Power Modeling of Blockchain Applications in Mobile Systems

Manuel Figueroa, *ITCR,* Esteban Leandro, *ITCR*

MC-7201 Introduction to Research

Instituto Tecnológico de Costa Rica

{*mfigueroacr, elc790*}*@gmail.com*

***Abstract*—Since security has become a major concern in the everyday use of technology. The impact of mobiles and the growing dependency that the general population has in mobile devices and systems has increased its potentially harmful impact of a security breach. Most of the interaction between users with systems, including banking and e-commerce are made using mobile devices. Recently the introduction of the blockchain technology as an effective security solution for many applications that involve transactions, also as hardware evolves those mobile devices now have larger processing capabilities that make it possible to run blockchain based solution in the mobile space. A definition of a power model allow us to describe, understand and predict the expected behavior of the power consumption demand in those kind of solutions and will help the system designers to estimate how the devices will behave in terms of power consumption. Also, it will help application designers to define the scope of its application in terms of performance and power consumption when it is executed in a mobile device and a high compute rate is expected to perform the blockchain mining process.**

***Index Terms*—LaTeX mobile systems, blockchain, power modeling.**

I. Introduction

A. Blockchain

Blockchain has been introduced in the last years as a technology method for data security problems, where there are several implementations of it, like Bitcoin Wallet [1], Ripples or Ethereum [2], as many others crypto currencies. Besides that, deleting the intermediary from the equation through a bank transaction between an account to another and giving that control to the users has been an interesting approach, where there is a big pool of users that approve those transactions if those are valid to be added to the block chain, with the difference that nobody knows which is the origin user and the destination user, the inly information needed is that a virtual wallet is sending some money or crypto currency to another wallet identified by an address.

After a transaction is created is grouped into blocks, and the links between blocks and their content are protected by cryptography and cannot be forged. Once that the transaction is inside the blockchain, there is no way to erase it.

B. Mining

Kroll et al. [3] explain that the mining process requires vast computing power as only a “brute force, trial and error” method can be used to calculate the SHA-256 hash. Every two weeks, the complexity of the challenge is adjusted to ensure that, on average, a block is mined every 10 minutes. The financial incentive of 25 bitcoins is offered to the first miner to successfully calculate the hash.

This technique may lead money earnings but also requires alot of computing resources consuming, as electricity, but worth to mention it as part of the whole blockchain and crypto currencies possibilities.

C. Blockchain and Internet of Things

This concept adapts to the blockchain and mobile relation, as there are daily millions and millions of devices moving transactions from one side to another, using bank accounts or orher payment methods which may several waits from clients, time consuming and more. Millions of mobile devices can avoid the bank intermediary by handling their transactions inside the blockchain.

As stuff and not just people are relation with the Internet every day, blockchain is a very advanced technique to interconnect transaction systems, as monitoring systems, health, finance, education and more.

Modern Internet of Things(IoT) software systems, like interconnected transportation systems, generate a lot if data every day. The data exchanges may charge a fee for handeling the transactions inside the wallets, which may also elevate costs, security concerns and privacy of several transactions for a single entity [4].

II. Background

A. Mobile Blockchain Systems

According to [5] a blockchain system can be seen as a distributed database of records. The system provides a public layer that keeps a record for every single event that have been executed among the participant parties. Each new transaction added to the blockchain requires a process to be included as a new block in the blockchain. That process requires some kind of validation, usually solving a proof-of-work puzzle. That kind of implementation is expensive and it has been hard to include a proper blockchain system in mobile architectures due to the lack of computing power and the limited energy of current mobile devices. For that reason some other approaches [6], [7] have been studied to enable blockchain application to be used in the mobile devices. In those approaches, the authors claim that is a good idea to offload the mining process to an edge computing service provider, this will eventually enable any device to participate as an active node in the blockchain network even if they are no capable of performing any mining process at all. In that scenario the network must be supported by an external service and that will reduce the *free-network* concept. The mobile devices will participate as dumb clients and the entire blockchain process will be performed in the cloud. Also this novel approach and will be excellent to support e-commerce initiatives and will not limit the participation of users due to lack of computational power.

B. Power Monitoring

According to [8] the bitcoin miners are considered electromagnetic alchemist, because they can convert massive amounts of megawatt-hours of electricity into the world's fastest-growing currency. Because of the calculations required to hash a transaction block and correctly include it in the chain it is estimate that a bitcoin transaction consumes more than 5,000 times as much energy as using a Visa credit card. Even when the computers are constantly getting faster and more power efficient, the bitcoin algorithm increase the difficulty of the hashing procedures to keep the chain integrity and security by making almost impossible to introduce malicious blocks by outrunning the entire network and producing a new longer chain with the fraudulent blocks. That causes a huge impact in the power consumption of the platform, and it is estimates in a total of 73.12 TWh or the same as the entire consumption of Austria [9].

Actually some strategies are implemented to solve this amount of power required to include a new block in the blockchain, some of them are related to change the proof-of-work algorithm to something more power efficient like Algorand [10], using the Bizantine agreements technique to reach consensus, and others like proof-of-learning [11] that use rankings of machine learning systems.

It is possible to measure the power consumption of a component using the Ohm's law that will express a value in *Watts* and can be expressed as the following equation:

$$Power(Watts) = V * I$$

where V is the volatage given in *Volts* and I is the current given in *Amperes*. We can use performance monitoring counters (PFC) [12] to measure the amount of power required by a blockchain network with local nodes, and therefore estimate the total amount of power required when it scales up.

To the best of our knowledge there is no a commercial implementation of a blockchain system running on mobile devices, perhaps an hybrid scheme would be feasible, and the MobiChain [13] is an approach that can run the mining process using mobile nodes.

It is part of our interest to know what is the power modeling of a mobile blockchain system using other consensus mechanisms and verify if that would make them and attractive option to be incorporated in mobile e-commerce platforms.

III. Implementation

Implementation

IV. Related Work

In another similar work, Suankaewmanee et al. [13] studied the performance of a mobile commerce application using blockchain technology in terms of computation energy, time consumption, and memory utilization. They introduce a mobile-commerce application using blockchain technology, the name was MobiChain, used for secured transaction. They develop an API which allows the mining processto be performed on mobile devices effectively.

Also, in [14] they describe approaches to modeling the energy consumption of both Proof of Work in Bitcoin and non-proof-of-work coins and associated consensus algorithms based on parameters including the size of the network, the number of messages sent per transaction, and the computing cost of such a consensus protocol.

The authors in [15] conducts a formal analysis of the newly proposed temporal "rolling" blockchain using the B language. It will examine the security principles of the proposed model and conduct an in-depth analysis of the results, which will be compared to the security principles of traditional blockchain networks. Their aim is to demonstrate that our proposed model is a possible replacement to the traditional blockchain, and is capable of solving the scalability issue without introducing any additional security issues into the core data structure.

In [16] the authors consider an edge computing enabled mobile blockchain network, where IoT devices or mobile users can access and utilize resources or computing services from an edge computing service provider to support their blockchain applications. First, they present overviews of blockchain and edge computing architecture, respectively. They propose a prototype of an edge computing system for mobile blockchain. Then they propose pricing schemes for the edge computing services for mobile blockchain.

V. Future Work

Future Work

VI. Conclusions

Conclusions

References

[1] e. a. T. Bamert, "Bluewallet: The secure bitcoin wallet," Sept.

[2] V. Buterin, "Ethereum: A next-generation cryptocurrency and decentralized application," Apr 2017.

[3] e. a. J. Kroll, "The economics of bitcoin mining or bitcoin in the presence of adversaries," 2013.

[4] e. a. T. Qiu, "Heterogeneous internet of things build our future: A survey, ieee communications surveys tutorials," February 2018.

[5] M. Crosby, "Blockchain technology: Beyond bitcoin," *Berkeley, Applied Innovation Review*, no. 2, p. 7–19, Jun 2016.

[6] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, “Optimal pricing-based edge computing resource management in mobile blockchain,” *2018 IEEE International Conference on Communications (ICC)*, 2018.

[7] ——, “Edge computing resource management and pricing for mobile blockchain,” 10 2017.

[8] P. Fairley, “Blockchain world - feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous,” *IEEE Spectrum*, vol. 54, no. 10, p. 36–59, Sep 2017.

[9] “Bitcoin energy consumption index.” [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption

[10] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, “Algorand,” *Proceedings of the 26th Symposium on Operating Systems Principles - SOSP 17*, 2017.

[11] F. Bravo-Marquez, S. Reeves, and M. Ugarte, “Proof-of-learning: A blockchain consensus mechanism based on machine learning competitions,” *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, 2019.

[12] R. Jain, *The Art of Computer Systems Performance Analysis*, 1st ed. John Wiley & Sons, 1991.

[13] K. S. et al., “Performance analysis and application of mobile blockchain,” Nov 2013.

[14] e. a. Ryan Cole, “Modeling the energy consumption of blockchain consensus algorithms.”

[15] e. a. Richard$_{D}ennis$, “$Atemporalblockchain : Aformalanalysis.''$

[16] Y. Z. et al., “When mobile blockchain meets edge computing,” April 2018.