1

BLOCKCHAIN TECHNOLOGIES

Recently, usage of Blockchain technologies has emerged as their applicability is not limited just to the financial sector, the sector Bitcoin first gain popularity (see Bitcoin A peer-to-Peer Electronic Cash System 2008 [2]). The domains which benefit from blockchain innovation range from healthcare and manufacturing to insurance and legal tech. Decentralization, improved security, immutability, transparency are some blockchain characteristics that bring new opportunities for a wide range of businesses.

Broadly speaking, a blockchain is a distributed ledger consisting of chronologically ordered transactions, bundled together in blocks. Blocks are timestamped and linked as a list data structure replicated across all peers participating in the blockchain network. Each block contains the hash of the previous block. This arrangement of blocks provides ***immutability*** of transactions, as it is infeasible to reconstruct the entire chain following a block where even a small change has been performed. i.e where a transaction has been tempered.

To ensure ***security*** various cryptographic primitives (digital signatures, hashing algorithms, PKI protocols) are adopted. This allows participants to generate, validate transactions and to cooperate without preexisting trust among each other.

One of the key properties of blockchains is that they allow peer-to-peer transactions without the intervention of any central authority. Anonymous accounts secured with pairs of criptographic keys may exchange funds without the mediation of third party intermediary like a bank. Bitcoin is referred to as **Blockchain 1.0** as it only offers payment services. Other examples of blockchain 1.0 implementations include Monero, Dogecoin, Litecoin.

The transition to more advanced blockchains was leveraged with the development of smart contracts. ***A contract*** is a terminology that refers to a program that runs on a blockchain. Bitcoin uses some basic *contracts* only to ensure transactions' validity. With the introduction of **smart contracts** in Ethereum network in 2015, blockchains are capable of managing complex business logic and processes implementations. Under the hood, smart contracts are also accounts in the blockchain network, associated with a private, a public key and having a cryptocurrency balance. In addition they store code and data related to the code they store. In Ethereum a transaction may not only represent a transfer of eth, but also the creation of a smart contract or the execution with the ***EVM (Ethereum virtual machine)*** of some code in a smart contract. The immutability applies not only to financial transactions but also to transactions running a smart contract. Thus it is mandatory to develop comprehensive tests for smart contracts, as any invocation of a smart contract function cannot be reverted and errors caused by it are permanently stored on the blockchain.

The shift Ethereum took from a distributed ledger to a distributed state machine capable of running almost anything (the ***EVM-Ethereum virtual machine is Turing complete***) lead to a new paradigm of programming and to a new phase in the evolution of blockchain technologies, **Blockchain 2.0**.

The development of Decentralized Applications (**DApps**) especially **DeFI** applications, the creation of decentralized autonomous organizations (**DAOs**), the bloom of non-fungible tokens **NFTs** etc. are catalyst in transforming the web experience. The current critiques of nowadays online interaction: centralization of power, privacy issues, censorship etc., seemingly encourage adoption of ***Web*3**. Web1 is known as the read-only web. Web2.0 with it's climax in social media expansion, is the read-write web. We may say that Web3 will be the internet of read-write-own. User will have financial stakes or digital assets such as NFTs and will be able to control their identity. *self-sovereign identity* is a new approach to digital identity leveraged by Blockchain technologies. **Blockchain 3.0** will control assets, not only trade them, proving the the property right of the information. In [22] Gavin Wood, a founder of Ethereum states: "Web 3 will be a reimagination of the sorts of things that we already use the Web for, but with a fundamentally different model for the interactions between parties. Information that we assume to be public, we publish. Information that we assume to be agreed, we place on a consensus-ledger. Information that we assume to be private, we keep secret and never reveal. Communication always takes place over encrypted channels and only with pseudonymous identities as endpoints; never with anything traceable (such as IP addresses). In short, we engineer the system to mathematically enforce our prior assumptions, since no government or organisation can reasonably be trusted."

Blockchain network is organized as a peer-to-peer decentralized network, each peer (node) maintains the same copy of the history of transactions. This ensures that transactions are always accessible, as long as at least one node remains active. A centralized system has a single point of failure, if the server is not available then request cannot be fulfilled. Nodes vote and agree on the ordering and the validity of transactions, i.e nodes synchronize, by adhering to a ***consensus protocol***. To mentions some examples, Proof of Work ***PoW***, used in Bitcoin, gives the right to vote over the transaction history in terms of power of computations; Proof of Stake ***PoS***, used in Ethereum enables voters that stake a security deposit; Practical Byzantine Fault Tolerance, used in Tendermint, ***PBFT*** decide with a majority of 2/3 votes the state of the chain).

It is a well known fact that PoW based consensus protocols are consuming energy in an unsustainable rhythm, but this is not the only reason other consensus protocols have been adopted in blockchains, as alternatives to the model introduced in Bitcoin. Visa is capable of processing 1,700 transactions per second, while BTC has a TPS of $5-7$ (TPS stands for *transactions per second*). Also, in Ethereum network, in case of network congestion, fees for processing transactions are very high. The number of transactions processed per second and the costs of transactions are only two examples of how design choices in the consensus protocol impact performance, capacity to process transactions, system fault tolerance and scalability.

Vitalik Buterin, the founder of Ethereum, coin the term ***scalability trilemma***, based on CAP theorem, to emphasize that a blockchain investing in improving the chain itself (adopting layer 1 scaling solutions) can only satisfy two of three ideal benefits: security, decentralization and scalability. As decentralization is implicit in public blokchains, the tradeoff is to be made between security and scalability. **Security** refers to the ability of a blockchain to defend itself from attacks such as 51% attacks, denial-of-service (DDos), sybil attacks, double spending etc. Scalability is the capacity of

0 blockchain to increase transactions throughput, and to accept network growth without affecting the performance.

Layer 1 scaling solution improve the chain itself, for example by changing the protocol form PoW to PoS or by implementing sharding, i.e. dividing information between nodes.

Layer 2 scaling solutions enhance the blockchain efficiency by processing and validating transactions on separate networks. Two examples of scaling solution used by Ethereum are sidechains and rollups. **Sidechains** are separate blockchains running their own consensus protocols to speed up the transfer of assets. **Rollups** execute hundreds of transactions outside the blockchain, compressed the transactions together, and sends them to the main network.

With regard to blockchain taxonomy, there are certain classification criteria to take into account. If we consider ownership, a blockchain may be ***public***, ***private*** or ***consortium***. If we analyze restrictions imposed on newly joined members of the network, a blockhain may be ***permissioned*** or ***permissionless***. A public-permissionless blockchain (e.g. Bitcoin, Ethereum) allows anyone to participate in the consensus mechanism, to add new transactions and update the ledger state. There is no authority that owns the chain. In a public blockchain parties are not constraint to reveal their identity. All information is ***transparent***, anyone has access to the entire history of the block chain. Anyone can store multiple pairs of public-private keys to sign transactions or to prove ownership of his assets. This kind of ***pseudo-anonymity*** is not suitable for all kinds of applications. For instance in healthcare domain, or in insurance industry, only entitled participants should be able to access protected records.

For applications in domains that handle sensitive data and require strict access control and identity management, private blockchains are a more suitable solution compared to public ones. Private blockchains are partially decentralized, usually controlled by a single organization, or by a group of organizations in case of consortium blockchains. In a private-permissioned block chain (e.g. Hyperledger Fabric) only verified parties are allowed to join the network. It is worthwhile mentioning that private blockchain have usually better performance and lower security risks as the number of nodes is significantly lower than the number of nodes forming a public blockchain.

With an impressive variety of scaling methods and advancements in both transparency and security, blockchains hold immense potential to revolutionize the way we conduct transactions, verify product authenticity, manage identities, and share information.