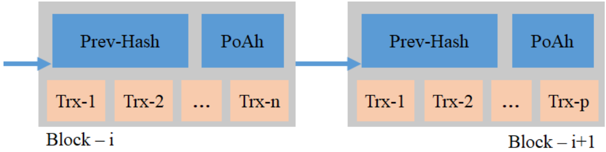

Figure 4. Proof-of-authentication in block transactions.

The initial step of miner in a network is to validate the block followed by evaluated the hash value, where as proof-of-authentication aims to authenticate the blocks following same transaction method of blockchain (Figure 4). The miners can be trusted nodes of the network and which is used for authentication. All the network nodes must maintain and record on the same distributed ledger and they can track the transaction information. The trusted nodes in the network authenticate the blocks to add into the distributed ledger. It includes two steps for authentication, (1) authenticate the block and source of the block, and (2) upon validating the authenticated block by trusted nodes, trust value increased by one unit who have authenticated the block at first. Followed by, all the nodes in network update the distributed ledger. In this process, individual transitions are verified from block. Any miner does false authentication loose a unit of trust value and become a normal node in the network after certain number of false authentication. Proof-of-authentication can avoid the inverse hash computation for energy efficient distributed secure communications and computing in IoT.

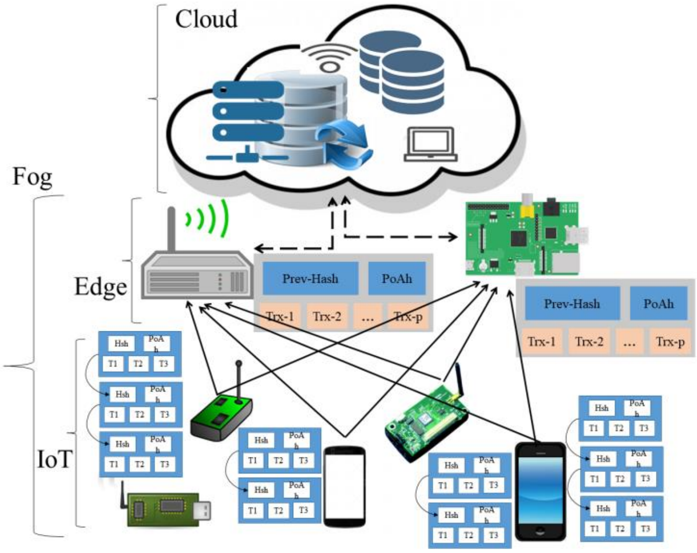

Figure 5. Blockchain in Fog computing.

The fog computing are integrated with IoT for scalable computing and communications. Fog computing integrates clouds and edge infrastructure with IoT, where cloud works as the fully trusted infrastructure to store security properties. Blockchain in fog computing can bring novel architecture while storing IoT device authentication properties to trusted cloud and keep their references at edge devices to work as miner in the network to evaluate proof-of-authentication (Figure 5). The edge devices work as partially trusted device. This will maintain the decentralised security framework in the network. Traditional IoT device deployment can be followed to register devices with fully trusted part such as cloud (Figure 5). Proof-of-authentication can also be integrated with these concepts for end-to-end secure infrastructure building. A comparison classification of different blockchain consensus algorithm is classified with their properties in Table 1.

Table 1. Comparison of different consensus algorithm of bclockchain

	Proof-of-Work (PoW)	Proof-of-Stake (PoS)	Proof-of-Activity (PoA)	Proof-of-Authentication (PoAh)
Energy consumption	High	High	High	Low
Computation requirements	High	High	High	Low
Latency	High	High	High	Low
Search space	High	Low	NA	NA

Conclusion and Future Thoughts

Proof-of-authentication remove reverse hash function from proof-of-work to lightweight the process. As a result, blockchain can efficiently integrate to resource constraint networks such as IoT and related applications. This also work efficiently in hierarchical networks and fog computing scenario. In future, we are aiming to implement proof-of-authentication into real-time IoT and fog testbed to measure the overall performance and efficiency of the network.

About the Authors

Deepak Puthal (deepak.puthal@uts.edu.au) is a Lecturer (Assistant Professor) in the Faculty of Engineering and IT at University of Technology Sydney, Australia.
Saraju P. Mohanty (saraju.mohanty@unt.edu) is a Professor at the University of North Texas who researches on Smart Electronic Systems.

References

[1] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as a Decentralized Security Framework", *IEEE Consumer Electronics Magazine*, Vol. 7, no. 2, pp. 18-21, 2018.

[2] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything You Wanted to Know About the Blockchain", *IEEE Consumer Electronics Magazine*, Vol. 7, no. 4, pp. 06-14, 2018.

[3] C. Dwork, and M. Naor, "Pricing via Processing or Combatting Junk Mail", in *Proc. of the Annual International Cryptology Conference*, pp. 139-147, 1992.

[4] M. Jakobsson, and A. Juels, "Proofs of Work and Bread Pudding Protocols", in *Proc. of Secure Information Networks*, pp. 258-272, 1999.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", *Whitepaper*, https://bitcoin.org/bitcoin.pdf, 2008.

[6] Proof of Stake, https://www.investopedia.com/terms/p/proof-stake-pos.asp, Last Accessed on June 4, 2018.

[7] S. King, and S. Nadal, "Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake", *Self-published paper*, August 19 2012.

[8] F. Tschorsch, and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies", *IEEE Communications Surveys & Tutorials*, Vol. 18, no. 3, pp. 2084-123, 2016.

[9] N. Kshetri, Nir, "Can Blockchain Strengthen the Internet of Things?", *IT Professional*, Vol. 19, no. 4, pp. 68-72, 2017.

[10] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", *IEEE Communications Surveys & Tutorials*, Vol. 17, no. 4, pp. 2347-2376, 2015.

[11] D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A.Y. Zomaya, "Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing", *IEEE Communications Magazine*, Vol. 56, no. 5, pp. 60-65, 2018.