

Blockchain Platforms Overview

Yassine Jebbar

April 11, 2017

Abstract

We take a look into different blockchain platforms, underlining their similarities and differences in the process. We discuss also how the blockchain technology can be used for records keeping and the existing solutions that are answering such specifications.

1 Introduction

Blockchain can be generally described as a distributed ledger linking numerous blocks of data in a sequenced manner, in order to keep track of the different transactions taking place within the system. The content of the ledger is being agreed on by all the participants in the system, through a distributed consensus algorithm, in which every participant is witnessing the transactions taking place and therefore proposing a block of transactions based on these witnesses. Although the principle is the same, different blockchain platforms choose different approaches (public/private, PoW/PoS,...) to implement this technology. This approach variation is mainly due to the application field (Finance, Health care, Copyrights protection,...) and what a developer may want to achieve with the blockchain technology stack. In the next section, we do an overview of multiple blockchain platforms with a display of their main characteristics and differences.

2 Blockchain Platforms

2.1 Bitcoin

The first, and most famous blockchain platform. Launched in 2009 by the anonymous Satoshi Nakamoto, the blockchain technology was directly involved in making Bitcoin the most valued cryptocurrency up to date [1]. The Bitcoin blockchain maintains the transactions' records made by the different participants in the Bitcoin network. It does also rely on the proof of work principle to prove the authenticity of the records. PoW is basically about solving a mathematical puzzle consisting of finding the right nonce. The "nonce" in a bitcoin block is a 32-bit (4-byte) field whose value is set so that the hash of the block will contain a run of leading zeros. the number of zeros is global variable in the Bitcoin network, and it changes after every 2016 blocks [2]. Bitcoins are put into circulation by mining. Mining is "is the process of adding transaction records to Bitcoin's public ledger of past transactions or blockchain" [3].

2.2 Ethereum

Relying on the same blockchain principles, ether (Ethereum-based cryptocurrency) is emerging as the second most successful digital currency behind bitcoins [1]. Nevertheless, Ethereum was designed to be much more than a payment system. It is "a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference" [4]. Ethereum block times are currently at about 14 seconds, compared to Bitcoin's 10 minutes. Ethereum also currently operates on a proof-of-work basis. Miners are rewarded for processing transactions and executing smart contracts, which create blocks.

3 Blockchain-based record keeping solutions

As interest in blockchain-based solutions -be it through companies or simple initiatives/projects- is growing dramatically [5], many companies who are adopting this technology prefer to build their solutions either on the Bitcoin blockchain or the Ethereum blockchain [6], given their well-established status as the two most successful Blockchain platforms currently [1]. Therefore, the evaluation of the record keeping solutions in these section should take into account how these solutions are making profit from Bitcoin/Ethereum Blockchains to ensure the security of their records.

3.1 Blockstack

Originally a naming system which is built on Bitcoin's Blockchain, Blockstack provides the ability of tracking key-value pairs in form of (unique) names and their associated data. In the Blockstack Whitepaper [7], there is another confirmation, after a handful of experiences, that the Bitcoin's Blockchain is probably the most secure Blockchain platform available currently. If that is partly due to the big network of participants in Bitcoin, the difficulty of controlling 51% of the processing power inside the network, where all the participants are even, is an important factor as well. On the other hand, Blockstack developers chose to take a different approach in terms of storage, given that the Bitcoin Blockchain can only hold data in the order of kilobytes [8]. Therefore, Blockstack uses blockchain "as a communication channel for announcing state changes, as any changes to the state of name-value pairs can only be announced in new blockchain blocks" [7]. As for storing these records of the name-data pairs, Blockstack uses a dedicated data plane for that purpose.

3.2 Proof of Existence [9]

An online service for storing and timestamping the existence of a document inside the blockchain. This secure storage is done traditionally by keeping a hash of the file in the chain, with a reference also to the time in which the document was stored. Consequently, such mechanism does not only ensure that the files' content cannot be seen by the Bitcoin's network participants (since PoE is built on Bitcoin's Blockchain), it allows also validating the document's existence "even if this site (proofofexistence.com) is compromised or down" [9]. On the technical aspect, it is worth noting that this solution also uses

the OP_RETURN field to pass specific information with the transaction. To confirm a document's existence at a certain timestamped time, checking the OP_RETURN field in blockchain transactions for the SHA-256 hash of the document, prepended by the PoE marker bytes (0x444f4350524f46) should be sufficient. The existence of that transaction in the blockchain proves the existence of the document at the timestamped time.

References

- [1] <https://www.cryptocompare.com/>
- [2] <https://en.bitcoin.it/wiki/Nonce>
- [3] <https://www.bitcoinmining.com/>
- [4] <https://www.ethereum.org/>
- [5] <https://trends.google.com/trends/explore?q=blockchain>
- [6] Blockchain Technology for Recordkeeping, Help or Hype ? (Appendix C: Blockchain companies), https://www.researchgate.net/profile/Victoria_Lemieux/publication/309414363_Blockchain_for_Recordkeeping_Help_or_Hype/links/580f539408ae009606bb62f6.pdf
- [7] Blockstack: A Global Naming and Storage System Secured by Blockchains, <https://blockstack.org/blockstack.pdf>
- [8] Bitcoin: A Peer-to-Peer Electronic Cash System, <https://bitcoin.org/bitcoin.pdf>
- [9] What is proof of existence ? <https://proofofexistence.com/about>