SoK on Blockchain Evolution and a Taxonomy for Public Blockchain Generations

Thuat Do[*]
(1st) Department of Mathematics, The Hong Kong University of Science and Technology,
Clear Water Bay, N.T, Hong Kong;
(2nd) FPT Blockchain Labs, FHO, FPT Corporation,
Hanoi, Vietnam.

March 2023
This version is to be developed

Abstract

Blockchain has been broadly recognized as a breakthrough technology of the world. Web3, recently, is emerging as a buzzword, indicating the next generation of Internet based on Blockchain, envisioning *the Internet of Money* to store and transfer value. However, when people want a comprehensive view throughout advancements in the Blockchain space, there is a missing in the academic domain and scientific publications regarding distributed ledger technology (DLT) classification and taxonomy for the evolution of public Blockchain generations. In this research, the author attempts to classify DLTs in terms of data structure (ledger type), governance and accessibility. Furthermore, based on the well-known problems and the most technical challenges in Blockchain space, the author studies breaking and significant inventions of various blockchain protocols to give a taxonomy for the evolution of four public Blockchain generations, blockchain layers (0, 1, 2, 3). The first and second generations are dominated by Bitcoin and Ethereum, respectively. The latest state-of-the-art blockchain protocols are developing and shaping the third and fourth generations, where several "*Ethereum-killer*" candidates are trying to solve major problems, to offer fantastic functions and capacity, by their own outstanding innovations and distinguished architectural designs. This work helps readers quickly capture historical evolution and innovations of Blockchain, envisioning the next advancements of Web3 as well as the Internet of Value (Internet 2.0).

Keywords: *Blockchain taxonomy, Blockchain evolution, Blockchain generations, multi-chains, public blockchains*

1 Introduction

This section provides a literature review on blockchain classification and taxonomy, both scientific publications and non-academic articles. It also summarizes the most important contribution of the paper and research method. Section 2 briefly summarizes the history of Blockchain technologies, the birth of Bitcoin - the first practical blockchain network of the world invented by Satoshi Nakamoto. Section 3 presents several database designs of distributed ledger technologies (DLTs). Section 4 gives a classification for DLTs and blockchains under operation and accessibility views. Section 5 extensively presents major problems and challenges of public blockchains, their innovation and evolution, then introduces a taxonomy of four public blockchain generations. Section 6 gives a short overview on the concepts of layers (0, 1, 2, 3) on blockchains. Section 7 is a brief discussion on Web3 and the future of the next generation of Internet, together with a conclusion of the work. Readers can find there application of our taxonomy on popular public chains.

[*] Thuat (Paven) DO is a PhD candidate at The Hong Kong University of Science and Technology, has been studying Blockchain Technology and its applications since 2018, now focusing on blockchain data analytics and reputation ranking system for Web3 space, founding Octan Network project to implement the concept into commercial production. He is currently Head of Development, FPT Blockchain Labs, FPT Corporation, Vietnam, building consortium blockchain platform for enterprise. He is a cofounder and former CTO of Spores, a multi-chain NFT marketplace and Web3 game launchpad. *Contact email: thuat86@gmail.com*

1.1 A literature review

Blockchain has been broadly recognized as a breakthrough technology of the world. Web3 refers to the next generation of Internet applications based on blockchain protocols, envisioning *the Internet of Money* (termed by Andreas M. Antonopoulos [1] in his book with the same title) to store and transfer value. Alternatively, some authors [2, 3] introduced and defined the concepts of *Internet of Value*, discussed how blockchain technologies connect and change businesses.

In academic field, many scientists have extensively investigated Blockchain. Under the views of system architects, X. Xu et al. [23], in 2017, proposed a taxonomy capturing significant architectural characteristics of blockchains and the impact of their principal designs which are useful for architectural considerations on the performance and quality attributes of blockchain-based systems. In 2019, Paolo Tasca [20], from bottom-up, deconstructed blockchains into their building blocks, then hierarchically classified into main and sub-components to identify and compare. Then, under technical view, a taxonomy tree is introduced across different blockchain architectural configurations.

Shehu M.S. et al. [29], in 2018, used existing methods in information systems to develop a classification regarding blockchain platforms. Olga Labazova et al. [21], in 2019, and Sam G. et al [22], in 2020, classified applications of Blockchain technologies in various industries and domains. Omer F. Cangir et al. [28], in 2021, proposed categorization for blockchain based distributed storage technologies, then used the taxonomy to compare and evaluate various solutions.

Considering consensus as the heart of any blockchain, in 2019, Shehar Bano et al. [24] proposed a systematic framework to study blockchain consensus mechanisms, their security and performance properties. In 2020, Sarah Bouraga [25] reviewed and analyzed 28 consensus protocols, then comprehensively categorized them under a framework of origin, design, performance and security. Jeff Nijsse [26] and Garay J. et al. [27] also proposed taxonomy for consensus mechanisms.

In the articles of Stephan Cummings (Feb 2019), Ruchika Dubey (Sep 2019), Kirsty Moreland (May 2021), Nathan Reiff (Sep 2021), Willigut (Oct 2022), The Nation Thailand (Nov 2022), the writers had various attempts to classify public blockchain generations. They almost agree on the 1st and 2nd generations, while having a controversy on the 3rd and the next ones. However, it was lack of scientific research methods in those mentioned articles.

1.2 Paper contribution

People cannot find a comprehensive and summarized view throughout key milestones and advancements along with the history of evolution in the Blockchain space. There is a missing in the academic domain and scientific publications regarding DLT classification and taxonomy for the evolution of public Blockchain generations. In this research, the author aims to fulfil the gaps.

1.3 Research method

The author studies Blockchain Evolution under historical points of view, hence finds out what problems and challenges are significant to motivate innovations, what inventions are breaking to shape a new chapter for important advancements of Blockchain Technology. More explicitly, instead of digging into consensus mechanisms, application perspectives or deep technology designs of blockchain protocols, the author considers the following criteria to categorize DLTs and blockchains, to classify four evolutionary generations of public chains.

- Development history;
- Major problems addressed to solve (e.g. digital cash system, decentralized settlement, scalability, Blockchain Trilemma, high performance, cross-chain interoperability, composability);
- System architecture:
  - Types of ledger (database): UTXO vs account, linear vs DAG
  - Governance models: permissioned vs permissionless
  - Access modes: public vs private
- Other significant technological designs: consensus, virtual machine, application-oriented modularity.

2 The early History of Blockchain

The "chain of blocks" concept with a cryptographic hash function was presented in the 1979 dissertation of Ralph Merkle [8]. The structure Merkle linked information is now well-known as "Merkle hash tree." The very first blockchain-like protocol by a cryptographer, David Chaum[1], appeared in his 1982 dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups." In 1991, Stuart Haber and W. Scott Stornetta [6] proposed a chain of blocks design secured by cryptography technique to make document timestamps tamper-resistant. In 1992, Haber, Stornetta, and Dave Bayer [7] introduced Merkle trees to the chain design to improve its efficiency. The historical origin and variations of blockchain technology is surveyed in [5] by Sherman, Alan T et. al (2019).

Hash function, Merkle tree, block-chaining design and public key cryptography (e.g. Elliptic Curve Digital Signature Algorithm) are fundamentals for Satoshi Nakamoto[2] to create Bitcoin, the first practical blockchain network in the world. Bitcoin's whitepaper [4] was publicly available on 2008 at the website `www.bitcoin.org` and Bitcoin mainnet went live on 3 January 2009. The Bitcoin Whitepaper entitled *"Bitcoin: A Peer-to-Peer Electronic Cash System"*, and in the Bitcoin's genenis block, the first coinbase transaction messaged the string *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"* mentioning the title of an article on The Times of London admid 2008-2009 financial crisis in U.K, U.S and several developed nations caused by failure of centralized bank systems. The Great Recession followed with extensive impact on global scale for nearly a decade.

In the author's opinion, by inventing Bitcoin, Satoshi Nakamoto made critical dedications to the world.

1. He orchestrated designs of distributed system, immutable data structure and cryptography techniques in a single software (i.e. Bitcoin core).

2. He introduced Nakamoto Consensus, the first and the most popular Proof of Work (PoW) consensus algorithm in the Blockchain space.

3. He introduced a tamper-proof ledger architecture (the first replicated state machine of the world).

4. He realized the concept of electronic cash system, more explicitly, cryptography currency (or cryptocurrency), together with the concept of toke economics (or tokenomics) based on game theory.

5. Satoshi Nakamoto fathered the philosophy of decentralized system and decentralized governance which contrasts to centralized entities.

Bitcoin, as the first blockchain network, has become the technology fundamentals for all the following blockchain platforms, including Ethereum. Bitcoin, as the first cryptocurrency, has been becoming the digital gold of the world, a miracle in the 21st century, and potentially promoting a new order of global money and finance systems. Readers can find more about Bitcoin in [1].

3 Types of Distributed Ledgers: UTXO vs Account, Linear vs DAG

Blockchain, or in general, Distributed Ledger Technology (DLT), refers to the technological infrastructure and protocols that allows simultaneous access, validation, and record updating in an immutable manner across a network that's spread across multiple entities or locations. DLT requires a peer to peer network accompanied with a consensus algorithm to maintain refer the distributed shared database (or ledger), which eliminates the need for a central entity to keep the ledger functioning correctly.

Among distributed ledgers, there are two types of balance record-keeping models. The first method is called the UTXO (Unspent Transaction Output) which is similar to physical cash (bank notes). UTXO model (see Fig. 1) is used by Bitcoin, Cardano, Dogecoin, IOTA, etc. The second method is account model which keeps tracking the balance of every account (i.e. the state change of the entire system) on every block, similarly to internet banking systems. The account model is used by Ethereum, Polygon, BNB Chain and almost smartcontract platforms (which also offer Turing completeness). While UTXO systems are much simpler to implement and deploy but very limited in applications, account model provides better programming capacity with complexity.

[1] David Chaum is credited as the godfather of cryptocurrency. He introduced the first digital currency in 1995 but failed in practice.

[2] Pseudonym of an anonymous programmer or an unknown group of cryptographers.

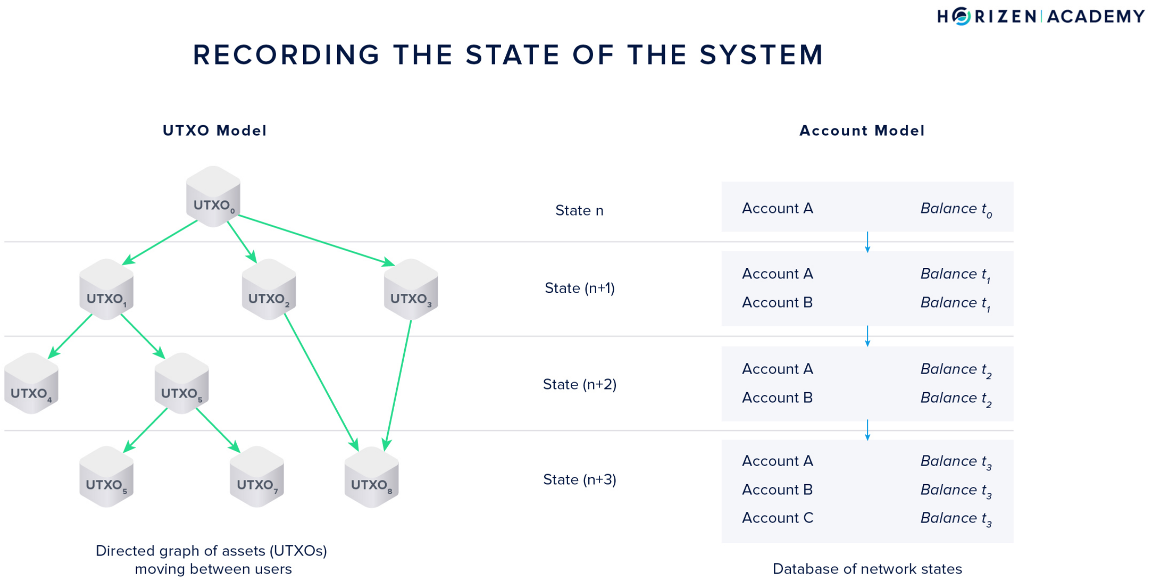

Fig. 1. UTXO vs Account model, by Horizen Academy

By data structure, distributed ledgers are either a linear chain or a Directed Acyclic Graph (DAG) of transactions. The linear structure is total-ordering, simply links blocks of transactional data by hash pointer technique, hence namely "block-chain", popularly used by Bitcoin, Ethereum and many others. DAG is partial-ordering, a non-linear and more complex structure of incoming transactions linked with previous ones. DAG (see Fig. 2) is used by IOTA, Avalanche, Hedera. Linear design provides a synchronicity (plus latency variation) but limited throughput and scalability. Linear ledgers are also convenient to equip virtual machines (VMs) and smartcontract programs running on top of linear ledgers. DAG, on the other hand, allows to build distributed systems with higher throughput capacity and horizontal scalability. However, DAG architecture is asynchronous and difficult to built VMs and smartcontracts on top. IOTA is a popular DAG-based distributed system. It launched mainnet on July 2016, but smartcontract beta-devnet was released 5-year later. Avalanche builds a distributed system of linear chains (to host smartcontracts) attached with a DAG-ledger (for asset issuance, accounting & exchange). Hedera, Avalanche and Cardano have attempted to build their VMs on UTXOs but the platforms has modest traction faraway from targets and expectation.

Linear chains or non-linear ledgers can be associated with either UTXO or account model. However, in DLT space, the most popular and active smartcontract platforms are built on account model and linear-chain structure (with total-ordering). Readers visit Table 3 for a summary.

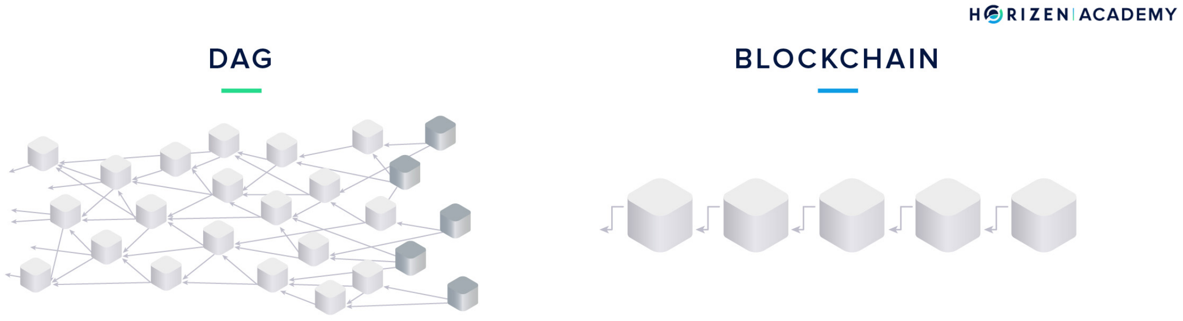

Fig. 2. DAG vs linear block-chain structure, by Horizen Academy

Table 1
A summary on ledger types

	UTXO	**Account**
Linear	Bitcoin, Cardano	Ethereum, Tron
DAG	IOTA, Avalanche	Hedera

4 Categories of DLTs & Blockchains

Along with development progress of Blockchains, DLTs and cryptocurrencies, many researcher have attempted to give a categorization for the space. D. Puthal et. al. [9] proposed a classification of Blockchain into public, private and consortium categories. Among others, the author proposes a taxonomy for DLTs and Blockchain space considering several characterizations as followed:

- Types of governance or permission to join the network as operators and governors;
- Types of accessibility (access modes) to the DLT as end users.

By *types of access mode*, we have *public* versus *private* DLTs. The former is fully transparently opened for everyone to watch and use the ledgers, while the later only allows access regarding certain registered accounts.

By *types of governance*, we have two major classes: *permissioned* versus *permission-less*. Readers see Table 2 also.

- **Permissioned blockchains** refer to a class intentionally designed for enterprise, in which new registered nodes need approval from an authority or existing operators to become a new legit operator in the network. This means a (total or partial) trust model needed. They may be specified as either *private chains* used for data sharing within a single organization, or *consortium chains* (alternatively, federated or federation chains) used for collaboration between many companies. The former is closed, total trusted and may not need consensus, while the later is partially open and trusted, and required a consensus mechanism among operating, governing nodes. Quorum, Hyperledger Fabric and Corda are the most popular frameworks for enterprise blockchains. Many companies use their open sources to develop their own private chains or consortium chains for various purposes. Almost permissoned DLT platforms are associated with multiple levels of privacy and accessibility.
- **Permission-less blockchains** (or permissionless blockchains) are open for every to join as operators, miners or validators, meaning trustless. This class, sometimes, mis-refers to *public blockchains* dominating the Blockchain space with hundreds of active and vibrant networks and platforms, typically with Bitcoin, Ethereum, BNB Chain, Dogecoin, Cardano, Polygon, Polkadot, and many others.

Noting that some public blockchains are still permissioned, for example, Hedera, POA Network, XRP Ledger, Stellar, VeChain, etc. However, on the other side, as the author's best knowledge, no private chain is permissionless (see Table 2).

Table 2
Blockchain and DLT categories

	Permissionless	**Permissioned**
Public	Bitcoin, Dogecoin, Ethereum, Cardano `fully transparent & trustless`	Hedera, Stellar, XRP Ledger `fully transparent, partially trusted`
Private	NA	Hyperledger, Corda, Quorum `partially transparent & trusted`

5 Taxonomy on Public Blockchain Generations

Among others, for an easy reading, the author follows the historical advancement of Blockchain Technology to propose a taxonomy regarding evolutionary generations of public DLTs and blockchains, considering several criteria and characterizations as followed:

- Development history;
- Major problems addressed to solve (e.g. digital cash system, decentralized settlement, scalability, Blockchain Trilemma, high performance, cross-chain interoperability, composability);
- System architecture and technological designs: network layer, consensus, virtual machine, application-oriented modularity, etc.

5.1 The 1st Blockchain generation

The 1st generation remarked by Bitcoin birthday on 3 Jan 2009, noting its mainnet launch date - the genesis block. The followers are XRP[3] (launched 2 June 2012), Dogecoin (launched 6 December 2013), Stellar - XLM (launched 31 July 2014), utilized Byzantine Fault Tolerance (BFT) consensus to develop digital currency for banking and financial sector. Litecoin (mainnet launched 13 October 2011) Bitcoin Cash (launched 1 August 2017), Dogecoin (launched 6 December 2013), all aiming to build corresponding crypto-currencies (alternatively, digital currencies) generated and kept by distributed ledger technologies as introduced and visioned by Bitcoin and its creator - Shatoshi Nakamoto. These cryptocurrencies aims to solve against the centralized, nontransparent control problem of fiat currencies and bank systems, then heading to the future of money which is decentralized, transparent and censorship resistant, backed by community and built for community.

5.2 The 2nd Blockchain generation

The 2nd generation refers to blockchains proposed to solve two major problems: **privacy transactions** and **programmable money**. Dash[4] (launched 18 January 2014), Monero (18 April 2014), Zcash (28 October 2016) are designed to hide the mapping between senders and receivers, hence offering transaction privacy in contrary to Bitcoin and the 1st blockchain generation.

Programmable money and decentralized applications are not available on Bitcoin and cryptocurrency network based on scripting languages. Vitalik Buterin (born 1994) had a great approach with Blockchain Technology as he conceived and found Ethereum in 2013, (visit his vision in Ethereum Whitepaper). Ethereum mainnet launched at 30 July 2015, introduced a Turing-complete platform to enable arbitrary smartcontract implementing and application programming on top of blockchain which was impossible and regarding Bitcoin, Dash, XRP, Stellar and others at that time. Vitalik Buterin and Ethereum Foundation's Imagination was a breakthrough in the Blockchain evolution, overhauling Bitcoin Core, inventing and paving the development way for the most important concepts in the Blockchain Space: smartcontract platform, tokenization, tokenomics, decentralized finance (DeFi) & stablecoins, decentralized autonomous organization (DAO), decentralized file storage, decentralized data feed (oracle), etc. Turing-completeness on blockchain, Ethereum Virtual Machine (EVM) and Solidity language, were outstanding inventions of Ethereum developers dedicated to the Blockchain space changing the world. Additionally, Ethereum runned Ethash-PoW algorithm, protecting the network against ASIC-mining, an issue on Bitcoin and its hard-forked networks.

Up to now, almost public blockchains are smartcontract platforms (or layer-1s in Section 6) counted by hundreds. Such typical examples after Ethereum are EOS (June 2018), Tron Network (July 2018), Polygon (June 2020), BNB Chain[5] (September 2020).

Currently, Ethereum is still the leading smartcontract platform in terms of developer & user community, application diversity, DeFi prosperity and composability. EVM is the most popular runtime environment for smartcontracts, and Solidity is the most smartcontract programing language[6].

Additionally, IOTA (launched 11 July 2016) introduced a Tangle protocol based on DAG, targeting a cryptocurrency network oriented for IoT devices and their applications, with theoretically unbounded scale.

[3] XRP is formerly called XNS, a cryptocurrency built by and affiliated with Ripple Labs.

[4] It was named Xcoin at launch, then Darkcoin.

[5] It was rebranded in February 2022 from Binance Chain and Binance Smart Chain - BSC. Binance Chain is based on Tendermint Core but no runtime environment (VM). It is now the beacon of BNB Chain, while BSC is the EVM-chain, making BNB Chain a multi-chain system.

[6] Solidity was created by Gavin James Wood (or Gavin Wood), cofounder of Ethereum, chef architect of EVM. It is mostly used to implement smartcontracts on Ethereum and EVM-compatible platforms like Tron, BNB Chain, Polygon.

Essentially, the 2nd generation remarked by Ethereum and the emerging of **smartcontract platforms**. Such blockchains have gained plentiful applications and wide range of adoption, while privacy chains (alternatively, privacy coins, as mentioned, Dash, Monero, Zcash) have not, even their impact and adoption have been going down due to lack of applications and regulatory concerns.

5.3 The 3rd Blockchain generation

The 3rd generation attempted to solve the problems of Ethereum smartcontract platform: **scalability** and the **Blockchain Trilemma**. In the past years, PoW-based Ethereum normally processed 14 transaction per seconds (TPS), congestion and gas spikes often happened on the network. Scalability and gas efficiency became the biggest challenge and concern for blockchain developers during 2016-2018. Scalability indicates ability of a blockchain to proccess more transactions when adding computing resources. This is very limited (even nearly impossible) for Bitcoin and PoW-Ethereum.

Many projects, Cardano mainnet launched in September 2017, EOS launched in June 2018, Tron Network launched in July 2018, proposed to build smartcontract platforms with better performance and scale, then killing Ethereum. They had novel consensus mechanisms based on Proof of Stake (PoS) to replace energy-consuming PoW and to enable scaling, accompanied with innovations on architectural designs and virtual machines. Cardano runs PoS Ouroboros and builds virtual machine (VM) on top of UTXO assets, white EOS and Tron are both Delegated Proof of Stake (DPOS) with 21 and 27 validators, offering much higher performance compared to Ethereum, respectively. Hedera introduced a public, permissioned ledger protocol (as an alternative to blockchain) based on invention of Hashgraph (non-linear) architecture and asynchronous BFT (aBFT) consensus. Hedera mainnet launched on 14 August 2018, claiming it can process around 10k TPS with ability to scale more. Polygon (former named as Matic Network), launched in June 2020, proposed to scale Ethereum as a sidechain solution (or layer-2 scaling) based on Plasma Bridge. Now, Tron and Polygon have plentiful of applications and wide adoption, ability to process up to thousands TPS. On the other side, EOS platform is complete with many merits in technology fundamentals but lack of applications due to the conflict between EOS community and Blockone (the initial developer of EOS). Cardano has PoS-Ouroboros consensus as its most important innovation, but it is incomplete, limited development tools for smartcontract implementation and application deployment. UTXO model results in difficulties to build VM. Haskell, the language to develop Cardano and to build contracts on its top, is also unfamiliar with developer community.

The Blockchain Trilemma was the most notable problem during 2018-2020, termed by Vitalik Buterin, raising *"decentralization, security, scalability"* triangle which is difficult to balance among those triple. It was an observation from Hedera, EOS, Tron and other projects offering higher performance than Ethereum but somehow sacrificing decentralization. More accurately, the Triangle is decentralization, safety, scalability, according to S. Leonardos et. al. [18]. In the paper, the authors explicitly introduced *PREStO*, a formal and systematic framework to assess blockchain consensus protocols under five axes: *optimality, stability, efficiency, robustness, and persistence.* Fig. 3 presents a visual representation of the Blockchain Trilemma in relation to the PREStO framework. The trade-off between safety, scalability and decentralization is precisely captured by the corresponding subcategories in optimality, efficiency and stability. Robustness and persistence offer alternative approaches for a long-term resolution of the Trilemma.

- Fig. 4 presents a dealing with the Blockchain Trilemma: The green dot denotes an ideal protocol that satisfies all three properties (safety, decentralization, and scalability) in equilibrium. The blue dot denotes a protocol that cycles around the ideal solution and which satisfies the incompatible properties in a weakly persistent (recurrent) manner.
- Scalability and decentralization are often held back by safety, but safety tends to be compromised by any shift on a network that offers scalability.
- Projects either choose to focus on two out of three or work on finding a solution to tackle the Trilemma once and for all.
- Finding a balance between the three properties is very difficult. However, a "good-enough" solution to the problem could lead to greater adoption of cryptocurrency and Blockchain and a wide-spread use of the technology across industries and the globe.

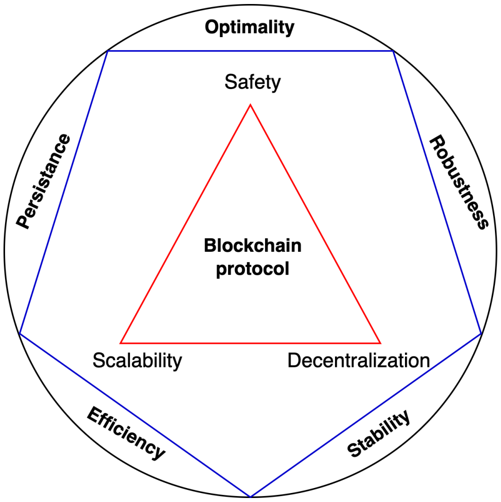

Fig. 3. Blockchain Trilemma in relation to the PREStO framework.

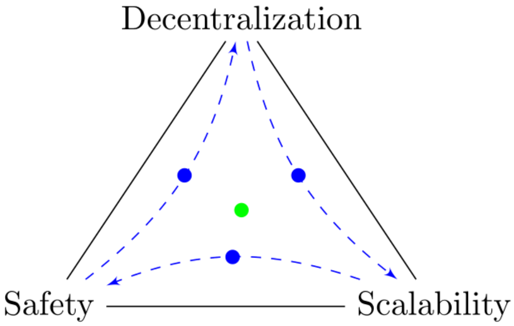

Fig. 4. Dealing with Blockchain Trilemma

Silvio Micali, a scientist at MIT, founded Algorand (mainnet launched in June 2019) claiming to solve the Blockchain Trilemma by inventing a Pure Proof of Stake (PPoS) consensus and a verifiable random function (VRF). Although Silvio Micali states that his team can boost Algorand to 46000 transaction per second (TPS), according to Algorand 2021 Performance report, Algorand throughput (average 1300, max 6000 TPS) at present is rather similar to Tron, EOS, Polygon. Audiences can refer to Mauro Conti et. al. [17] presenting a security analysis of Algorand and an attack scenario by exploiting a security flaw in the messages validation process of the Byzantine Agreement.

Regarding scalability problem, an important solution is **sharding technology**, partitioning a large database and a network into many shards to multiply performance. Readers refer to Gang Wang et al. [30] for a systematic and comprehensive review on sharding techniques and protocols. Zilliqa (mainnet launched on 31 January 2019), Near Protocol (22 April 2020), and TON - Telegram Open Network (May 2021) are frontiers among sharding protocols. Sharding protocols are supposed to be promising for great number of TPS (up to 100k TPS and more). After The Merge (successfully executed on 15 September 2022) transitioned Ethereum to PoS consensus mechanism, Blockchain communities are waiting for Ethereum 2.0 with sharding upgrades to be officially released. All sharding chains require a special chain at the center to govern and coordinate all other shards. They can be considered as *homogeneous multi-chain systems*, contrasting with *heterogeneous multi-chain systems* classified as the 4th generation in Section 5.4.

Overall, although a candidate for The Blockchain Trilemma is not yet acknowledged widely, radical innovations of the 3rd generation are very significant to advance Blockchain Technology and to bring extensive applications and usecases to the Blockchain and cryptocurrency space, heading to mainstream adoption in the future. The 3rd generation are remarked by innovations of PoS and DPoS consensus mechanisms, hashgraph design and sharding technologies.

5.4 The 4th Blockchain generation

The fourth generation continues to deal with blockchain scaling solution, and also raise a new big challenge in cross-chain communication and application-custom flexibility.

High performance blockchain is another approach to the scaling problem, firstly introduced in commercial production by Solana (Mar 2020). Aptos, Parallel Chain projects follows to build monolithic chains with high throughput (measured by TPS) and fast finality (i.e. low latency). Their developers claim they can build such single and linear chains to reach tens of thousand TPS and few-second finality. In Solana Whitepaper [10], Anatoly Yakovenko said that the protocol can reach up to 71000 TPS thank to a deterministic block producer selection mechanism, Proof of History and Tower BFT consensus. Rati Gelashvili et. al. [15] presents Block-STM, a parallel execution engine for smart contracts, running in production on Aptos, which helps the chain achieves up to 110k tps in the Diem benchmarks and up to 170k tps in the Aptos benchmarks. Unfortunately, in some way, they sacrifice security (more explicitly safety and liveness) and/or decentralization. People has recorded 7 times of outage on Solana since mainnet launch on 16 March 2020. Aptos just launched its mainnet on 12 October 2022, currently having 102 active validators and few real transactions (visit `https://explorer.aptoslabs.com/` for real-time explorer on Aptos mainnet). Parallel Chain [16] is yet in the third testnet, but proposing a hight throughput up to 100k TPS from a single node and the performance proportionally increasing with number of nodes.

Cross-chain interoperability is one among major problems and big challenges of Blockchain technology. By sovereignty nature, each chain is separated and isolated from all others. Simply speaking, it is impossible to move bitcoin on Bitcoin Network to Ethereum (i.e. asset transfer from a chain to another). More generally, how to make different blockchains communicate and interoperate with each other?

Cosmos (mainnet launched on 13 March 2019), Polkadot (launched 26 May 2020), by radically outstanding inventions, are pioneers to propose *heterogeneous multi-chain systems*, for which a special chain at the center governs and coordinates all other chains (built on a standardized framework) in the system. This architecture allows triple-addressing scalability, cross-chain interoperability, and customization for various application-purposed chains. Cosmos has a Cosmos Hub and zones based on Tendermint Core and IBC, while Polkadot has a Relay Chain and parachains built on BABE-GRANDPA. Avalanche (launched 21 September 2020), Internet Computer Protocol - ICP (launched on 7 May 2021) then follows with their distinguished innovations. Avalanche differentiates itself by a hybrid architecture of DAG and linear ledgers, of UTXO assets and account model, powered by Snowman consensus, and governed by P-Chain at the center. On the other hand, ICP is built on Chain-key cryptography derived from threshold BLS signatures, multi-subnet architecture governed by a Network Nervous System, and Motoko smartcontract language. ICP mainnet can process 11500 TPS normally, and horizontally scale infinitely with every thing feasibly hosted onchain. Following the multi-chain direction, BNB Chain, Polygon, Tron Network and Klaytn have been upgrading and transforming to heterogeneous multi-chain models (or modular blockchain systems) since early 2022.

Despite of extremely high complexity in design and development, multi-chain system is a very important advancement to address scalability, interoperability and application-custom modularity, potentially to bring a higher degree of composability according to Section 5.5 and Jesse Walden [11].

Although sharding chains are classified as the 3rd generation in Section 5.3, we may consider such homogeneous multi-chain systems as the 4th Blockchain generation, because they share some similarities with heterogeneous systems, e.g. complex architecture, addressing to solve scalability, secure cross-shard interoperation at once, potentially offering a new degree of scalable composability (see Section 5.5).

5.5 On Blockchain composability

According to Jesse Walden [11], a blockchain platform is composable if its existing resources can be used as building blocks and programmed into higher order applications. Composability is important because it allows developers to do more with less, which in turn, can lead to more rapid and compounding innovation. On the other words, composability is a very important property of smartcontract platforms (or Turing complete blockchains) presenting a seamless connection, interaction, composition across contracts and applications. In the article, Jesse Walden studies the evolution of blockchain computing, then sketching out a mental model of four distinct eras, each with varying architectures and priorities with regards to composability:

- Calculator Era: Application specific (e.g. Bitcoin), limited composability.

- Mainframe Era: Turing complete (e.g. Ethereum, BNB Chain), high composability.
- Server Era: Application specific (e.g. Cosmos, Polkadot, Avalanche, other multi-chain systems), punt on composability.
- Cloud Era: Turing-complete (e.g. ICP, Ethereum 2.0, etc), scalable composability.

We have observed a big success of Ethereum in terms of composability. Currently, monolithic chains (i.e. one single chain executes all), for instance, Ethereum, Solana, Tron, BNB Chain, Polygon, Algorand, have been providing the best *composability* in the Mainframe Era. We are looking forward to showing of the same property on Server Era and Cloud Era of Blockchain computing (i.e. pointing to heterogeneous and homogeneous multi-chain systems). This also matches with our generation classification.

5.6 A summary

Although some people assume impossibility to find a solution for The Blockchain Trilemma, advancement in the space is fast with bundles of breaking innovations and initiatives. We observed and analyzed the most significant criteria and characterizations to classify public blockchain generations as following.

- Major problems addressed to solve in Blockchain space: digital currency, decentralized settlement, scalability (in particular, high performance blockchain), the Blockchain Trilemma, and cross-chain interoperability.
- Breaking architectural designs (network layer, ledger database, custom modularity)
- Novel consensus mechanisms
- Innovative virtual machines (i.e. Turing-complete runtime environments) and smartcontract language

In Table 3, we summary four generations (and its typical examples) along with Blockchain Evolution, addressing the most significant problems and protocols solving them, corresponding with their consensus type and most important inventions. We also include performance[7] of the protocols: real TPS (TPS) on mainnet, theoretical possible-Max TPS, time to transaction finality (TTF) or latency, although it is difficult to measure and there is a confuse between performance versus scalability (see J. Bonneau [19]).

Gens	**Problems**	**Protocols**	**Cons.**	**Inventions**	**TPS**	**Max**	**TTF**
1st	P2P cash system	Bitcoin 2009	PoW	Nakamoto Consensus	7	7	60m
	Censorship-resistant			Decentralized ledger			
2nd	Smartcontract	Ethereum 2015	PoW,	Turing-completeness	15	30	6m
	Dapps		PoS	EVM & Solidity	20	84	6m
3rd	Scalability	Hedera 2018	BFT	Hashgraph, aBFT	2k	10k	6s
	Scalability	Tron 2018	PoS	DPoS, TronVM	2k	4k	36s
	Blockchain Trilemma	Algorand 2019	PoS	Pure PoS & VRF	1k	6k	4s
4th	Interoperability	Cosmos 2019	BFT	Tendermint & IBC	1k	10k	7s
	Interoperability	Polkadot 2020	NPoS	BABE-GRANDPA	1k	100k	60s
	High performance	Solana 2020	PoS	PoH & Tower BFT	4k	50k	1s
	High performance	Aptos 2022	BFT	MOVE & MoveVM	2k	170k	1s
	Scalability & Interop.	ICP 2021	PoS	ChainKey cryptography	11k	infinite	2s
	Scalability & Interop.	Avalanche 2021	PoS	Hybrid ledger, Snowman	1k	4500	3s

Table 3
A summary on four generations of public blockchains

[7] Note that in this paper, performance indexes are neither a focus nor significant investigation of the author, and they may be different with other sources or measurements (read [19] also). The author includes the indexes as a supplement but not important chracterizations to Blockchain evolutionary classification.

6 Layers in Blockchain: L0, L1, L2, L3

Blockchain communities are waiting for Ethereum upgrades heading to sharding stage and more scale solution after the PoS-Merge. Meanwhile, many scaling solutions (layer-2, side-chain, state-channel, rollups, etc) have been proposed for Ethereum scaling which can be generated to apply for other layer-1s as well. Among them, Zero-Knowledge Rollups (ZK-rollups) are emerging as secure and seamless solutions, extensively invested and developed for Ethereum scaling layer-2s. More generally, we will investigate the concept of four layers in Blockchain.

Layer-0 (L0) is the underlying protocol and infrastructure upon which multiple layer-1 blockchains can be built. L0 often solves interoperability, scalability and application-flexible modularity (i.e. customizable blockchain SDKs) at once. This is the same as heterogeneous multi-chain systems: Polkadot, Cosmos, Avalanche, Internet Computer (ICP). Readers are referred to Binance article about Layer-0.

Layer-1 (L1): A layer-1 blockchain refers to the underlying or base protocol that provides the foundation for the network and its applications. An L1 is either a monolithic chain at origin (e.g. Bitcoin, XRP, Ethereum, Solana) or built on SDKs of a certain L0 (e.g. Terra and Cronos built on Cosmos SDK, Moonbeam built on Polkadot Substrate). L1s are either general-purposed smartcontract platforms (e.g. Ethereum, Solana, Moonbeam, etc) or for application-specific purposes (e.g. Bitcoin and XRP for cryptocurrency and settlement, Terra for programmable money, Theta Network for video streaming, etc).

Layer-2 (L2) refers to scaling solutions that processes transactions off a layer-1 to reduce its workloads and save gas cost. Many layer-2 scaling solutions for Ethereum have been proposed and developed with different technologies and purposes, then applying for other L1s.

- Polygon is a layer-2 sidechain, anchored to Ethereum via Plasma bridge to build a general-purposed smart-contract platform. Polygon has its own native currency for gas payment.
- Polygon Hermes is building zkEVM as a generalized layer-2 (i.e. offering EVM) based on ZK-rollups. Polygon is evolving as a comprehensive scaling foundation on top of Ethereum with many available SDKs for bundles of applications, envisioning to a heterogeneous, interoperable multi-chain system on Ethereum.
- Arbitrum One, Optimism, Boba Network are generalized layer-2s based on optimistic rollup.
- Loopring, zkSync, zkSpace, AzTec, all based on ZK-rollup, are application-specific layer-2s for payment, exchange, or NFTs.

Layer-3 (L3) is unpopular, refers to application-specific layer, including games, wallets, privacy and other DApps. Sep 2022, Vitalik Buterin, in an article on layer-3 scaling, discussed necessity and intuition of L3, then proposed some meaningful approaches.

- If L2 is for scaling, then L3 is for specific functions (e.g. privacy).
- If L2 is for generalized scaling, L3 is for customized scaling (i.e. specified applications).
- If L2 is for trustless scaling (ZK-rollup), layer-3 is for weakly-trusted scaling (validiums).

Layer-2, especially, ZK-rollups and zk-EVM are emerging as the most interesting solution for Ethereum scaling at presence. Vitalik B. gives *a guide to Rollups*, scaling Ethereum hundred of times regarding specified applications, and classifies *different types of zk-EVMs* offering Turing-complete runtime environment based on Zero-Knowledge techniques. However, for thousands of TPS, he still heads to incoming sharding technology (i.e. Ethereum 2.0).

7 Web3 and conclusion

Web2 refers to the internet of information as most of us know and use every day. Tech giants (e.g. Apple, Amazon, Google, Facebook, etc) dominate and control almost everywhere in the World Wide Web, in which the companies provide many platforms and services in exchange for user data. Web3 or the third Web generation is emerging as a hot key word recently in which developers are ambitious to build a next generation of Internet applications on top of blockchain protocols. Web3 leads to a new iteration of the World Wide Web which incorporates decentralization, Blockchain technologies and token-based economics. By utilizing Blockchain as the backbone and foundation, Web3 emphasizes user ownership and community governance which is never recognized in the Web2 space. Although many limitations and challenges are needed to overcome, Web3 envisions *the Internet of Money* (termed by Andreas M. Antonopoulos [1] in his book with the same title) to store and transfer value natively on the Internet, all controlled by users. Alternatively, some authors [2, 3] introduced and defined the concepts of *Internet of Value*, discussed how blockchain technologies connect and change businesses. Michael Gronager, CEO and cofounder of Chainalysis, in his speech at World Economic Forum - Davos 2023, discussed why cryptocurrency needed for Internet of Value, and opportunities of Web3 to improve billion of lives unsupported by conventional banking & finance systems. Web3 technologies are potential to

- Unlock new use cases in finance those impossible due to the illiquidity of traditional assets.
- Increase transparency and foster more direct relationships among producers, sellers and customers.
- Bring decentralization to the business world by enabling user ownership and community governance.

Before seeing a clear landscape of Web3 applications in practice and real life, we are observing bundles of blockchain protocols aiming to build decentralized assets and computing infrastructure, as well as decentralized applications for a next generation of Internet. After decentralized finance (DeFi), NFT and gamefi waves (brought hundred billions of dollar and millions of users to crypto space), thousand of social & media platforms, decentralized autonomous organizations (DAOs), are building on Web3. People may expect next trends in socialfi, DAO, edutech, healthcare, insurance, and so on, to extend the application and adoption of Blockchain and Web3. Some typical examples shows that many projects are developing infrastructure and applications for Web3.

- Filecoin is a decentralized file storage network.
- Lens Protocol is developing a composable and decentralized social graph where many Web3 social platforms and applications can build on its top. Chainflix is a blockchain-based video sharing platform.
- The Graph is an indexing protocol for Ethereum-compatible chains and IPFS networks to make onchain data more accessible to everyone.
- Ocean Protocol and Golem are building marketplaces for data and computing power, respectively, powered by blockchains and tokenomics.
- Chainlink and DIA, decentralized oracle networks, feeds offchain data to smartcontracts.
- Ethereum Name Services provides decentralized naming for website domain, wallets, while Civic offers identity across multiple chains.
- Singularity Net and Fetch Network are developing protocols allowing AI to be implemented, deployed and executed on top of Blockchain.
- Octan Network and Orange Protocol are developing different reputation systems to establish trust and credibility on Web3.

To conclude the paper, the author applies proposed categorization and taxonomy to briefly classify popular public blockchain platforms and L2-projects on the Top of Coinmarketcap. The classifying characteristics and examples are useful for readers to apply for their own cases. It is worthy to note that some platforms have been evolving with many planned upgrades in the future, hence they may overlap in several generations. Readers see classifying examples in Tables 3, 4, 5, 6, 7, and abbreviation explanation in Appendix. We have some remarks as followed.

- Generation classification only applies for true blockchain platform, not for specific applications. It considers system designs (monolithic chains, homogeneous sharding vs heterogeneous multi-chain systems).
- The 1st generations and some in the 2nd refer to platforms building cryptocurrencies and settlement layers but not Turing-complete.
- The 2nd generation is mostly characterized by Turing-complete smartcontract platforms but very limited in performance.
- The 3rd generation is dominated by Turing-complete smartcontract platforms with better performance and scalability compared to the 2nd one. The platforms are either standalone L1s or built on top of other L1 or L0.

- The 4th generation is remarked by high performance layer-1s and multi-chain systems, promising to offer greatest scalability, application-custom modularity, and scalable composability.

Platforms	**Gens**	**Ledger type**		**Governance**	**Cons**	**Layer**
Bitcoin, Dogecoin, Litecoin, Bitcoin Cash	1st	UTXO	linear	Permissionless	PoW	L1
XRP, Stellar	1st	account	linear	Permissioned	BFT	L1
Monero, Zcash, Dash	2nd	UTXO	linear	Permissionless	PoW	L1
IOTA (Approval Weight consensus)	2nd	UTXO	DAG	Permissionless	AW	L1
Ethereum (PoS from Sep 2022)	2nd	account	linear	Permissionless	PoS	L1
EthereumPoW, Ethereum Classic	2nd	account	linear	Permissionless	PoW	L1

Table 4
The 1st and 2nd Gens (Ethereum, Ethereum Classic, EthereumPoW are EVM-smartcontract platforms)

Platforms	**Ledger type**		**Governance**	**Cons**	**VM**	**Architecture**
BNB Chain	account	linear	Permissioned	PoSA	EVM	heterogeneous
Tron	account	linear	Permissionless	DPoS	EVM	heterogeneous
Cardano	UTXO	linear	Permissionless	PoS	Plutus	monolithic
Algorand	account	linear	Permissionless	PPoS	AVM-TEAL	monolithic
Hedera	account	DAG	Permissioned	BFT	EVM	monolithic
VeChain	account	linear	Permissioned	PoA	EVM	monolithic
Fantom	account	linear	Permissionless	BFT-PoS	EVM	monolithic
Theta	account	linear	Permissionless	PoS	EVM	monolithic
EOS	account	linear	Permissionless	DPoS	WASM	monolithic
Tezos	account	linear	Permissionless	PoS	TezosVM	monolithic
Flow	account	linear	Permissionless	PoS	FlowVM	monolithic
Klaytn	account	linear	Permissionless	PoS	EVM	heterogeneous
Casper	account	linear	Permissionless	PoS	CVM	monolithic
Oasis	account	linear	Permissionless	PoS	EVM, Ewasm	monolithic
Chiliz	account	linear	Permissioned	PoSA	EVM	monolithic

Table 5
The 3rd generation, layer-1 smartcontract platforms (some are evolving to heterogeneous multi-chain systems)

Platforms	**Gens**	**Governance**	**Cons**	**Layer**	**VM**	**Based on**
Polygon	3rd	Permissionless	PoS	L2	EVM	L1-Plasma
ImmutableX, Loopring, dYdX		Centralized	no	L2	no	L1-ZK-rollup
Optimism		Centralized	no	L2	no	L1-Optimistic Rollup
Cronos	3rd	Permissioned	PoA	L1	EVM	L0-CosmosSDK
Terra, THORChain, Osmosis	3rd	Permissionless	BFT	L1	no	L0-CosmosSDK
Moonbeam	3rd	Permissionless	PoS	L1	EVM	L0-Polkadot Substrate
BitTorrent	3rd	Permissionless	PoS	L2	EVM	L1-Tron

Table 6
L1s built on L0s and L2s built on top of L1s. Some L1s have no VM but they are application-oriented platforms with built-in contracts, hence are 3th generation. Some L2s are actually specific applications, hence cannot be classified into any blockchain generation.

Platforms	**Ledger type**		**Cons**	**Layer**	**VM**	**Architecture**
Solana	account	linear	PoS	L1	LLVM	monolithic
Aptos	account	linear	BFT	L1	MoveVM	monolithic
Polkadot	account	linear	NPoS	L0	EVM, WASM	heterogeneous
Avalanche	hybrid	hybrid	PoS	L0	EVM, WASM	heterogeneous
Cosmos	account	linear	BFT	L0	EVM, WASM	heterogeneous
ICP	account	linear	PoS	L0	WASM	heterogeneous
Near, MultiversX	account	linear	PoS	L1	WASM	homogeneous-shards
TON	account	linear	PoS	L1	TonVM	homogeneous-shards
Zilliqa	account	linear	PoS	L1	EVM	homogeneous-shards
Ethereum 2.0	account	linear	PoS	L1	EVM, Ewasm	homogeneous-shards

Table 7
The 4th Gen: high performance and homogeneous sharding L1s, heterogeneous multi-chain systems. They are all permissionless.

8 Acknowledgement

The author thanks my supervisor, Prof. Yang Wang, vice president of the Hong Kong University of Science and Technology, regarding his great encouragement and support during my PhD study at HKUST, especially, regrading my shift from data science & AI to Blockchain Technology.

9 Appendix

Term and abbreviation explanation for the Tables 3, 4, 5, 6, 7:

- BABE-GRANDPA: BABE (Blind Assignment for Blockchain Extension) is the block production mechanism that runs between the validator nodes and determines the authors of new blocks. BABE [13] is comparable as an algorithm to Ouroboros Praos [12], the consensus algorithm of Cardano. GRANDPA [14] (GHOST-based Recursive ANcestor Deriving Prefix Agreement) is the finality gadget that is implemented for the Polkadot Relay Chain to finalize blocks (visit Polkadot Consensus Wiki).
- NPoS: Nominated Proof of Stake used in Polkadot.
- PoSA: Proof of Staked Authority by BNB Chain.
- MOVE & MoveVM: MOVE is a new language for smartcontract programming in Libra-Diem, a consortium blockchain project, invested by Facebook (Meta). It formally announced on 18 June 2019, aimed to build a cross-border stable-coin system backed by a basket reserve of several fiat currencies. The project was terminated and all Diem assets sold according to Diem Association announcement on 31 January 2022. Some former developers of Libra-Diem are now developing Aptos and Sui L1s based on MOVE language and Move Virtual Machine (MoveVM).
- IBC: Inter-Blockchain Communication, an interchain protocol for cross-chain interoperation invented by Cosmos developers, aiming to build an Internet of blockchains.
- Tendermint Core is a BFT consensus mechanism used in Cosmos and CosmosSDK.
- WASM: WebAssembly (abbreviated as WASM) is a binary instruction format for a stack-based virtual machine.

References

[1] Antonopoulos A.M., Hariry S.H.E., Lords M.K., Morgan P., Scothorn M., Zolt-Gilburne S., The Internet of Money: Talks by Andreas M. Antonopoulos, Merkle Bloom LLC, 2016.

[2] Nikhil Vadgama, Jiahua Xu, Paolo Tasca, Enabling the Internet of Value: How Blockchain Connects Global Businesses, Springer Cham, 2022. https://doi.org/10.1007/978-3-030-78184-2.

[3] Treiblmaier H., Defining the Internet of Value. In: Vadgama N., Xu J., Tasca P. (eds), Enabling the Internet of Value: Future of Business and Finance. Springer Cham, 2022, pp 3–10. https://doi.org/10.1007/978-3-030-78184-2_1

[4] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, 2008 (accessed Feb 2023).

[5] Sherman Alan T., Javani Farid, Zhang Haibin, Golaszewski Enis, On the Origins and Variations of Blockchain Technologies, IEEE Security Privacy, 17 (1) (2019) 72–77. doi:10.1109/MSEC.2019.2893730

[6] Haber S., Stornetta W.S., How to time-stamp a digital document, J. Cryptology 3 (1991) 99–111. https://doi.org/10.1007/BF00196791.

[7] Bayer D., Haber S., Stornetta W.S., Improving the Efficiency and Reliability of Digital Time-Stamping, In: Capocelli R., De Santis A., Vaccaro U. (eds), Sequences II. Springer, New York, NY, 1993. https://doi.org/10.1007/978-1-4613-9323-8_24

[8] Merkle R. C., Secrecy, authentication, and public-key systems, PhD Thesis, Stanford University, 1979. https://cir.nii.ac.jp/crid/1571417125520618240?lang=en

[9] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and G. Das, Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems, IEEE Consumer Electronics Magazine 7 (4) (2018) 6-14. doi:10.1109/MCE.2018.2816299

[10] Anatoly Yakovenko, Solana Whitepaper, https://solana.com/solana-whitepaper.pdf, 2020 (accessed Feb 2023).

[11] Jesse Walden, 4 Eras of Blockchain Computing: Degrees of Composability, https://a16z.com/2018/12/16/4-eras-of-blockchain-computing-degrees-of-composability/, 2018 (accessed Feb 2023).

[12] Bernardo David, Peter Gazi, Aggelos Kiayias and Alexander Russell, Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain, In: Nielsen, J., Rijmen, V. (eds) Advances in Cryptology – EUROCRYPT 2018, EUROCRYPT 2018. Lecture Notes in Computer Science(), vol 10821. Springer Cham. https://doi.org/10.1007/978-3-319-78375-8_32017

[13] Handan Kilinc Alper, BABE protocol, https://research.web3.foundation/en/latest/polkadot/block-production/Babe.html (accessed Feb 2023).

[14] Alistair Stewart, Eleftherios Kokoris-Kogia, GRANDPA: a Byzantine Finality Gadget, https://github.com/w3f/consensus/blob/master/pdf/grandpa.pdf, 2020 (accessed Feb 2023).

[15] Rati Gelashvili, Alexander Spiegelman, Zhuolun Xiang, George Danezis, Zekun Li, Dahlia Malkhi, Yu Xia, and Runtian Zhou, Block-STM: Scaling Blockchain Execution by Turning Ordering Curse to a Performance Blessing, 2022. https://arxiv.org/pdf/2203.06871.pdf.

[16] Arthur D. Little, Market Opportunity Report, https://parallelchain.io/reports-and-whitepapers/ADL_Report_2020_3e8a4d0c2d.pdf, 2020 (accessed Feb 2023).

[17] Mauro Conti, Ankit Gangwal, and Michele Todero, Blockchain Trilemma Solver Algorand has Dilemma over Undecidable Messages, In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES'19). Association for Computing Machinery, New York, NY, USA, Article 16 (2019) 1–8. https://doi.org/10.1145/3339252.3339255

[18] S. Leonardos, D. Reijsbergen and G. Piliouras, PREStO: A Systematic Framework for Blockchain Consensus Protocols, in IEEE Transactions on Engineering Management 67 (4) (2020) 1028-1044. doi:10.1109/TEM.2020.2981286.

[19] Joseph Bonneau, Why blockchain performance is hard to measure, https://a16zcrypto.com/why-blockchain-performance-is-hard-to-measure/, 2022 (accessed Feb 2023).

[20] Tasca P., Tessone C. J., A Taxonomy of Blockchain Technologies: Principles of Identification and Classification, Ledger 4 (2019). https://doi.org/10.5195/ledger.2019.140

[21] Olga Labazova, Tobias Dehling, Ali Sunyaev, From Hype to Reality: A Taxonomy of Blockchain Applications, Proceedings of the 52nd Hawaii International Conference on System Sciences, IEEE, Wailea, Maui, HI, USA (2019).

[22] Sam Goundar, Shalvin Chand, Jalpa Chandra, Akash Bhardwaj and Fatemeh Saber, A Taxonomy of Blockchain Applications, in: Blockchain Technologies, Applications and Cryptocurrencies, World Scientific 2020, pp. 49-71. https://doi.org/10.1142/9789811205279_0003

[23] X. Xu et al, A Taxonomy of Blockchain-Based Systems for Architecture Design, 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 2017, pp. 243-252. doi:10.1109/ICSA.2017.33.

[24] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis, SoK: Consensus in the Age of Blockchains, Proceedings of the 1st ACM Conference on Advances in Financial Technologies (AFT'19), Association for Computing Machinery, New York, NY, USA, 2019, pp. 183–198. https://doi.org/10.1145/3318041.3355458

[25] Sarah Bouraga, A taxonomy of blockchain consensus protocols: A survey and classification framework, Expert Systems with Applications 168 (2021) 114384, ISSN 0957-4174. https://doi.org/10.1016/j.eswa.2020.114384.

[26] Jeff Nijsse, A Taxonomy of Blockchain Consensus Methods, Cryptography 4 (4) (2020) 32. https://doi.org/10.3390/cryptography4040032

[27] Garay J., Kiayias A., SoK: A Consensus Taxonomy in the Blockchain Era, In: Jarecki S. (eds) Topics in Cryptology – CT-RSA 2020, Lecture Notes in Computer Science 12006. Springer Cham, 2020. https://doi.org/10.1007/978-3-030-40186-3_13

[28] Omer F. Cangir, Onur Cankur, Adnan Ozsoy, A taxonomy for Blockchain based distributed storage technologies, Information Processing & Management, 58 (5) (2021). https://doi.org/10.1016/j.ipm.2021.102627.

[29] Shehu M. Sarkintudu, Huda H. Ibrahim and Alawiyah Bt Abdwahab, Taxonomy development of Blockchain platforms: Information systems perspectives, AIP Conference Proceedings 2016, 020130 (2018); https://doi.org/10.1063/1.5055532

[30] Gang Wang, Zhijie Jerry Shi, Mark Nixon, and Song Han, SoK: Sharding on Blockchain, Proceedings of the 1st ACM Conference on Advances in Financial Technologies (AFT '19), Association for Computing Machinery, New York, NY, USA, 2019, pp. 41–61. https://doi.org/10.1145/3318041.3355457