OVERVIEW: PERMISSIONED BLOCKCHAINS – ETHEREUM VERSUS HYPERLEDGER

[1]Khalid Alhamazan,' [2]Ammar Alanazi
[1]College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia
[1]K.alhamazani@uoh.edu.sa
[2]The National Center for AI and Big Data Technology, King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia
Salanazi@kacst.edu.sa
(Presented at ICSC, 2019, KSA)

ABSTRACT— *The blockchain as a technology considering its core feature to provide secured transactions using cryptography has proven its suitability to be applied in various applications. Permission-less blockchain such the Bitcoin blockchain is one main example, which gained popularity in demonstrating the blockchain features and capabilities. It shows how transactions can be cryptographically secured, accordingly, demonstrating a new structure in handling data. Though, in order to utilize such features brought by blockchain, permissioned blockchain is the one to opt over permission-less blockchains. In other words, when there is a need to adopt blockchain in-house, the suitable option would be those blockchains and frameworks that assist in creating permissioned blockchain. Among others, Ethereum blockchain and Hyperledger framework software are two possible choices to create a permissioned blockchain. This paper demonstrates an overview of the aforementioned technologies, namely, both the Ethereum and the Hyperledger. As stated above, for various applications or projects, specific features of one framework or blockchain can be critical in choosing what is more suitable. The demonstration of this paper targets the researchers in this field as an audience, as well as projects' decision-makers.*

Keywords— Blockchain, Ethereum, Hyperledger, Smart Contracts, Distributed ledger

INTRODUCTION

A blockchain is basically a particular form of data structure, where records (usually transactions) are linked together as a chain of blocks. Blocks of such records are distributed to establish a distributed public ledger [1]. The first open and public blockchain was known as the Bitcoin blockchain. It was based on a research work presented by Satoshi Nakamoto.

Blockchain Core Components

In essence, blockchain technology is unique based on three broad technologies made to work together.

Cryptographic hashing: A standard approach used for message authentication. In this process, cryptographic hash functions are utilized e.g. MD-5 and SHA256 [2].

Asymmetric Cryptography: This technology is leveraged to create digital signatures that are used in blockchain for validating transactions [3].

Peer-to-Peer Networks: A network structure formed up by a group of nodes connecting together in a decentralized manner avoiding a single point of failure [4]. In this network structure, peers communicate with other peers directly to share and exchange data.

Permission-less Blockchain

Indicates a blockchain where the participant (nodes) are not controlled to join/leave the blockchain. The Bitcoin Blockchain is the best example of permission-less blockchains. Moreover, participants in permission-less blockchain can be either pseudonymous or anonymous [5]. In other words, participants do not require to be authenticated to join the blockchain.

Permissioned Blockchain

In contrast to permission-less blockchain, permissioned blockchain has a control layer to control participants (nodes). As a result, transactions validation process in such blockchains is limited to white-listed permissioned participants.

Distributed Ledger

In the blockchain, all validated transactions are recorded in an open ledger, which is public and distributed among all participants in a blockchain. This nature of the distributed ledger makes it an immutable ledger. No single node in a blockchain will have superiority to alter any committed records in this distributed ledger. As a technology, distributed ledger presents a unique paradigm of database where data are shared over a network [6].

ETHEREUM

After the first present of blockchain in 2009, several blockchains followed. Ethereum is one of the blockchains that gained popularity above others, especially because of its generic nature. Originally, Ethereum is a project aimed to present a new generic technology to provide a generalized environment on which end-developers can build decentralized applications on top of Ethereum blockchain [7]. In addition, the state machine concept is adopted in all digital transactions within the Ethereum blockchain [7]. For peers' discovery within Ethereum blockchain, Ethereum incorporates Kademlia's peer-to-peer protocol to find peers for communication [8]. Though, this protocol is not related to the Ethereum consensus protocol. Among other goals, one main goal of the Ethereum project is facilitating digital transactions between compliant Ethereum users [7]. Such users basically have no agreeable means to be able to commit transactions due to many factors e.g. geographical distances, interfacing difficulty, uncertainty, or they may lack existing legal systems. In essence, Ethereum blockchain is a public blockchain, however, it can be deployed in a private environment [9]. As a result, this deployment provides a permissioned blockchain.

HYPERLEDGER

In [10], Hyperledger Fabric is a framework originated by IBM and currently is hosted by the Linux Foundation. It is an open-source technology for a distributed ledger platform. It also stands as a modular architecture enabling pluggable implementations of different functions [9]. Moreover, it

Evaluation Dimension	Ethereum	Hyperledger
Public/Private	Permission-less and permissioned [9]	Only permissioned [15]
Consensus Protocol	Proof-of-Work – PoW [16]	Practical Byzantine Fault Tolerance - PBFT [15]
Core Currency	ETHER [16]	None – Does not support cryptocurrency [16]
Currency Issuance	Tokens [16]	None – Does not support cryptocurrency [16]
Smart Contracts	Supports smart contracts [7]	Supports smart contracts [15]
Smart Contract Programming Language	Solidity [7]	GoLang, Java [15]
Supporting Community	More mature community of developers compared to Hyperledger, 300,000 + developers.	Supported by Linux Foundation Community.
Scalability	Less scalable compared to Hyperledger [9]	More Scalable compared to Ethereum [9]
Peers Communication	Over TCP [17]	-
Service Discovery	Kademlia's peer-to-peer protocol over UDP. [17]	-
The Block	Called uncles, targets interval 10-20 Seconds. [17]	-
Smart Contract Execution Environment	Ethereum Virtual Machine – EVM [18]	Docker Environment [19]

enables developers to create permissioned blockchain in a private network, called a "channel". In some cases, more than one channel can be hosted and running in the same private network [11]. Only permissioned participants can see transactions within a single channel.

DISCUSSION – ETHEREUM VS. HYPERLEDGER

Several dimensions at which, Ethereum blockchain and Hyperledger platform can be discussed to present a comparative overview for both of them. Exploring these dimensions will advance the knowledge in research filed and business adoption. In this discussion, we will examine such dimensions that we believe have an importance when adopting a permissioned blockchain.

Consensus Algorithm

Proof-of-Work (PoW) consensus algorithm was initially adopted by the bitcoin blockchain. PoW however, causes a high consumption of computational power and electrical resources. As a result, it is not practical for permissioned blockchain to use PoW as consensus. Ethereum, adopts a PoW variant protocol, called Greedy Heaviest Observed Subtree (GHOST) [12][13]. On the other hand, Hyperledger uses

Practical Byzantine Fault Tolerance (PBFT) for consensus [14]. PBFT, in particular, has demonstrated its safety properties [12]. Both, GOHST and PBFT are more suitable for permissioned blockchain than adopting PoW. However, Hyperledger allows pluggable mechanism within its framework where developers can use alternative consensus protocols based on their permissioned blockchain needs.

Smart Contracts

Smart contract term indicates a software code stored and run in a blockchain. Users can write smart contract code using programming languages in the same way codes usually are written. After it is deployed, this software code will then act on behalf of the entity who deployed it into a blockchain. Mostly, the smart contract code follows the form of (*if… then clause)*, where conditions are triggered once they are logically met. This logic makes smart contracts irreversible such that if a smart contract executes, no entity can reverse the actions committed by this smart contract code. Ethereum blockchain provides users with the ability to create any required computations by a form of a smart contract [6]. Based on these user pre-defined smart contracts, decentralized applications (dApps) can be built on top of Ethereum blockchain. This makes Ethereum the most generic blockchain for developers. A user can invoke a smart contract by making a transaction to an address, which represents the smart contract. Typically, each smart contract has its own unique address within the blockchain [9]. Ethereum smart contracts are executed with an execution engine provided by ethereum, called Ethereum Virtual Machine EVM [9]. In Ethereum blockchain, each Ethereum validating node runs an EVM. On the other hand, in Hyperledger, smart contracts, called "chaincode" can be written using different programming languages.

Scalability

In [9], a study demonstrated that within the execution layer, Hyperledger consumed less memory to execute a number of smart contracts. Whereas, Ethereum shown a large comparable memory overhead in order to execute the same operations in EVM. As a result, in the study scenario which focuses on the execution layer, Hyperledger outperformed the Ethereum. Although, this scenario will not apply to Ethereum in case of permission-less mode of operation. But for permissioned blockchain, the execution memory consumption is a critical dimension to take into consideration. In contrary, when the number of nodes increases, Hyperledger encounters difficulty to scale, unlike Ethereum scaling capabilities. Although the clients request rate is fixed, Hyperledger fails to handle an increasing number of nodes [9].

In table 1, we summarize dimensions in which Ethereum and Hyperledger can be compared in similarities and differences. We believe such dimensions gain high priority for researchers in this filed to conduct future research work and experiments. As well, decision-makers require such a piece of knowledge when adopting permissioned blockchain in-house.

CONCLUSION

This paper presented an overview and discussed the research dimensions in the area of permissioned blockchain. In doing so, it presented several technical dimensions that could be

considered to evaluate a permissioned blockchain. It also presented two of the popular and widely used permissioned blockchains, namely, Ethereum and Hyperledger.

As future work, real-world experiment will be conducted for further analysis of such permissioned blockchains in terms of other research directions e.g. scalability and fault tolerance.

REFERENCES

[1] Crosby, Michael, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. "Blockchain technology: Beyond bitcoin." Applied Innovation 2, no. 6-10 (2016): 71.

[2] Bellare, Mihir, Ran Canetti, and Hugo Krawczyk. "Keying hash functions for message authentication." In Annual International Cryptology Conference, pp. 1-15. Springer, Berlin, Heidelberg, 1996.

[3] Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, and Huaimin Wang. "Blockchain challenges and opportunities: A survey." Work Pap.– 2016 (2016).

[4] Bahga, Arshdeep, and Vijay K. Madisetti. "Blockchain platform for industrial internet of things." Journal of Software Engineering and Applications 9, no. 10 (2016): 533.

[5] Xu, Xiwei, Cesare Pautasso, Liming Zhu, Vincent Gramoli, Alexander Ponomarev, An Binh Tran, and Shiping Chen. "The blockchain as a software connector." In 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), pp. 182-191. IEEE, 2016.

[6] Mills, David C., Kathy Wang, Brendan Malone, Anjana Ravi, Jeffrey Marquardt, Anton I. Badev, Timothy Brezinski et al. "Distributed ledger technology in payments, clearing, and settlement." (2016).

[7] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151 (2014): 1-32.

[8] Kiffer, Lucianna, Dave Levin, and Alan Mislove. "Stick a fork in it: Analyzing the Ethereum network partition." In Proceedings of the 16th ACM Workshop on Hot Topics in Networks, pp. 94-100. ACM, 2017.

[9] Dinh, Tien Tuan Anh, Ji Wang, Gang Chen, Rui Liu, Beng Chin Ooi, and Kian-Lee Tan. "Blockbench: A framework for analyzing private blockchains." In Proceedings of the 2017 ACM International Conference on Management of Data, pp. 1085-1100. ACM, 2017.

[10] Cachin, Christian. "Architecture of the hyperledger blockchain fabric." In Workshop on distributed cryptocurrencies and consensus ledgers, vol. 310. 2016.

[11] Robinson, Peter. "Requirements for Ethereum Private Sidechains." arXiv preprint arXiv:1806.09834 (2018).

[12] Ritz, Fabian, and Alf Zugenmaier. "The impact of uncle rewards on selfish mining in ethereum." In 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 50-57. IEEE, 2018.

[13] Natoli, Christopher, and Vincent Gramoli. "The blockchain anomaly." In 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), pp. 310-317. IEEE, 2016.

[14] Androulaki, Elli, Christian Cachin, Angelo De Caro, Andreas Kind, and Mike Osborne. "Cryptography and protocols in hyperledger fabric." In Real-World Cryptography Conference. 2017.

[15] Vukolić, Marko. Hyperledger fabric: towards scalable blockchain for business. Tech. rep. Trust in Digital Life 2016. IBM Research, 2016. URl: https://www. zurich. ibm. com/dccl/papers/cachin_dccl. pdf, 2016.

[16] Baliga, Arati. "The blockchain landscape." Persistent Systems(2016).

[17] Gencer, Adem Efe, Soumya Basu, Ittay Eyal, Robbert Van Renesse, and Emin Gün Sirer. "Decentralization in bitcoin and ethereum networks." arXiv preprint arXiv:1801.03998 (2018).

[18] Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli. "A survey of attacks on Ethereum smart contracts." IACR Cryptology ePrint Archive 2016 (2016): 1007.

[19] https://www.hyperledger.org/wp-content/ uploads/ 2018/08/ HL_ Whitepaper_IntroductiontoHyperledger.pdf