Blockchain Platforms Overview

Yassine Jebbar

April 17, 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, Blockcstack 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 difficuly 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, Blockcstack developpers 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, Blockcstack 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 traditionnaly by keeping a hash of the file in the chain, with a referrence 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 (proofofexsitence.com) is compromised or down" [9]. On the technical aspect, it is worth noting that this solution also uses

the OP_RETRUN 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 trasancations for the SHA-256 hash of the document, prepended by the PoE marker bytes (0x444f4350524f4f46) should be sufficient. The existence of that transaction in the blockchain proves the existence of the document at the timpestamped time.

3.3 Hyperledger

Even though we stated earlier that most current well-established solutions are either Bitcoin or Ethereum based, Hyperledger succeeded to make a name for itself as a smart contract blockchain platform, relying on a somewhat different approach. Initiated by The Linux Foundation, Hyperledger started a set of distributed ledger solutions based on different platforms and programming languages. Hyperledger is based on the expectation that there will be many blockchain networks, with each network ledger serving a different goal [10]. In this section, we present the Hyperledger Blockchain explorer, and then we take a keen interest on Hyperledger Fabric.

Hyperledger Blockchain Explorer

A blockchain explorer web application. It allows "to view/query blocks, transactions and associated data, network information (name, status, list of nodes), chain codes/transaction families (view/invoke/deploy/query) and any other relevant information stored in the ledger " [11]

Hyperledger Fabric

Hyperldger Fabric is simply "a permissioned blockchain platform aimed at business use. It is open-source and based on standards, runs user-defined smart contracts, supports strong security and identity features, and uses a modular architecture with pluggable consensus protocols" [12]. It aims to advance blockchain technology by identifying and realizing a cross-industry open standard platform for distributed ledgers, which can transform the way business transactions are conducted globally. Generally, Hyperledger Fabric offers the major advantage of ensuring private transactions/contracts between sinlge nodes in a network of nodes. This is made possible through providing private communication channels between participants. Therefore, any two (or more) participating nodes can share their own distributed ledger, containing their own private transactions, with the rest of the network being unaware of this private ledger. As for the participating peers in the network, the fabric distinguishes between two kinds of peers: A validating peer is a node on the network responsible for running consensus, validating transactions, and maintaining the ledger. On the other hand, a non-validating peer is a node that functions as a proxy to connect clients (issuing transactions) to validating peers. A non-validating peer does not execute transactions but it may verify them [12]. the smart contracts run by Hyperledger Fabric are written in Go language, and they are called chaincode. The transactions' operations are generally divided into 3 categories

1. **Deploy** Allows traditional deployment of smart contracts, as this operation installs the chaincode taken as its input in the peers of the network. After the deployment, the chaincode can be invoked by the different peers.

2. **Invoke** Provide the ability to invoke a transaction of a particular chaincode that has been installed earlier through a deploy transaction [12]. Depending on the arguments taken by the operation; the chaincode defines the type and executes the transaction, may read and write entries in its state accordingly, and indicates whether it succeeded or failed.

3. **Query** Returns an entry of the state directly from reading the peer's persistent state [12].

3.4 Namecoin [13]

Just like Blockstack, Namecoin is another blockchain based solution for namespaces' storage. Relying on forking the Bitcoin's blockchain (using Bitcoin's blockchain itself for specific purposes and additional functions), Namecoin allows secure storage of key value pairs, ensuring consequently the uniqueness of names inside the blockchain. On the other hand, the values associated to different namespaces aren't necessarily unique, as the same value can exist within different namespaces. For the additionnal functions, Namecoin introduced three new operations: **NAME_ NEW** which allows a client to choose a name (if it's not already taken), **NAME_ FIRSTUPDATE** takes as input the output of the previous operation, and allows the client to associate initial values to the chosen name and **NAME_ UPDATE** takes as input the output of NAME_ FIRSTUPDATE and gives the client the possibility to change or insert new values in the name that he has chosen.

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`

[10] Hyperledger Whitepaper, http://www.the-blockchain.com/docs/Hyperledger\%20Whitepaper.pdf

[11] https://www.hyperledger.org/community/projects

[12] Architecture of the Hyperledger Blockchain Fabric, https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf

[13] An empirical study of Namecoin and lessons for decentralized namespace design, http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_kalodner.pdf