Literature Review on

A Vademecum on Blockchain Technologies: When, Which and How

Author: Marianna Belotti, Nikola Božić, Guy Pujolle, Stefano Secci

Presented By

Ali, Shaiaz

17-33829-1 || CSE

Outline:

- Introduction
- Methodology
- Fundamental Bricks of Designing
- Blockchain Architechture Layers
- Distributed Ledger Technology (DLT)
- Consensus
- Smart Contract
- Modes of Blockchain: Permissionless and Permissioned
- Journey of a Transaction
- Processing of a Transaction
- Blockchain as a platform
- Existing Blockchain Platforms
- Conclusion
- Remarks & Fields of Improvement
- Reference

Introduction

In terms of quality of the database technology, blockchain has been a great leap of advancement till date. As admiring as it's benefits could be, blockchain in not completely understood to many people, proposing the need of a strong vademecum (a handbook or guide that is kept constantly at hand for consultation) to guide to help software architect & designers to make the decision to adopt blockchain technology. Such a vademecum is attempted to be presented in this particular article.

Methodology:

Thorough analyzing a selection of vast literature on blockchain that emerged in the past few decades, a general representation of blockchain is represented that goes far beyond it's usage in Bitcoin (a type of digital crypto-currency that utilizes blockchain). Key features, methods and functionalities are discussed to provide a good sense of it's benefits and when to utilize it or not also the advanges and the disadvantages.

Fundamental Bricks of Designing:

The two fundamental brick of the blockchain technology are

1. *Cryptographic Security &*
2. *Distributed Consensus Validation Protocol.*

- ***Cryptographic Security:*** Communications and transaction data storage are regulated by cryptographic security, network nodes have to agree on both the validity and the order in which transactions are listed in the blockchain
- ***Distributed Consensus Validation Protocol:*** Distributed consensus protocols solve these issues in a scenario where each node comes to vote. The first example of such a blockchain is Bitcoin. The Bitcoin behaviour traces what can be defined as the 'classical' blockchain, consisting in a permissionless blockchain alternative enabling a digital, distributed and decentralized payment system.

Blockchain Architechture Layers:

There are 5 layer in the blockchain architecture.

i. Network Layer,
ii. Data Model Layer,
iii. Excecution Layer,
iv. Consensus Layer &
v. Application Layer

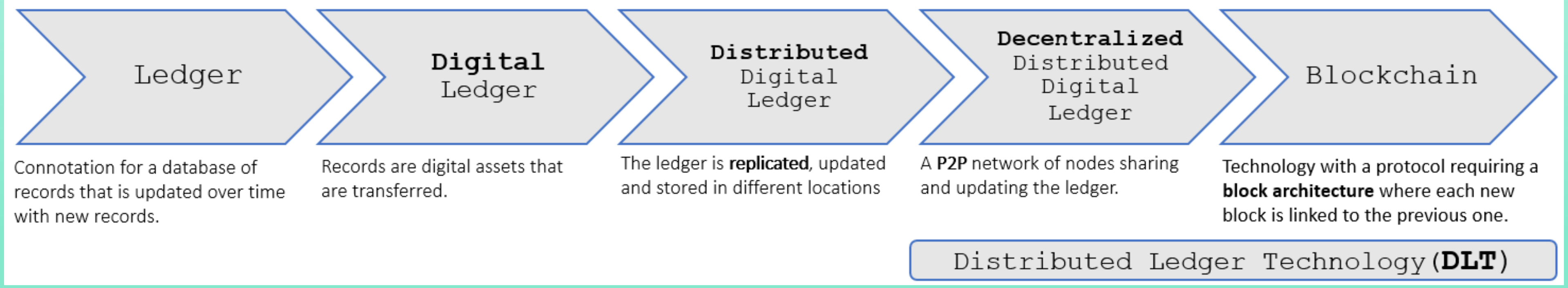
Particularly focusing on these layer is very crucial for deciding –

- *Whether to adopt the blockchain technology or not.*
- *Which of the exsiting blockchain technology is the closest to certain use-case.*

Distributed Ledger Technology (DLT):

A distributed ledger is a type of digital data structure residing across multiple computer devices, generally at geographically distinguished locations and DLT designs a type of technology enabling storing and updating a distributed ledger in a decentralized manner.

Blockchain consists in a transaction database (distributed ledger), shared by different users of it's network. Generally, Distributed Ledger Technologies (DLTs) are designed to deal with database in the form of data shared in a distributed manner. The blockchain and all its variations belong the spectrum of DLTs.



Ledger

Digital Ledger

Distributed Digital Ledger

Decentralized Distributed Digital Ledger

Blockchain

Connotation for a database of records that is updated over time with new records.

Records are digital assets that are transferred.

The ledger is **replicated**, updated and stored in different locations

A **P2P** network of nodes sharing and updating the ledger.

Technology with a protocol requiring a **block architecture** where each new block is linked to the previous one.

Distributed Ledger Technology (**DLT**)

Fig. DLT evolution: from the traditional ledger to blockchain.

Consensus:

Consensus in blockchain network refers to the process in which the participating nodes of the network votes to validate a ledger of any change/update when it is to occur.

A consensus algorithm is in place to ensure –

I. *The data on the ledger is the same for all network nodes &*
II. *Prevent malicious actors from manipulating the data.*

Smart Contract:

A smart contract is a computer program within the blockchain that executes predefined actions when certain conditions are met. This is basically the controlling program of a decentralized application (in blockchain) after being deployed. Smart contract provide the transactions language, allowing the ledger state to be modified.

Modes of Blockchain: Permissionless and Permissioned

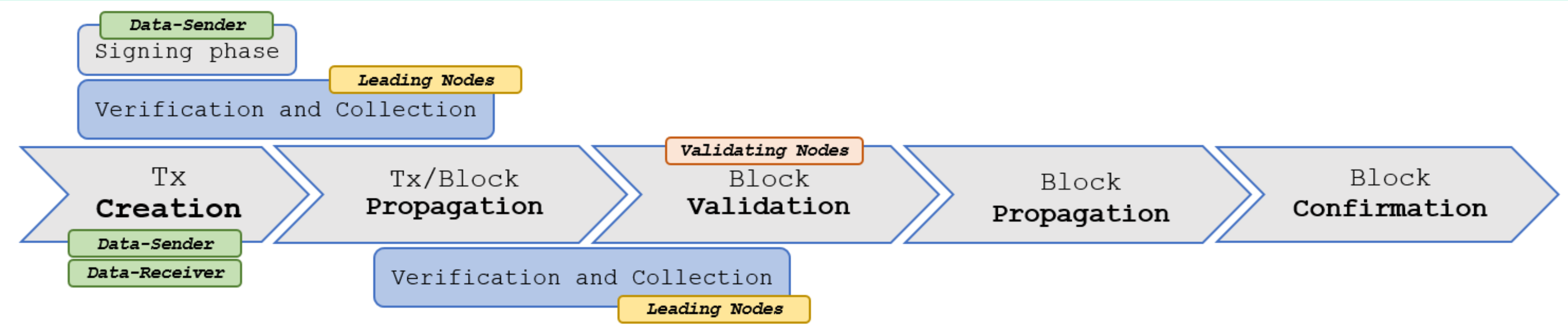
These are just two modes of blockchain. On is Permissionless Blockchain (also known as Public Blockchain), another is Permissioned Blockchain (also known as Private Blockchain).

i. ***Public Blockchain:*** *Participation in consensus in open-access and public, meaning that any participating node in the network is allowed to make updated to the blockchain (of course after fullfilling some criteria and requirements).*

ii. ***Private Blockchain:*** *Participating nodes of the network must have privillage to make any updates to the blockchain (or participate in consensus/validation), otherwise, just able to read data from the blockchain network.*

Journey of a Transaction:

Here down below is a simple graphical representation of how a transaction in blockchain network is confirmed from being created.



Processing of a Transaction:

When creating a transaction in the blockchain networks, there are a few things to keep under consideration. Such as blockchain actors and corresponding roles. There are a few key roles a node (with atleast reading permission) can assume in a blockchain network.

Those are –

A. ***Transacting Parties:***
   i. *Data-Sender &*
   ii. *Data-Receiver.*
B. ***Leading Nodes &***
C. ***Validating Nodes***

A. Transacting Parties:

A transacting party (also known as transacting node) is such a node that is either issuing a transaction to i) Send data or a node that is ii) Receiving data.

i. ***Data-Sender:*** *The data-sender is the node transferring data through an atomic operation (i.e. transaction) to receiving node.*

ii. ***Data-Receiver:*** *Any user receiving a signed transaction who can recover the sender's public-key from the message and verify the transaction authenticity is a data-receiver.*

B. Leading Node:

Consensus can be established by the election of a temporary leader node acting as a 'dictator'. The leader is responsible for both deciding which block to propose as a candidate to be included in the blockchain ledger and verifying the block proposal correctness.

The leader goes out of power immediately after the validation of its block proposal.

C. Validating Node:

The validating nodes are such nodes that participates in a consensus by running the programmed consensus algorithm. Such consensus participating nodes are responsible for establishing the agreement on the proposals made by the leading nodes.

The validation of a block corresponds to the consensus among validating nodes on which block to publish and in which order.

Blockchain as a platform:

In general a blockchain-based system enables digital data- sharing, digital data-storing and virtual interactions among peers (also previously mentioned as Nodes). The principal goal of a blockchain platform is to form P2P digital relationships favouring digital exchanges and business automatization.

The purpose of such platform can be –

i. ***Asset Digital Exchange:*** *Blockchain enables the sharing of any valuable data among parties without any geographical and timing constraint. Both the asset nature and the size of the data-flow impact on the choice of the blockchain nature and its architectural design.*
ii. ***Business Automization:*** *Blockchain platforms allow smart contract deployment and execution with the aim of letting any business automate its functionalities which are sensitive.*

Existing Blockchain Platforms:

There are a lot of blockchain platforms out there but the major ones are –

1. ***Bitcoin Blockchain:** Bitcoin is a public, permissionless blockchain network, giving open-access to its transaction logs. Bitcoin protocol also does facilitate a weak version of Smart Contract as well.*
2. ***Etherium Blockchain:** Etherium is an open platform that is designed to build and use decentralized applications and run smart contract. It has a built-in Fully-fledged Turing-complete programming language (named Solidity) to create & deploy smart contracts.*
3. ***Hyperledger:** Hyperledger is an umbrella open-source project hosted by The Linux Foundation, created to favour cross-industry blockchain technologies.*
4. ***Corda:** Corda is a permissioned blockchain framework, created by the software company R3 that leads a consortium of two hundred global financial institutions.*

Conlusion:

Besides being evident for currency systems, these features are useful for any transactional system that is to be used by multiple independent trust-less parties. The concept of distributed systems very useful in terms of user information privacy and most definitely in transactions. Blockchain allows the user to be able to fully own their possessions without being depending on any other entity. This article provides an excellent guide for helping organizations to make the choice of adapting and deploying blockchain technology. Many concepts of blockchain mechanism are well explained in details to serve such purpose.

Remarks & Fields of Improvement:

The guide well serves it purpose of providing a guilde to adopt blockchain. However, such guide won't be sufficient to help beginners to start their journey on blockchain and has no explanations for development environments of blockchain, nor does it has any discussions regarding simulators to learn & develop decentralized applications on blockchain. The article could be improved for beginners by introducing and adding such discussions regarding the development of decentralized apps.

Reference

Marianna Belotti, Nikola Božić, Guy Pujolle, Stefano Secci. A Vademecum on Blockchain Technologies: When, Which and How. Communications Surveys and Tutorials, IEEE Communi- cations Society, Institute of Electrical and Electronics Engineers, 2019, 21 (4), pp.3796-3838.10.1109/COMST.2019.2928178 . hal-01870617