Deloitte.

POLITECNICO MILANO 1863

The Blockchain Galaxy

A comprehensive research on distributed ledger technologies

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Executive summary

Blockchain technology has recently passed the 10 years mark since the first Bitcoin block creation on January 3, 2009, by one or more people under the pseudonym Satoshi Nakamoto.

The first years of life of the Bitcoin network have passed relatively quietly, away from the media spotlight and the attention of malicious hackers. However, the growing value of Bitcoins could not remain in the shadows for long.

In 2013, the first alternative to Bitcoin's Blockchain with Ethereum was born, thanks to the white paper written by a very young Vitalik Buterin (not even twenty at the time).

The two Blockchain, still the most popular, face different problems and offer solutions that overlap only marginally.

Over the following years, industries began to explore these Blockchain to try to optimize their internal processes or take courageous initiatives. Thanks to the exponential appreciation of cryptocurrencies, which have brought huge capital to the industry, media attention and numerous developer communities, since 2016 we have seen a proliferation of new Blockchain, new programming languages, new ideas and new use cases that have accelerated infrastructure creation and adoption, including at the institutional level.

In 2020 we can count several projects that aspire to create national currencies such as the Chinese DCEP (Digitial Currency / Electronic Payment), the Swedish eKrona, the Turkish government or the Digital Dollar Project in America.

In a survey conducted by Deloitte in 2019 , interviewing a sample of 1,386 executives in 12 countries (Brazil, Canada, China, Germany, Hong Kong, Israel, Luxembourg, Singapore, Switzerland, United Arab Emirates, United Kingdom and the United States) at companies with at least $500 million in turnover, we found that most industries have planned multi-million dollar investments in Blockchain despite the fact that they still have privacy, taxation and anti-money laundering issues.

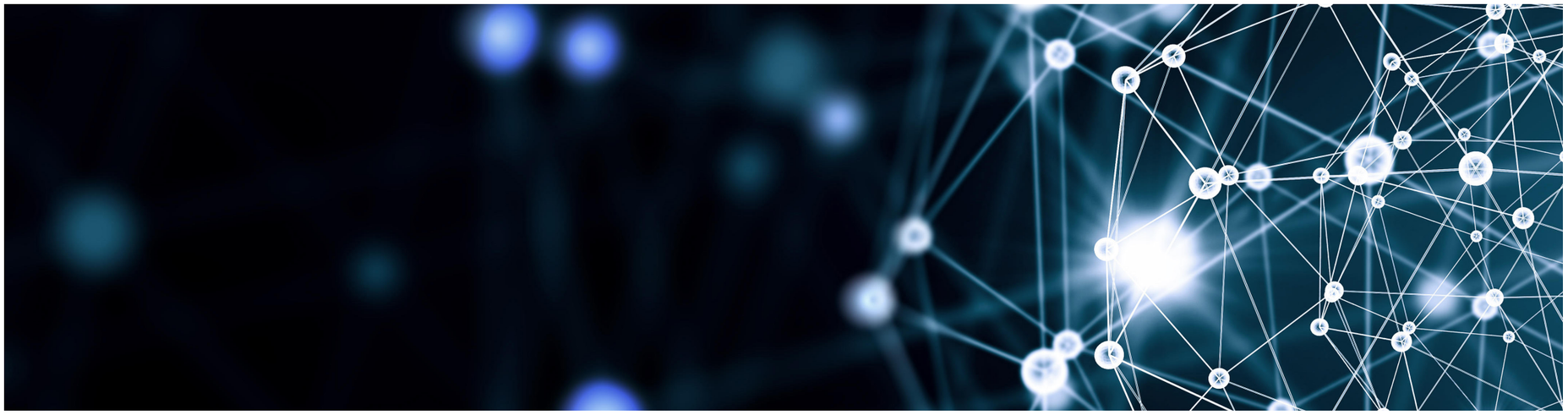
Probably the first profound reflection that anyone approaching Blockchain should face eventually is the dichotomy between public and consortium Blockchain. The debate and perplexities are similar to what we saw at the dawn of the Internet with private and public networks and it is somehow following this historic example. In fact, several consortia have decided to use a consortium Blockchain to avoid problems of scalability, privacy and use of cryptocurrency, typical of public Blockchain.

Finally, we highlight the growing technical difficulty in identifying and selecting the correct Blockchain for a given use case. Difficulties due to their constantly growing number, the specific technologies used and last but not least the uncertain future of the communities of developers that feed these protocols.

The Blockchain Galaxy

1.

Blockchains: an historical introduction



A blockchain is a distributed ledger based on a growing list of blocks, each one being connected to the previous one exploiting cryptography. The first blockchain was conceptualized by Satoshi Nakamoto (a pseudonym) in 2008. It was created as a transaction ledger for the cryptocurrency Bitcoin. The novelty was in the Hashcash-like method to add blocks to the chain without requiring a trusted third-party: the mining procedure. The main characteristic of the Bitcoin blockchain are:

- Decentralization.
- Immutability.
- No double spending allowed.
- No trust between the nodes (e.g., the device on the blockchain network) needed.

In fact, Satoshi Nakamoto's white paper describes a distributed ledger, the blockchain, were it is not possible to delete/modify transactions once they are recorded in the blockchain (immutability) and which prevent double spending. Moreover, Bitcoin blockchain is based on wallet cryptography security, and on a mining procedure to chain the blocks together: more precisely, mining is the procedure which ensures the immutability of the blockchain, even in absence of trust between the miners. The miners, i.e., the network device which are delegate to mining, are remunerated for the high computational work to be done for mining through the transaction fees and the new Bitcoin created according to an algorithm due to Satoshi Nakamoto which mimics the scarcity of gold (this is the reason why the words mining/miner are used). To better understand mining, we need to deal with the Byzantine Consensus Protocol, which are the core of Bitcoin blockchain system, as well as of most blockchains. It is the mechanism that guarantees that honest nodes agree on the updates to be performed on their independent local copy of the blockchain, in absence of trust. Literature at the beginning of the 80s established that it was not possible to reach consensus by means of a deterministic protocol in an asynchronous network if even one single process crashes silently. Literature also dealt with the byzantine failure: a byzantine node, besides crashing and therefore stopping its participation to the protocol, can behave arbitrarily, therefore violating in every possible way the correct behavior described by the protocol. The distributed and permissionless nature of Bitcoin, meaning that nodes do not need to know each other to participate in the network, showed that Byzantine Fault-Tolerance (BFT) protocols had many very interesting applications still to be explored, as for example cryptocurrency. The main problem is how to ensure the correct operation of a distributed transaction ledger, even in presence of a Byzantine fault.

To better explain the Byzantine Consensus Protocol, literature related the problem of coordination among computers, allowing some of them to be adversarial, to an experiment in which there are a number of divisions of the Byzantine army camped outside an enemy city. The generals of the divisions have to exchange messages in order to decide a common plan of action. Some of these generals may of course be traitors trying to prevent honest generals to reach an agreement.

Proof of Work (PoW) is the original blockchain consensus algorithm theorized by Satoshi Nakamoto to solve the Byzantine fault problem. A proof of work is essentially the solution of a complex mathematical problem. It takes a lot of work to create (hence the name) but it is easy to be validated by other nodes. In Bitcoin, as well as in other blockchain, this mathematical problem is related to the computation of an hash. In fact, miners search for the correct hash associated to both the last block in the blockchain as well as the new block to be chained, until one of them finds the correct answer. This solution is then verified by other miners. Once confirmed, the new block is added to the blockchain by the other miners, which then use this new block as the input for the hash problem related to the next block. Therefore, PoW solves the Byzantine generals problem as it achieves a majority agreement without any third-party central authority. The Bitcoin PoW also prevents malicious miners from sabotaging the network: the hash signature (i.e., the result of the complex mathematical problem to be solved) of each block is stored in the subsequent block. Any change to an earlier block would therefore require all successive blocks to also be changed. This would take an excessively large amount of computing power, and therefore the ledger is immutable. Moreover, the miners are remunerated for their work, therefore for a miner it is convenient to play in favor of the good functioning of the Bitcoin system.

Starting from Natoshi Sakamoto idea, other blockchain were created, among them we recall Ethereum, proposed in 2013 and online from 2015. Ethereum blockchain is important because it supports smart contract. The galaxy of blockchains is very vast, and each blockchain shows its main purposes (e.g., cryptocurrency transactions -Bitcoin-, or smart contract -Ethereum) as well as its own characteristics. As an example, not all blockchains are designed to solve the problem of consensus with the PoW: other protocols have been implemented, such as the Proof of Stake (a person can mine or validate block transactions according to how many coins he/she holds).

The purpose of this document is therefore to analyze the main features of some of the existing blockchains.

The Blockchain Galaxy

2. Technological analysis of the main blockchains

In the following, we analyse in detail the main blockchains, to better address the differences, the pros and cons, and the potentialities.

For a summary table we refer to the Appendix.

Bitcoin

The first concrete evidence of the Bitcoin project was the registration of the domain "bitcoin.org", happened on August 18th, 2008. The famous paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" was than released few weeks later, on October 31st, 2008, by an unknown author (or group of authors) under the pseudonym Satoshi Nakamoto. At the beginning of the next year the Bitcoin code was released as open-source software, giving birth to the first and most famous blockchain system.

Bitcoin is essentially based on the UTXO (Unspent Transaction Output) model, in which the value on the network is associated to transactions that only people able to solve a (sort of) "programming puzzle" can spend. Generally, these puzzles are base on the knowledge of a particular private key associated to the public key which has is included in the transaction data. The Bitcoin Script, the programming language of the above mentioned puzzles, is powerful enough to express a quite wide and interesting set of functionalities, such as transfer money, demonstrably burn it and implement multi-signature solutions or multi-user lotteries. However, Bitcoin Script has been intentionally designed for being non-Turing-complete, thus there are more complex behaviours that fall outside its expressiveness possibilities. Other limits of Bitcoin Script are its lack of state (an UTXO has to be spent in one step, so it is not possible to implement intermediate states), its value-blindness (the impossibility of modulating the amount of coins of a particular UTXO that a user can spend: the UTXO has to be spent completely, as a whole) and its blockchain-blindness (the impossibility of accessing data contained in the chain).

These limitations are the reason of the origin of Ethereum, an account-based blockchain specifically designed for being a worldwide computing platform able to run Smart Contract, pieces of code typically written in Solidity, a Turing-complete programming language. On the other hand, the intentional limitations of Bitcoin Script make it somehow shielded by the classic problems of programs misbehaviours, drastically reducing the risk of issues such as The Dao Hack (one of the most famous hack of Ethereum, which gave birth to the hard fork that splitted the blockchain in two: Ethereum and Ethereum Classic).

Being the "original" and most renowned blockchain, the main strong point of Bitcoin is of course its capitalization (around $93 billion at the time of writing), which makes it the obvious choice for notarization tasks. Most of the critics against Bitcoin are related to its use for illegal transactions (weapons, drugs, etc.) its huge electricity consumption (due to its consensus mechanism, based on the Proof-of-Work protocol) and the volatility of its value (which makes it difficult to exploit Bitcoin as a real-world currency for buying/selling goods or services).

Ethereum

Ethereum is a blockchain based computing platform devised by Vitalik Buterin, already active in bitcoin research, development and dissemination, in 2014. The main reason of its inception was to overcome some limitations with which Bitcoin programmability was intentionally constrained, in order keep its computing requirements and effects predictable. Ethereum is instead endowed with a language that is Turing complete, i.e. has the same expressive power of the widespread general purpose programming languages.

The metaphor with which Ethereum is presented is that of a "world computer": a global computing machine, decentralized in the same way as Bitcoin is, in which it is possible to upload software agents that are unstoppable, completely transparent, whose execution is fully auditable, and that can handle token transfers. This technical and conceptual tool is immediately seen as the substrate that can implement the idea/concept of "smart contracts", proposed by Nick Szabo in 1994: "A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises". Indeed, Ethereum calls the software agents running within it "smart contracts". Smart contracts expressive power is shown in one the first examples in the documentation, where an independent token system is defined in few lines code, showing how Ethereum language generalizes existing blockchain applications. Other implications are soon devised: voting systems, automated insurances, identity management, decentralized crowdfunding autonomous organizations, various kinds of tokens with different economic properties, both fungible and non fungible. Ethereum borns inheriting the fundamental features of Bitcoin: consensus is based on validator election through Proof-of-Work, albeit with an algorithm that prevents ad-hoc acceleration using application specific integrated circuits, with the intent of limiting concentration of mining power. Some parameters are tuned differently, like time between blocks, that is around 15 seconds. A stark difference from Bitcoin is the presence of a planned, ambitious technological roadmap, in which to noteworthy changes are planned: migration to a mixed proof-of-work/proof-of-stake consensus mechanism, and sharding, a feature that would allow individual nodes to only validate a share of the transactions, and to memorize a part of the state of the system. This would make the commitment to maintain a node much less onerous. Ethereum shares with Bitcoin limitations in throughput and high latencies, to address which different solutions such as State Channels, Raiden and Plasma sidechains are proposed. Ethereum is the first and main platform, both in term of capitalization and of active developers, aimed at the development of general smart contracts and applications. Its story includes difficult moments, such as the DAO hack, in which the main application on the platform, a decentralized crowdfunding organization, got hacked due to an unforeseen behavior of a part of its smart contract. The event led induced hard confrontations in the community on how to deal with the theft, which eventually led to a fork of the platform. The pressures it underwent and its "war wounds" make Ethereum the most mature and battle tested platform in its arena.

Neo

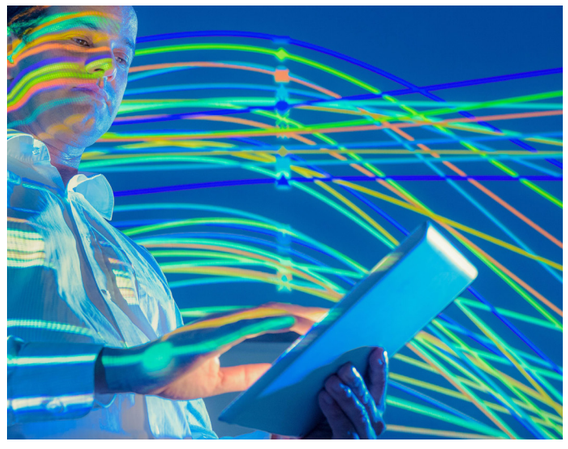
Neo was founded by Erik Zhang and Da HongFei, in 2014. Its declared main aim is to support the development of a "smart economy", relying on three pillars: Digital Assets, Digital Identity, and Smart Contracts. As consensus mechanism, it uses a Delegated Byzantine Fault Tolerance.

It uses a double token monetary architecture (such as Vechain, for instance), where the token representing value, NEO, steadily generates GAS, that is used to pay for operations.

One of its most distinctive features is the native presence of a X.509 compliant identity layer, that can serve different purposes. On one hand, identity can be bound to the dBFT consensus mechanism, in that validator nodes can be linked to real world identities. Native identity can also be used in tracking property of digital assets, facilitating compliance with regulatory frameworks.

To develop smart contracts, different compilers for popular languages are available (C#, VB.Net, F#, Java, Kotlin, Python), aiming to lower barriers for developers.

Neo competes in the same applicative domains of ethereum (dapps, digital assets, more broadly Turing-complete smart contracts), but takes a much more opinionated stance, with the aim of offering ready to use solutions to some problems (stability of operation costs, predictable governance through the control of the BFT validators). The inclusion of a built in identity layer is meant to address regulatory requirements right away. The same problems are being addressed in the ethereum space (e.g. mechanisms to implement self sovereign identity models), at a slower pace, but with a more open and general approach.



Iota

IOTA is a cryptocurrency founded in 2015 by David Sønstebø, Sergey Ivancheglo, Dominik Schiener, e Dr. Serguei Popov. They currently are, with the addition of Ralf Rottmann, the members of the Board of Directors of the IOTA Foundation, which is a non-profit organisation created in 2017 in Germany by Dominik Schiener and David Sønstebø. The main goals of the IOTA Foundation spans from the research on the protocol layer to the development of production-ready software for the community, including education, promotion and standardization activities related to the Internet of Things ecosystem.

The main raison d'être of IOTA lays in the definition of a highly scalable and zero-fee infrastructure for the exchange of digital value, which was envisioned as one of the most important enabling factors for the diffusion of IoT. In order to accomplish this task, IOTA defines a completely new infrastructure, quite different from the classic blockchain approach. IOTA is in fact based on a Tangle (basically a Directed Acyclic Graph, or DAG) in which different transactions are connected to each other. Thus, the distributed ledger of IOTA does not rely on a chain of transactions blocks, but on a stream of single transactions entangled together.

In this context, in order to include a transaction in the Tangle, a user (typically the sender) has to perform a small amount of computation to verify other previous transactions. Following this principle, every actor of the network has to validate two transactions in order to insert a new one, which will be validated by some other subsequent transaction. Since the IOTA network has been designed for tiny devices, such as sensors, the computational requirements to perform the validation are quite low. Thanks to this 'pay-it-forward' validation system, financial rewards become unnecessary and the scalability problem can be considered solved, since increased network activity decreases transaction settlement times.

Even though IOTA does not natively support smart contracts, there is an interesting work in progress project, named Qubic, that aims at implementing a powerful, distributed fog computing platform for building complex IoT applications, a new type of smart contract, which collects micro-payments in real time as it runs and a reward system for incentivizing honest participation in the Tangle.

IOTA has been the first zero-fee cryptocurrency, thus it competes with more recent platforms such as Nano in the area of non-programmable micropayments, even if the Qubic experiment aims at projecting it well beyond this field of application.

Eos

Eos was created in 2017 by Dan Larrimer, and initially funded by means of the most succesfull ICO to date. It aims to provide a platform for the development of decentralized applications and smart contracts.

It uses delegated proof of stake as a consensus mechanism. Block verification is delegated to twenty one validators, that are elected by the holder.

Its currency is the EOS, of which 1 billion was initially initially sold through the ICO. The monetary policy is intertwined with the governance model: Block Producers, that are continuously delegated by the EOS holders to make up and validate new blocks, get 1% of the tokens minted at a 5% annual inflation rate. The other 4% goes to a contract governed by token holders for investments in the network (https://www.whiteblock.io/library/eos-test-report.pdf).

A distinctive feature is the approach to scalability. In addition to the fast consensus algorithm, in EOS it is possible to span parallel, communication blockchains that widen the transaction bandwidth. In principle, smart contracts can be written in any language that compiles to WebAssembly. In practice, at the moment only a C++ toolchain is provided and supported. Current applications are mainly gambling, games and exchanges (https://dappradar.com/rankings/protocol/eos/).

Eos competes in the arena of dapps and generic smart contracts (together with e.g. Neo and Vechain). With respect to ethereum, it offers improved performances, in terms of transaction throughput, at the cost of a much less decentralized approach to consensus.

NEM

The New Economy Movement (NEM) project has been launched in 2015. Its main building blocks are:

- The NEM blockchain, on which services such as Smart Assets run.
- The XEM cryptocurrency, used to pay for DApps development and network fees.
- The NEM Foundation, established in 2017 by the NEM co-founder Lon Wonand and in charge of developing The main distinctive aspect of NEM is its unique consensus mechanism, based on a variation of Proof-of-Stake and known as Proof-of-Importance (POI), in which the weight of each node is computed by taking into account both the corresponding wallet balance and its network activity (mainly in terms of transactions). In particular, POI considers three main factors to determine (by means of the NCDawareRank ranking system) the chances of "harvesting" a block:

  1. Vested stake: only coins that are held for a certain period of time are taken into account; a fraction (10%) of the "unvested" wallet balance is considered "vested" each day; a minimum of 10.000 coins have to be "vested" to enable "harversting".
  2. Transaction partners: wallet performing transactions with others nodes in the network are rewarded with a score.
  3. The number and the value of the transactions in the last 30 days are both kept into account (only net transactions over time are considered, so that users cannot simply trade back and forth the same amount of coins among few accounts).

Block harvesting can also be delegated to other nodes by lending POI score to the remote node, thus making it possible for it to harvest a block on your behalf.

Among the other interesting features of NEM it is possible to find multi-signature accounts, encrypted messaging, a notarization and timestamping system called Apostille and the Eigentrust++ reputation system, which makes it possible to guarantee network integrity by monitoring the (past) behavior of network nodes.

The next release of the NEM engine is called Catapult. This "coming-soon" technology should be able to power both private and public networks. However, it seems Catapult is not ready yet, and in the meanwhile the NEM Foundation is going through a quite rough period. Lon Wong resigned in April 2018, and Kristof Van de Reck served as the interim president of the NEM Foundation until Alexandra Tinsman was elected as president in December 2018. A financial audit has been performed at the beginning of 2019, since the NEM Foundation revealed that they are running low on both XEM and FIAT funds. In this context, the newly elected president of the NEM Foundation is currently submitting a funding request to rescue the organization. Although Tinsman repeatedly stated that the NEM Foundation operates as a separate entity with respect to the NEM blockchain platform, the impact of this situation on the NEM ecosystem as a whole (e.g., the XEM price) is anything but negligible. For these reasons, before considering the NEM platform as a suitable option for the deployment of high performance decentralized applications, it will be necessary to carefully follow the evolution of the NEM Foundation situation.

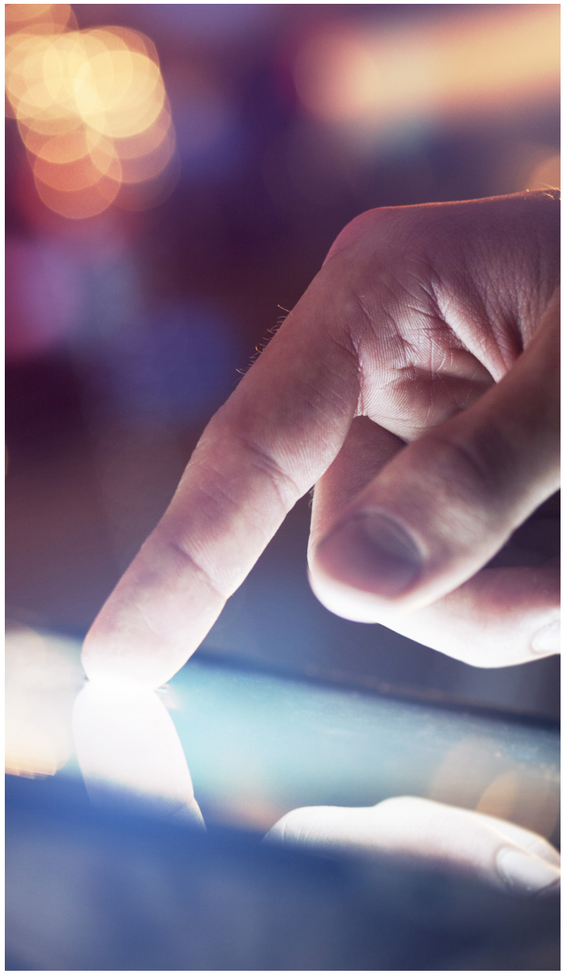
Waves

WAVES was created by a russian engineer, Sasha Ivanov, and officially launched in November 2016, thanks to a crowdfunding campaign able to raise around $16 million. WAVES provides users with a decentralized system characterized by a wide range of helpful and easy-to-use tools, accessible as Platforms as a Service and aiming at:

- Enabling the possibility of creating new crypto-coins, called Custom Application Tokens (CATs), without the need of programming skills (and in less than a minute, WAVES claims). CATs can be created directly through the lite client, available both on the web and on mobile devices (Android and iOS). The Typical use cases are projects crowdfunding, simple ICOs, in-app currencies or loyalty rewards programs.
- Letting users define their Decentralized Apps (DApps) over their custom tokens by means of (non-Turing-complete) Smart Contracts written in RIDE, a new programming language specifically designed for WAVES. Typical example of WAVES Smart Contracts are multi-signature addresses (in which two or more parties are required to sign the same transaction to make it valid), asset freezing (making it possible to lock a token and preventing its transfer until a certain block height is reached), atomic swaps, voting and oracles, even though the latter is a coming soon feature that will make it possible to connect the blockchain to an external data source, triggering WAVES Smart Contracts on the base on information coming from a third party. Differently from Ethereum, WAVES Smart Contracts do not require Gas (a payment proportional to the number and the complexity of computational operations performed) to be executed, since a minimal flat fee is charged for each execution;implementing a simple and decentralized mechanism for exchanging and trading custom tokens, such as the Decentralized Exchange (DEX). Whenever a user issue a new CAT, a fixed cost of 1 WAVES has to be paid and the CAT is automatically listed by default on DEX. Even though transactions can be performed using CAT, transaction fees are always paid in WAVES cryptocoins.

The consensus in WAVES is reached by means of the Leased Proof-of-Stake (LPoS) mechanism, a modified version of Proof-of-Stake in which tokens can be staked by "leasing" them to the full nodes contributing to the maintenance of the network integrity. These nodes receive a monthly reward both in WAVES and in Miner Reward Tokens (MRTs), which is one of the CATs tradeable in the DEX.

With respect to the other platforms providing similar services (such as token economy, decentralized applications and smart contracts), WAVES mainly focuses on mass adoption exploiting simplicity and ease of use as its main weapons. Even though this choice somehow limits the set of functionalities achievable within the platform, the potential of this approach could be huge, especially in a scenario in which technological entry barriers are certainly non-negligible.



Komodo

Komodo has been founded by James Lee (JL777) as a fork of Zcash, which is a fork of Bitcoin in which privacy has been introduced by means of zero knowledge proofs (allowing untraceable transactions). Komodo has a total fixed supply of 200 million coins, out of which 100 million were pre-mined and distributed in the ICO (October 15, 2016 – November 20, 2016). Out of this 100 million, 90 million were distributed to investors, and 10 million were kept aside for future development and marketing of the Komodo platform. The remaining 100 million coins are still being mined via PoW.

The main innovation of the Komodo platform is its Federated Multi-Chain Blockchain Architecture, in which:

- Security is provided by the delayed-Proof-of-Work (dPoW) mechanism, which is a dynamic checkpoint notarizations on the Bitcoin blockchain. Every ten minutes, a block hash from a block in the KMD chain is written into a block on the Bitcoin blockchain. This task is performed by Komodo Platform's 64 notary nodes, which are servers elected annually and dedicated to this fundamental operation. Currently, the Komodo's Blockchain Security Service is exploited by several other projects, such as GAME Credits, Kreds, Einsteinium, HUSH, SUQA, and GIN Coin.
- Scalability is achieved by providing every project with a customized and dedicated blockchain, so that predictable performance can be easily guaranteed. If necessary, additional blockchains can be added to an existing one in order to form a cluster and boost performance. All the blockchains in the Komodo's ecosystem are synchronized with a Multi-Chain Syncing mechanism (involving Merkle Trees to notarize transactions that take place on one chain onto every other chain) and can "communicate" by means of Cross-Chain Smart Contracts.
- Interoperability is guaranteed by Komodo's Multi-Chain Syncing technology, so that all projects are granted seamless cross-chain interoperability with other interlinked chains. Every blockchain is also connected to chains outside the ecosystem via atomic swaps (currently supporting around 95% of all cryptocurrencies), which makes it possible to exchange two different coins directly from one user to another, wallet to wallet. In addition to this, Cross-Chain Smart Contracts allows inter-blockchain transfers of value without performing a swap or trade, thanks to a combination of notarized Merkle Tree proofs and a burn protocol: coins on one chain are burned while the value is allowed to appear on a separate chain within the ecosystem.

Among the different innovations of the Komodo platform, Crypto-Conditions powered Smart Contracts (based on the UTXO concept) seem to be on the podium, since they make the Bitcoin protocol Turing-complete. This has been achieved by introducing an additional payment script that designates a UTXO as belonging to a specific Custom Consensus (CC) module. Currently, just four basic CC modules have been activated on Komodo Platform: Assets, Faucet, Rewards, and Dice. If a project within the Komodo ecosystem would like to use a module that isn't already in the code base, they can submit a Pull Request to the Komodo repository on Github. If accepted, Komodo will write the module and make it available for all blockchains within the Komodo ecosystem at the next notary hardfork.

The Komodo Federated Multi-Chain Blockchain Architecture is a charming solution, also because it makes it possible to create a new chain in few minutes, allowing a very easy customization of its consensus mechanism (PoW, PoS or a mix of the tow), coin/token parameters (supply, optional premine of any percentage of supply), block time (1 minute or on demand), privacy (exclusively zero-knowledge trades or transparent chain with optional privacy), mining rewards (rewards amount and structure) and governance (tax from transaction fees or from mining rewards).

Komodo can be seen as an opponent of Ethereum, Neo and Dragonchain, since it brings the Bitcoin network in the arena of tokenization and smart contracts. With respects to its competitors, Komodo focuses more on scalability and on the interoperability, both within the federation of blockchains it enables and with the outside world, thanks to atomic swaps. Crypto-Conditions powered Smart Contracts are really interesting, even though only very few Custom Consensus module are currently supported and the mechanism to add a new one seems to be a bit farraginous (and centralized).

Dragonchain

The Dragonchain project has been originally developed at The Walt Disney Company in Seattle in 2014. In 2016 the project has been open-sourced and in 2017 the non-profit organization named Dragonchain Foundation was created with the main goal of maintaining its source code. The commercial blockchain platform built on top of this code is managed by the commercial entity named Dragonchain Inc., founded by Joe Roets (founder and CEO).

Dragonchain is a public/private hybrid blockchain platform specifically designed for enterprises with the main aim of keeping sensitive business logic private, while guaranteeing immutability thanks to notarization on public blockchains. The consensus on this hybrid architecture, named Dragon Net, is achieved by means of independent verification nodes, which belongs either to the Dragonchain community or to external partners. These nodes are hierarchically organized in the so called '5 Level Spectrum of Trust':

- Private business Node, where sensitive data is stored and business logic is executed.
- L2 Nodes, which are responsible for blocks, headers, and signatures validation. The rules used for the validation activity, performed without the need of knowing without the actual data or the business logic, can be customly defined by enterprises.
- L3 Nodes, used to guarantee the level of consensus by checking that the transactions are validated by a sufficient number of L2 Nodes.
- L4 Nodes, hosted by external partners, which provide notarization functionalities by signing the verification records received by L3 Nodes.
- L5 Nodes, which perform proof of existence by checkpointing successfully verified transactions on public blockchains. This task is achieved by means of the Interchain mechanism, which basically records the hash of the private transactions on public blockchains, such as ETH, ETC, NEO, or BTC.

Almost instant transaction processing, fixed 5-second blocks, quite good scalability and a wide range of smart contract programming languages (including Node.js, Python, Go, Java, C#) are among the main distinctive features of Dragonchain. In addition to this, Dragonchain is GDPR compliant by design, since enterprises can freely select in which global region public and private information is stored, and supports the self-sovereign identity paradigm thanks to Dragon Factor, which provides secure and decentralized authentication and access to applications.

The Dragonchain platform contemplates an utility token that represents tokenized micro-licenses (TML). These tokens are known as Dragonchain tokens (DRGN), even though they are often referred to as Dragons. Each Dragon tokens holder is awarded with a Dragon Days of Slumber Score (DDSS), representing the result of the multiplication between the number of Dragons held and the number of days this amount of Dragons has been held in the account. DDSS can be used to access specific features of the Dragonchain ecosystem, such as the permission to run L2, L3 or L4 nodes.

Dragonchain present several similarities with respect to Komodo, such as the possibility of running multiple chains in parallel and the recording of proofs of existence on public blockchains. With respect to the other ecosystems such as Neo, Komodo and Ethereum, Dragonchain focuses more on GDPR-compliant features, such as the separation of sensitive data and business logic from the achievement of the consensus, the possibility of storing data on specific global regions and the native support to authentications based on the self-sovereign identity paradigm.

Stratis

Stratis was created by Chris Trew in 2016, as the principal asset of Stratis Group Ltd.

It is proposed as a Blockchain as a Service (Baas), in that it essentially allows to quickly create and deploy private, application specific sidechains that are anchored to a main chain. Its execution environment is the C# virtual machine, and it is explicitly bound to Microsoft technologies.

The consensus mechanism is mixed, in that it is a Proof of Stake for the main blockchain, and Proof-of-Authority for the sidechains. One of the main value propositions is the ease for C# developers and enterprises to build distributed applications.

It features built-in identity representation and management capabilities, with which users can create proof of their identity by logging into a social networking site (LinkedIn, Google, or Microsoft). Identity information can then be secured and shared selectively.

Stratis main target is the development of enterprise blockchain applications, which is the more evident from the company consultant activities.

Corda

Corda is a Distributed Ledger Technology (DLT) specifically developed by R3 to solve some real-world business problems of financial institutions, such as maintaining a shared ledger of transactions without keeping private ledgers to be constantly updated (and cross-checked) after each interaction among different entities and without disclosing publicly private transactions data. R3 has been founded in 2014 by David E. Rutter (the current CTO is Richard G. Brown) and it is a consortium of hundreds of firms involved in the research and development of distributed ledger solutions for financial systems. The source code of the Corda project has been open-sourced in November 2016.

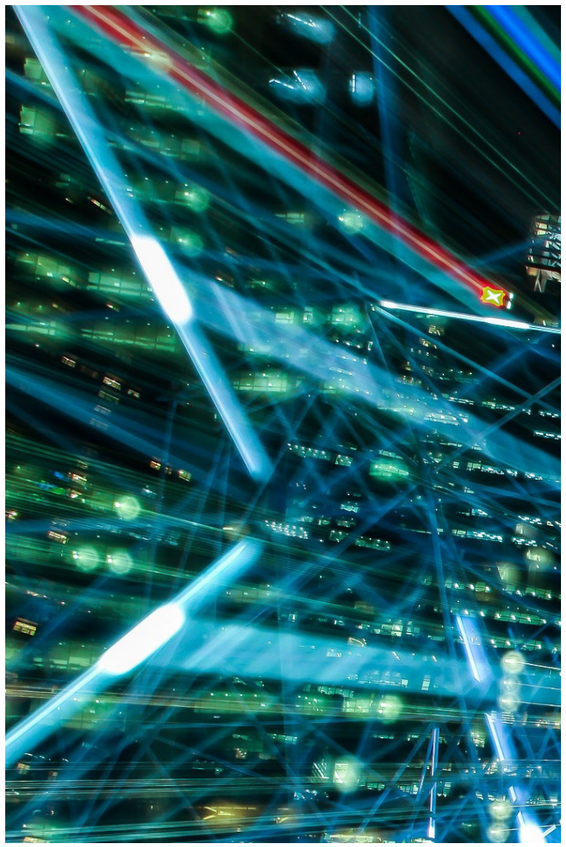
The Corda Network consists of nodes (running Corda and CorDapps) communicating among them in a point-to-point and encrypted fashion. The network is permissioned, since access is granted by the network operator: doing so, each node can be associated to a single well-known real-world legal identity.

The Corda Ledger can be seen as fragmented in several pieces, or facts, that can represents stocks, bonds, loans, KYC data, identity information, etc. Each network node keeps tracks only of a portion of the fragments, the ones that the node considers relevant, storing them in its vault. As a result, each peer only sees a subset of facts on the ledger, and no peer is aware of the ledger in its entirety. However, the Corda architecture guarantees that two nodes sharing an on-ledger fact are always aligned on the same version of the fact. To be precise, Corda exploits an UTXO-based model to store ledger facts, each one of which is represented by an immutable state. States are evolved by marking them as "historic" and creating a new version of it (an updated state), thus implementing a sequence of states in which the last one represents the most recent (and valid) information.

In this context, transactions are proposals to update the ledger, which are commit if and only if it is contractually valid, it is signed by all the required parties and it does not incur in double-spending issues. Differently from other well known blockchains, Corda transactions can refer (by hash) to attachments, which are ZIP/JAR files containing arbitrary content that can be used to validate the transaction itself. In addition to attachments, transactions can also refer to specific time-windows, which are the time periods in which transactions can be committed. In order to avoid double spending and validate time-windows, the Corda architecture envisages the use of notary pools (or notary clusters), network services running specific consensus algorithms, providing uniqueness consensus and serving as trustworthy time-stamping authorities.

Corda Contracts, used to validate transactions, are written in a JVM programming language (such as Java or Kotlin) and can exploit the full capabilities of the language. As in the other blockchains, contract execution is deterministic (a contract should either always accept or always reject a given transaction) and can only be based on the transaction content.

The main competitor of Corda is another permissioned approach: Hyperledger Fabric. With respect to this solution, Corda has been designed to scale better with the number of participants joining the system. In addition to this, Corda faces privacy and security of transaction data in a completely different way: in Corda data is not broadcasted to the whole network (such as happens in public blockchains), but it is shared only between the counterparties signing the deal and eventually the regulators in charge of validating it, thus preserving secrecy by design.

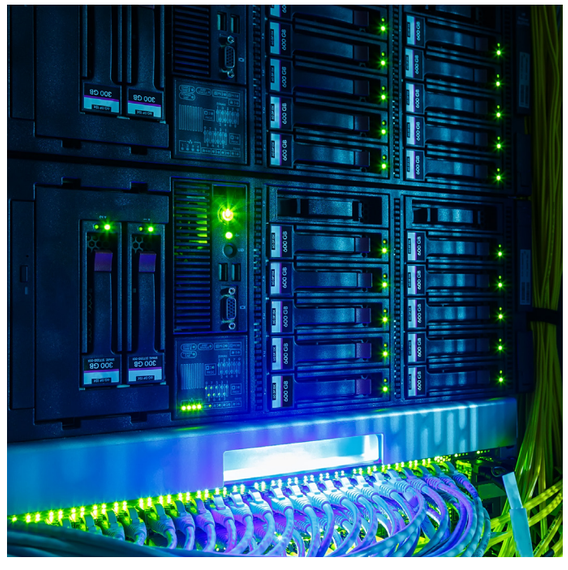


HyperLedger

Hyperledger is a project started in December 2015 by the Linux Foundation, and currently supported by big industry players such as Cisco, Fujitsu, Hitachi, Huawei, IBM, Intel, NEC, Nokia, NTT DATA, Samsung, SAP and Oracle. The main goal of this project is to support cross-industry research and development of blockchain-based distributed ledger and related open-source tools. Hyperledger aims at becoming a hub for the innovation of the management of global business transactions, especially for major technological, financial and supply chain companies, with particular attention on performance and reliability.

Among the different projects that compose Hyperledger it is possible to find Burrow (a smart contract machine based on EVM), Composer (a tool for building blockchain business networks), Explorer (to query the ledger and make it possible to create user-friendly web applications), Indy (a collection of tools, libraries and further components for decentralized identities on blockchains) and Cello (a blockchain as-a-service deployment model). However, the most famous projects are probably Sawtooth and Fabric.

On the one hand, Sawtooth is a modular blockchain suite developed by Intel, written in Python and successfully employed in use cases such as supply chain tracking, bonds transfers and digital assets management. Sawtooth is characterized by a novel consensus mechanism called Proof of Elapsed Time (PoeT).



In PoeT, network mining rights are fairly distributed by means of a sort of lottery in which each participating node is required to call a secure CPU instruction (which is more and more available in new processors like Intel builds) to request a random wait time: the first node that wakes up after the sleep wins the right to build the new block, getting write access to the blockchain. Differently from other blockchains, the validators do not need specialized “mining” hardware and do not have to spend money (or energy) to perform their task (thus the winning validator does not receive any reward for its work): in this way, environmental and energy-consumption issues connected with Proof of Work consensus algorithms are completely solved.

On the other hand, Fabric is a production-ready and plug-and-play solution, implemented in Go and presented in 2017 by IBM, for the development of blockchain-based permissioned and modular architectures. Its main goal is the development of high-scaling (up to more than 1.000 transactions per second) blockchain applications with a flexible degree of permissions. Components such as consensus and membership services can be customized to match the target application requirements. Fabric has typically tewer nodes than a public blockchain and usually requires participants to register to join the network and issue transactions. It also supports confidential data, thus providing its uses with privacy by design. Fabric also includes a smart contract system called Chaincode, which exploits container technology (i.e. Docker) to host and execute the application logic of the system (such as the business logic of assets and the rules for reading and altering their state). Smart Contracts can be written in Go and JavaScript, even though other languages (such as Java) can be used by installing appropriate modules. Another peculiar characteristic of Fabric is the distinction in the roles of the nodes composing the network infrastructure. In Fabric, in fact, the nodes that build, validate and propagate transactions and execute chaincode are separated by design from the nodes that ensure the consistency of the blockchain, ordering and delivering the endorsed transactions to the peers of the network.

Instead of focusing on cryptocurrencies and tokens, the Hyperledger project mainly works on blockchain backbones, frameworks and integration tools. In this context, the different projects that orbit around Hyperledger constitute a very interesting ecosystem for the development of high-scaling blockchain-based industrial applications. The number and the relevance of the partners that are currently contributing to the Hyperledger project represent another non negligible advantage.

Stellar

Stellar was developed and launched by Jed McCaleb, former founder of Mt. Gox and Ripple, in 2014. Its main aim was to create a cross border network of assets exchange. With respect to Ripple, it focused more on protocol openness: Stellar ledger is open for view, and doesn’t require permission to join. Moreover, Stellar is non for profit, and promotes development within its ecosystem.

One of the main feature of Stellar is its ability to represent real world assets, to be exchanged freely by users, relying on trusted anchors. Anchors are gateways that accepts assets from users, register them on the ledger, and are responsible for preserving them. The property of the assets represented can then be digitally transferred among accounts.

For consensus, Stellar uses a variation of the Bizantine Agreement that generalizes the notion of quorum (a quorum is the minimum number of nodes that must converge on a statement to reach consensus). In Federated Bizantine Agreement, nodes can decide to trust smaller sets of peers (slices) to vote on. The consensus mechanism allows to achieve throughputs in the order of the thousands transactions per second.

One of the potential problems arises from the fact the consensus protocol works properly only if the slices chosen by nodes exhibit some topological features (e.g: the slices must be overlapping). Another issue is that, even if the real-world assets representation is very flexible, it requires trust in the anchors that act both as gateways and custodians of the assets.

The way Stellar generalizes the Byzantine Agreement, allowing nodes to make evaluations about the trustworthiness of a set of nodes, is one of its outstanding features among other platforms. Under the assumption that nodes make the right choice in choosing proper sets of nodes, this improves reliability and raises decentralization.

Even though it allows for simple programmability, its lack of Turing-completeness does not position it head on against Ethereum and other smart contract focused platforms such as EOS. Its native ability to represent external assets, through the collaboration with gateway actors and institutions, make it a competitor with Ripple and, indirectly, with stablecoin tokens issued on other platforms. With respect to Ripple, it focuses on inclusiveness and openness, giving its explicit aim to offer low cost financial tools that can be adopted even in developing countries.

Ripple

Even though the conceptual foundation of the Ripple protocol were laid in 2004, Jed McCaleb begun seeking investments for the company Ripple Labs in 2013.

The problem that it meant to solve was that of cross border, interbank transfer of value and assets. The scene was (and still is) dominated by the SWIFT system, that dates back to 1973. Ripple addresses the problem of transfer value by letting financial actors building a network of credit lines, that somehow resemble the payment channel of Bitcoin lightning network. Actors involved in a transaction exchange IOUs, that are recorded and accounted in a ledger. Crucially, the ledger is currency agnostic, in that IOUs can be expressed/valued in any currency that both the counterparties accept. IOUs can be transferred and used to compensate debts, so that if A owes B 1000€, B owes C 1000€, and C owes A 500€, the IOUs can “ripple” through the network, and settle to a situation where A owes C 500€. The network features a token, XRP - present in finite supply, is needed to perform operations, and it is used mainly as a protection against network flooding and spam. XRP can itself be used as a payment instrument.

Ripple ledger is updated using a consensus mechanism peculiarly based on trust relationships. Sets of verified transactions, and consequent updated versions of the ledger are agreed upon by a set of validators, that are special nodes that control issued transactions, validate them, and signal the information to the rest of the network. Crucially, each validator has a Unique Node List (UNL) of validators it trusts. In principle, everyone could run a node and enable the validator behavior, but the effective role and weight in the consensus process depends on being inserted in some other validators UNL. Validators, then, to propose themselves have to be identified. This makes Ripple’s a peculiar protocol, that is technically permissionless, but in which validators have to be identifiable to gain other nodes trust.

Non native assets (i.e. not XRP) accounted on Ripple “enter” through gateways, institutions that accept assets from users, guard them over time, and acknowledge to give the asset back in change for the corresponding digital representation. Gateways are held accountable by local jurisdictions, and have to undergo KYC and AML procedures. Ripple Labs is a for profit company, and provides solutions to financial actors for specific applications needs, such as connectors with SWIFT, payment interfaces for businesses, tools to manage liquidity, etc.

Ripple main feature is the ability to track and account for asset transactions among to perform payments. Its architecture, based on a consensus mechanism that requires trust between actors, of which incentivizes identification, and gateways that are recognizable points where “real” assets enter the network, make it particularly suitable for adoption by existing, “traditional” financial institution, and software financial solutions software by Ripple Labs makes the the most prominent and mature platform for world wide payments that aim at minimizing friction with regulatory constraints.

Hashgraph/Hedera

Hashgraph is a consensus mechanism devised by Leemon Baird in 2014. Its first industrial exploitation was within the society Swirlds, funded by Baird and Mance Harmon, that focused on the development of a private ledger. In the fall of 2017 another company, Hedera, was spun off Swirlds, with the aim of using hashgraph to build and deploy a public ledger.

The main difference with other consensus mechanisms is that there are no competing attempts at ordering transactions, like in Bitcoin or Ethereum blocks building and mining. In hashgraph every node can generate transactions, and sends them into the network. Transactions are then propagated to other nodes with a gossip algorithm, similarly to what happens in Bitcoin. In addition, pairs of nodes involved in a gossiping event generate some information about their communication, that is also propagated. This way, nodes become aware not only of transactions, but also of how they travelled through the network. This information is then exploited to compute a commonly agreed timestamp for every transaction through a stake-weighted virtual voting mechanism. Since anyone can join the network as a validating node, the mechanism is indeed permissionless. According to authors, the algorithm guarantees asynchronous byzantine fault tolerance, fairness, and scalability bounded only by network capacity.

While the consensus mechanism is permissionless, Hedera embraces a permissioned governance model, centered on a council composed of up to 39 members, taken from industry and geographically distributed, with equal vote right and serving limited terms. Aim of the governance model is mainly to prevent the risk of forks. The governance model is inspired by that used originally by VISA. Hedera, like other platforms, contemplates a mechanism to represent real-world identities in the ledger, to cope with present and future regulatory constraints.

Hashgraph allows execution of Turing-complete smart contracts, with resource usage regulated by gas, as in Ethereum. It also natively incorporates the notion of “shard”, that allows contracts to be executed only by portions of the networks (sharding is a mechanism contemplated also in the Ethereum roadmap to improve performance and reduce resource usage).

Hedera main peculiarities are its novel distributed consensus mechanism, with potentially substantial advantages in on-chain throughput and scalability, and its duality of permissionless consensus and “permissioned” governance based on a council of selected members. At time of writing Hedera is available as a testnet, and connecting requires a registration procedure.

Cardano

Cardano was founded In 2015 by Charles Hoskinson and Jeremy Wood, as a product of the IOHK (Input Output Hong Kong) research and development company.

The distinctive feature of Cardano is its “research-first” approach to design. Peculiarly, the project is not informed by a foundational whitepaper, but rather by a set of design principles, among which: implementation of core components in highly modular functional code, small groups of academics and developers competing with peer reviewed research, development of a decentralized funding mechanism for future work, a long-term view on improving the design of cryptocurrencies so they can work on mobile devices with a reasonable and secure user experience, abstracting transactions to include optional metadata in order to better conform to the needs of legacy systems, find a healthy middle ground for regulators to interact with commerce without compromising some core principles inherited from Bitcoin

The consensus mechanism, called OUROBOROS, is based on proof of stake, in which the block creator is chosen with a fair coin tossing among stakeholders. One of the features of the protocol is a very high throughput. The algorithm, for the first time, was peer reviewed at the Crypto 2017 conference.

Cardano is described by its creators as the 3rd generation of blockchains, in a genealogical line where the first generation was that of Bitcoin, which implemented value transfer without middlemen. The second generation is represented by Ethereum, that introduced advanced programmability, but had problems with scalability and governance. Cardano aims to bring about a generation where consensus mechanisms and governance are carefully planned and thought out, with a slower but more careful and prudent approach.

Cardano foundational idea is that it is unlikely that the first blockchains got it completely right from the start, and that correcting them in evolutive fashion is suboptimal, while it worth to redesign everything from the ground up, extensively analyzing the current approaches, carefully thinking ahead of all the issues etc. The problems highlighted in the analysis process by Cardano are compelling: scalability, chain interoperability, compliance with regulations (through the consideration of identity information, for example). In this sense, Cardano seems to compete with approaches like Algorand’s.

Vechain

VeChain was founded by Sunny Lu, former CIO of Louis Vuitton China, in 2015. Its main declared aim is to build a system with clear applicative and business purposes as driving forces. This perspective is pervasive in all the design of technical and governance architectures. Value exchange and operational costs are represented by two different tokens, with the declared objective of making operation cost stable and predictable.

Predictability is also a goal for the governance and the tightly bound consensus mechanism. Vechain uses a Proof of Authority mechanism, in which authority is distributed among different actors and stakeholders, some of which require to undergo KYC procedures enforced by the Foundation. In general, it is evident an effort to create a consensus architecture encompassing different forces.

Another distinctive feature is the embedding of services and application such as voting and identity verification into the blockchain. This is a design decision that sits at the opposite of minimalist approaches in which the blockchain implements only some core functionalities (mostly consensus), and the other, more applicative features, are built upon it as upper layers.

Another demonstration of Vechain maximalist approach is the design and production of ad-hoc hardware solutions that can “directly” and natively interact with the Vechain blockchain. In particular, they have built a system-on-chip that features technical solutions to guarantee uniqueness and identifiability of the device when used e.g. for tracking purposes. The solutions include generation of hardware protected private keys, and exposure of public key for representation on the blockchain.

Vechain has a very opinionated position towards centralizing some governance and technical design decision, with the clear objective to provide a full fledged, ready to go solution for development of business applications, with supply chain ahead. They are also very active in seeking for partnerships, both with the demand and with the offering (recently also with Deloitte). The strong stance towards early applicability can be both an advantage and a problem: e.g. how locked in from a hardware perspective will be a solution that relies on vechain chips? Some aims, like that of providing predictable operational costs through the stabilization of a native coin, seems very ambitious.

Tendermint / Cosmos

Tendermint is a consensus protocol/ and library that aims at providing a layer upon which it is possible to decentralize any application, written in any language, as long as it represents a deterministic finite state machine. Tendermint defines a core module that implements network transport and base consensus mechanisms, and an Application BlockChain Interface (ABCI), through which an application can process the transactions defining the finite state machine behavior.

With respect to existing systems, Tendermint can be seen as a generalization of popular distributed key-value stores such as Zookeeper, etcd, consul, since it allows to distribute arbitrary applications with a consensus mechanism that is also Bizantine Fault Tolerant. Compared to Bitcoin, Ethereum and other blockchains, Tendermint offers the consensus component in a modular fashion. Tendermint consensus protocol consists of a BFT core that leaves the definition of the validators to the applications: if validators are chosen according to the possession of some token, then the corresponding application chain will feature a PoS consensus, while if the validators belong to a whitelist, the chain assumes permissioned-like features.

Cosmos SDK is a set of modules that facilitate development of application specific blockchains upon Tendermint. Cosmos proposes an opinionated vision where applications are built and deployed on custom blockchains, which communicate exchanging token through atomic swaps.

The main peculiarity of Tendermint, which lays in the software engineering dimension, is its modularization of the elements that form blockchains and distributed applications. Similarly to the way smart contracts generalize cryptocurrencies (building a token system is one of the basic examples of smart contracts in Ethereum), Tendermint seeks to generalyze blockchains (as an example, there is a port of Ethereum and its VM, as an application on top of Tendermint and Cosmos SDK (https://github.com/cosmos/ethermint)).

Quorum

Quorum is basically an enterprise platform for Ethereum private blockchain deployment developed by JPMorgan Chase and supported by several partners, such as Microsoft. The main goal of Quorum is to provide a permissioned implementation of Ethereum, guaranteeing high-performance (in the order of hundreds of transactions per second) and supporting transaction and smart contract privacy. This goal is achieved by means of a layer on top of Ethereum, which makes it possible to perform private transactions and use different consensus algorithms. The main advantages of Quorum can be exploited in application fields such as the financial industry, since banks and other financial institutions typically require the high-speed and high-throughput processing of private transactions among well-known entities.

Being a permissioned solution, only validated and authorized nodes can join the network, thus all the transactions take place between participants that are pre-approved by the designated authority. Quorum exploits this consortium approach to implement its consensus mechanisms and most of its privacy protocols.

Instead of adopting classic PoW or PoS schemes, Quorum offers the possibility of choosing alternative consensus mechanisms, such as PoA (Proof-of-Authority), RAFT (a Crash Fault Tolerant consensus engine for faster blocktimes, transaction finality, and on-demand block creation) or IBFT (an implementation of the Practical Byzantine Fault Tolerance algorithm with modifications).

Privacy is guaranteed by means of peer-to-peer encrypted message exchanges, which make it possible to safely transfer private data to other network nodes without exposing it. Before propagating a private transaction in the network, the sender replaces the payload with the hash of the encrypted data received from one of the component of Quorum enabling private transaction, named Constellation (which is by the way a general-purpose mechanism, non necessarily specific to the blockchain use case). In this way, only authorized nodes can retrieve the actual payload, replacing the placeholder hash included by the sender in the transaction, while the other participants of the network will process the transaction as propagated by the sender (without private data).

One of the main advantages of Quorum, with respect to other permissioned solutions, is its compatibility with the existing tools created for the Ethereum ecosystem, such as Truffle, MetaMask, Remix and OpenZeppelin. In addition to this, the privacy guarantees and the high performance achievable with Quorum make it a good choice for banking companies and financial institutions in general. This is particularly true when considering smart contracts, which can contain investment strategies or sensitive internal information that the owner could be worried to publicly expose.

Nano

Nano cryptocurrency (formerly known as Raiblocks) was conceived in 2017 by Colin LeMahieu.

The main reason of its inception was to address the costs, latency and throughput limitations that, in the coin designer's opinion, prevented main cryptos from becoming a major means of frequent value exchange for small amounts. The blockchain structure, a lattice of connected ledgers, is substantially novel (it's not a fork of other blockchains). The distinctive design goal was to achieve zero cost transactions, with very low latency, high throughput, and high scalability. The features were intentionally kept at a minimum (in the author's words: "Do one thing, and do it well - In block-lattice we trust!"). There is no scripting language, and the protocol even lacks timestamping: value transfer, in its purest meaning, is the only feature.

The main (and the most distinctive) feature of the Nano ledger is the block-lattice structure: each account in the ledger has a specific blockchain of send/receive transactions, which contain the update of the account balance. The lattice structure generates a fruitful asymmetry: an account ledger can only be updated by the account owner. This way, system wide updates are split into the sender transaction, that can be added by the account owner immediately, and the receiver update, that can be performed asynchronously, at any later time. Network spam attacks are prevented using non competitive proof of work (much like hashcash for antispam purposes). Double spends can arise from account owners that produce conflicting state updates. They are solved with a delegated form of proof of stake consensus.

A consequence of the particular ledger design, and of the lack of timestamping, is that there is no total ordering of the transactions. Of course, there are partial orderings in place: in particular, all the transactions relative to a given account are totally ordered.

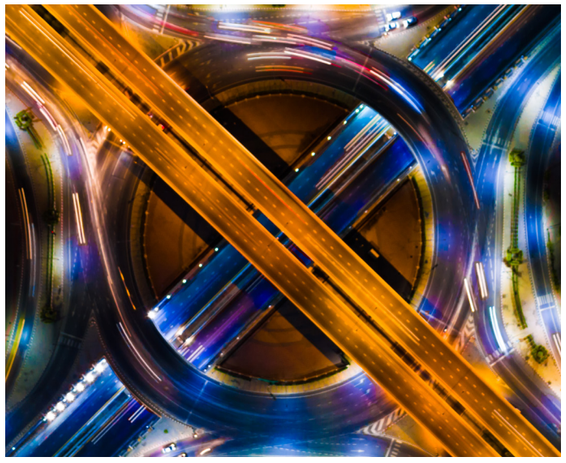
The uniquely essential design of nano makes it an interesting competitor for the niche of economies and applications that require very quick and very frequent value exchanges. With respect to other currencies in the same arena, such as IOTA, it features a sleeker feature set (for instance, there is no attempt to introduce any form of scripting or programmability). Thus, Nano could compete to be the crypto of choice for non programmable micropayments. In this regard, it is complementary with Bitcoin and Ethereum, and it competes with IOTA.

Tempo

Tempo is basically an european-wide anchor (grounded in Paris) for Stellar blockchain payments. The main goal of Tempo is "making money transfer fair and convenient" and it aims at doing that by implementing a fast, easy and secure bridge between cash money and cryptocurrencies. In addition to the EURT digital asset (stabilized with the value of EUR), Tempo provides its users with more than 300 authorized agent locations in Europe and a payment network with over 105 000 payout locations in almost 100 countries worldwide.

The EURT is a stable crypto coin on the Stellar blockchain, backed by on hand cash (1 EURT = 1 EUR), available for purchase online and usable at all the Tempo service locations. Thus EURT funds can be easily sent to a receiver by means of the Tempo worldwide network, traded for other cryptocurrencies or cashed out one-to-one with euros. In order to guarantee for the EURT stable coin, Tempo has applied for and has obtained a EU PSD license from the ACP arm of the Banque de France, it is regularly audited (since it has to maintain on hand cash for all EURT purchases) and is a member of the International Association of Money Transfer Networks.

In addition to the EURT stable coin, Tempo is currently working to an ICO involving a Tempo token, which is not stable and is mainly intended to provide discounts and customer perks. The main goal of the ICO, as claimed by the Tempo team, is obtaining the resources to increase their business since the Tempo network has grown rapidly but is not profitable yet. Among the initiatives included in the ICO project, the Tempo team propose to fund EURT stable coin (as well as other stable coins) issuance, ensure they are backed by on hand cash, develop new apps for crypto exchanges and payments, create a loyalty reward system, expand their services (such as authorized agents and payout locations) geographically and finally financially support blockchain developers with incentives.



Holochain

Holochain was devised by Arthur Brock and Eric Harris-Braun, and formalized in a whitepaper in 2018. The conceptual starting point is the assumption that complete consensus of all the participants on all the data of all the distributed applications is not necessary. The authors claim that the whole approach turns a tenet of blockchains upside down: data is local first, in that it is generated by the agents while running applications, and stored locally. Data is then shared in the so called "distributed hash table" (DHT), a data structure similar to Bittorrent or the InterPlanetary File System. One of the advantages of this structure is that it allows to distribute storage on the network participants instead of replicating it completely.

Every dapp in Holochain is defined by code whose main role is to provide validation rules that define if some data was generated correctly or not. After an agent generates some data, it sends it to other agents, chosen randomly according to the data hash, for validation before being added to the DHT. If some agent tries to share some bad data, the agents that fail to validate it will gossip the problem to other peers, possibly causing a ban of the malicious agent, according to a mechanism that the authors of Holochain liken to an organism immune system.

Holochains also deployed Holo a platform for hosting running dapps based on a mutual system resource credit relying on the ad-hoc token Holo (same name of the platform).

Holochain essentially implements a multichain approach to the distribution of applications, in which responsibility for correct behavior is upon single agents. It shares scalability and distribution of resources usage advantages with other multichain approaches (such as Nano, Stratis, Komodo, Dragonchain).

A distinctive feature of the Holochain approach is the implicit reputation system that emerges from the "immune system". In terms of development ease, some issues about the difficulty of conceptually structuring applications to fit the DHT are reported. Holochain aims at competing with general purpose dapps platforms such as Ethereum, with the advantages of a multichain based approach.

Monero

Monero is a cryptoasset platform that focuses on privacy and untraceability of transactions. It relies on the CryptoNote protocol, that is the base for other, less capitalized, privacy-centered cryptocurrencies. Monero relies mainly upon two information hiding devices/mechanisms: stealth addresses and ring signatures. Stealth addresses are special addresses that can be used to transfer coins to a recipient, without revealing its identity. The sender uses publicly available information about the receiver (the equivalent of the public key in other systems) to generate an address that can be controlled only by the receiver, and makes it impossible for anyone else to link to his address. To protect the identity of the sender, CryptoNote coins exploits ring signatures: the sender generates a signature that allows the transaction (unlocks the output), but comprises a set of other keys, and from the outside it's not possible to tell which key actually did the unlock.

Monero is the main platform for private, untraceable payments (and the main one relying on CryptoNote). This makes it attractive for a set of uses, some of which could attract regulators concerns. Its main competitor is ZCash, that uses a more advanced (with higher obfuscating power) cryptographic device (zero knowledge proofs), but is afflicted by other problems, in particular the requirement of an initial trusted setup that use randomness that, if not deleted, would allow to forge proofs.

Grin

Grin is a quite recent open-source cryptocurrency project implementing a MimbleWimble blockchain and officially launched at the beginning of 2019. For this reason, it is still in an "experimental state", and it is emblematic that the developers themselves give this advice to the user: "Use at your own risk!".

The main peculiarity of Grin is its lack of amounts and addresses, which alone guarantees complete privacy (by default). As an example, to spend a Grin output transaction, in the form of "(r*G) + (v*H)", a user should know both the so-called blinding factor (r) and the amount of Grin available (v). The latter is known (v) is know both by the sender and the receiver of each transaction, while the blinding factor is a sort of private key chosen (and thus known only) by the recipient of each transaction. For this reason, only the receiver of a particular transaction can spend the Grin associated to it.

Most of the relevant features of Grin are relies on strong cryptographic primitives (mainly Elliptic Curve Cryptography), which are exploited also for removing most of past transaction data, in order to increase scalability and maintain a lightweight chain (potentially orders of magnitude smaller of other similar blockchains), without compromising security.

An interesting consequence of this characteristic is the increased efficiency in the synchronization of new nodes with the rest of the network. Grin is community driven, thus it is not controlled by any company, foundation or individual. In addition to this, it has been launched free of ICO, without pre-mining and founder's reward, thus mainly relying on donations. The project is overall interesting, even though more time is definitely necessary to validate its solidity, especially given the lack of a (financially involved) controlling organization.

Zilliqa

Zilliqa is a blockchain platform whose most distinctive features regard consensus mechanisms, scalability and smart contract language. Consensus is achieved through a multi-stage process in which proof of work is used to initially form validators pools, that in a following step coordinate in a practical Bizantyne Fault Tolerant round to propose and approve blocks. In the selection phase of the consensus process, actors that want to play as validators perform a time-bounded proof of work task. Results are evaluated, and the best performing actors are chosen as validators. For the time of an epoch (a time frame spanning a predefined number of blocks), each validator is chosen in turn to propose a block, and consensus is reached through pBFT.

This peculiar architecture allows to exploit time performance of the pBFT mechanism, while the proof of work admission round prevents Sybil attacks. This way, work expenditure is extremely limited.

Zilliqa features a sharding system that partition nodes in subsets, each of one can reach consensus in parallel with the others, allowing to scale performances with the number of contributing actors. Consensus reached in the shards is then consolidated and merged in new blocks at the blockchain level, making the consensus process hierarchical.

Smart contracts capabilities are based on Scilla, an ad-hoc intermediate language for the specification of smart contract logic. Scilla most notable features, as claimed by proponents, are it ability to address the specific sharding architecture of Zilliqa, for example through the possibility of specifying the size of consensus group for a certain task. Moreover, the language is not Turing complete, and its expressiveness is tuned to allow to perform static analysis by means of reasoning tools such as Coq. Zilliqa competes with other platforms aimed at hosting distributed applications, such as Ethereum. With respect to approaches such as EOS and Vechain it exhibit a more minimalistic stance, with less built-in features (e.g. identity is not natively considered) and a resolute thrust towards basic technology innovation improvement (multistage consensus, statically analyzable language).

Sovrin

The Sovrin project has been launched in September 2016 by the Sovrin Foundation. It aims at creating a global and decentralized system supporting the self-sovereign identity paradigm, in which the identities are owned and controlled by end-users instead of a central authority. The Sovrin network relies upon open-source distributed ledger technologies based on the Hyperledger Indy Project. In particular, Sovrin is a permissioned blockchain governed by the Sovrin Foundation, in which only know, trusted and verified entities can serve as nodes. These entities are called Stewards, and operate by donating time, resources, and computing power to maintain the network while agreeing to abide by the requirements of the Sovrin Governance Framework. Currently, there are over 50 Stewards from 13 countries over six continents, among which Cisco, Deutsche Telekom AG, Digicert, IBM, InfoCert and NEC. However, being a public permissioned distributed ledger, identity owners can freely access the public network, without any restriction. The combination between the presence of trusted nodes and the public access to the system provides the security and the transparency necessary for several kinds of marked-ready applications, without requiring intermediaries or a central authority.

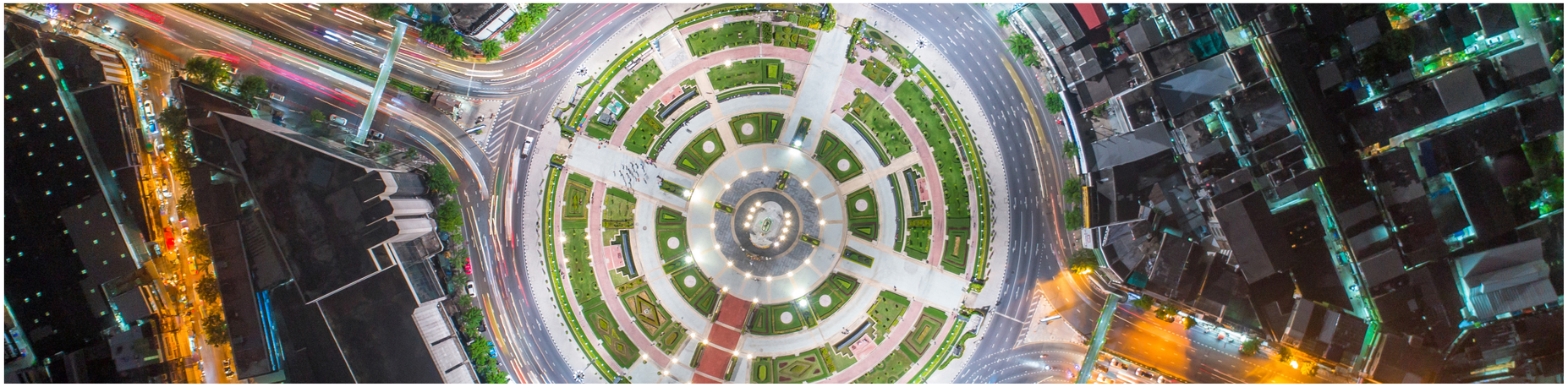
Among the goals and the distinctive features of Sovrin it is possible to find the following:

- Sovrin exploits Decentralized Identifiers (DIDs) and Zero Knowledge Proofs technologies, making it possible to privately issue, control, manage and share digital credentials (or claims).
- In addition, the Sovrin Network aims at defining a new standard for digital identity, in order to let its users (people, organizations, objects) collect, carry and manage their own verifiable digital claims.
- The Sovrin Network makes it possible also for IoT devices to prove facts (or claims) to other objects or to human users, exploiting data that can be easily verified by the other party.
- The Sovrin Foundation is non-profit, committed to transparency and neutrality, and only aims at providing business, legal, and technical support for the Sovrin Network.
- Sovrin relies on the contributions of an active and supportive open source development community community.

From the technological point of view, Sovrin nodes are synchronized by means of an advanced distributed consensus algorithm, called Plenum. This consensus algorithm achieves Byzantine fault tolerance and is essentially based on advanced elliptic-curve cryptography. With respect to classical proof-of-work pro tocols, Plenum achieves higher performance (in theorder of thousands of transactions per second) while providing lower latencies (in the order of seconds).

The Blockchain Galaxy

3. Our view



It appears very hard to make reliable and defined forecasts on the future of the blockchain domain, for different specific reasons: the field is technologically magmatic and evolving; there's much hype and emotivity; there are ideological attitudes that borders with tribalism. It is not dissimilar from the internet of the early days, but emotionally much more loaded, also for financially speculative drivers, in a more destabilizing meta-technological context. Having said that, it is possible to propose some considerations with respect to different "dimensions".

Applicative dimension

Will the only/main usage remain cryptocurrencies, or all the other much anticipated applications (identity, asset tokenization, supply chain distributed information management, decentralized insurance) find practical deployment?

If monetary value representation will be the only significant application, two components must be considered: payments and store of value. For store of value protocol and governance stability, size of the network, and market cap are paramount, Bitcoin would have an upper hand. On the other hand, if the killer application will be payments of any value (-mini and -micro included), other features will be important. Among these are low fees, low latency, high throughput, price stability. Main public blockchains based on proof of work (Bitcoin and Ethereum) have fees that can float with hashing power required to validators and coin value, and their value can float wildly, while other platforms, such as Nano and Iota, are built to minimize fees and latency and maximize throughput. On the other hand, many blockchains could leverage Layer 2 solutions such as Lightning Network and Plasma to build faster payment network. This approach has also raised skepticism among personalities such as Buterin, for their some technical and game-theoretic complexities

(https://www.trustnodes.com/2019/08/22/vitalik-buterin-is-more-and-more-pessimistic-about-scaling-through-second-layers).

At the same time, Ethereum is developing other solutions, among which most notably sharding, which introduce scaling possibilities on layer 1. On the other hand, if beside digital cash, blockchain technologies will be effectively used to deploy products as decentralized apps, then flexible, Turing complete programmability could be a fundamental feature. In this case, Ethereum and those platforms that offer smart contract capabilities will most probably prove indispensable.

Synergic vs competitive dimension

Will the different technologies interact competevely to conquer value and adoption, or will cooperative contexts and synergic mechanics arise?
An important consideration is whether the platforms will interact in a zero sum fashion, where the growth of one is at the disadvantage of another. An example of the zero-sum scenario is that in which store of value is the only application, and every user must decide where to store the value he owns. Most of the other plausible scenarios, on the other hand, are decidedly non-zero sum. For instance, different blockchains (or different tokens) could offer the possibility of distinct, diverse value transfers and interactions. In this case, different platforms wouldn't compete for the same market share, but would instead be able to create value otherwise frozen or not available. Crucially, this scenario will be possible if some interoperability protocols/technologies will become available, such as, for instance Atomic Swaps.

Permissionless vs Permissioned Dimension

Another dichotomy is between permissioned and permissionless solutions. Permissioned at the moment have advantages that span from scalability (in terms of throughput and latency) to costs (low and stable) and simplified (more predictable) governance. These advantages come at the cost of reduced decentralization, mainly in the form of lower resistance to censorship due to collusion of designated validators. In addition, responsibilities are concentrated in the hands of known and potentially small sets of actors.

On the other hand, permissionless technologies are working to fix scalability problems, keeping decentralization as an indispensable feature. Potential solutions are in the domain of permissionless consensus mechanisms (e.g. proof of stake), chain structure (e.g. sharding), hierarchical layering (e.g. Lightning and Plasma). In the long term, it is reasonable to imagine that these approaches will become effective, thus reducing the performance gap between the two classes.

Other reasons why permissioned are currently considered more viable solutions are inherently cultural and psychological: permissioned network may appear more predictable, and even more reliable, even if technically the opposite is true.

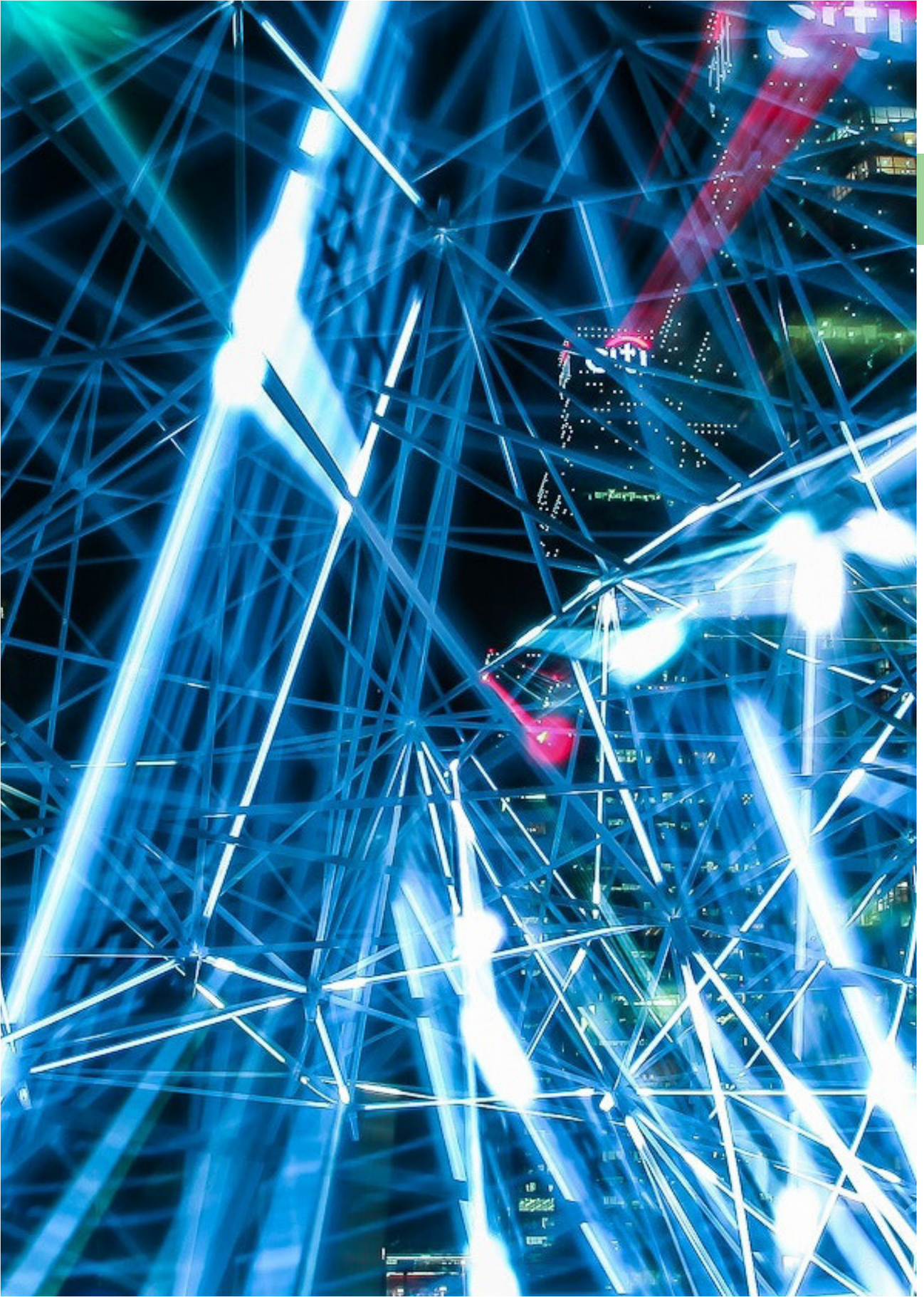
This is similar to what happened with the Internet, where a network with a globally undefined (and undefinable) ownership scared most of the potential early adopters. It is conceivable that this gap will narrow as the technological awareness increases in the operators and users.

Summing up

In the most likely (and interesting) scenario blockchains will interact in a non-zero sum environment, in which many platforms will create value thanks to their different features and qualities, and different applications will be able to exploit the best tradeoff along dimensions such as security, performance, latency, cost, smart contract expressiveness, governance flexibility (or rigidity). In this perspective, trying to forecast market shares of the current technologies is as hard as it is pointless. On the other hand, should a zero-sum scenario play out, competition outcome would depend on main applications, initial network size, technological advantages.

A store of value only (digital gold) scenario would most probably see Bitcoin at the top of the food chain. If payments should play a major role, Bitcoin would have to solve scalability (latency, throughput, fees) issues to maintain a prominent position. The main way for doing that would be through layer 2 solutions. On the other hand, Ethereum will probably feature sharding as a layer 1 solution to improve scalability.

Other solutions such as Ripple, Nano, and Iota are currently pursuing these goals through alternative consensus protocols/algorithms.



Appendix

Blockchain Vocabulary

Blockchain: Blockchain is a type of distributed ledger, where digitally recorded data are stored in packages called blocks. Each block is then 'chained' to the next block, using a cryptographic hash.

Byzantine Fault Tolerance (BFT): A Byzantine fault is a condition of a distributed computing systems, where a) components may fail and b) there is imperfect information if a component has failed. The term takes its name from the "Byzantine Generals' Problem" where actors must agree on a concerted strategy to avoid catastrophic system failure, but some of the actors are unreliable. In blockchain technology, the Byzantine fault condition the actors are the peers of the network, while the system failure is to transmit false transactions. In fact, in the absence of BFT, a peer would be able to transmit and post false transactions effectively nullifying the blockchain's reliability. To make things worse, there is no central authority to take over and repair the damage. Therefore the necessity to solve the Byzantine fault problem exploiting consensus algorithms.

Consensus Algorithm: A consensus algorithm ensures that all participants agree on the next block to add to the blockchain which thus constitutes the one and only version of the truth. It also keeps powerful adversaries from successfully forking the chain. The most used forms of consensus algorithms are Proof of Work and Proof of Stake.

Hash: A hash is a function that converts an input of letters and numbers into an output of a fixed length. Hash functions are implemented so that they are hard to invert and guarantee that collisions are hard to find. A hash is created using an algorithm (Bitcoin uses SHA-256).

Initial Coin Offered: An initial coin offering (ICO) is a type of funding using cryptocurrencies. In an ICO, a quantity of cryptocurrency is sold in the form of "tokens" ("coins"), in exchange for legal tender or other cryptocurrencies. The tokens sold are promoted as future functional units of currency if or when the ICO's funding goal is met and the project launches.

Proof of Work: Proof of Work is a system that relies consensus algorithm to computational power. More precisely, a proof of work is a problem which is difficult (costly, time-consuming) to solve but easy for others to verify and which satisfies certain requirements. In the blockchain framework, the proof of work relies on the computation of hashes: in order for a block to be accepted by network participants, the miners must complete a proof of work which covers all of the data in the block. Due to the computational power spent by the miners for the Proof of Work, a miner is remunerated with transaction costs and/or an amount of newly-generated cryptocurrency once a block he/she mined is accepted by the network.

Proof of Stake: Proof of Stake is an alternative to the proof-of-work system, in which your existing stake in a cryptocurrency (the amount of that currency that you hold) is used to calculate the amount of that currency that you can mine. More precisely, the creator of the next block is chosen via an algorithm which combines randomization with stake. The probability of being chosen as the next proposer of a block is proportional to the stake one holds.

Blockchain Features

In the following, we describe for each blockchain

- If it is Permisionless or not
- Which kind of Consensus Protocol/Mechanism is considered
- Known issues
- If it is Open Source (github, ..)
- Possibility to change type of ownership (ex. From private to public)
- Availability of off/on chain ausiliary applications (IPFS, digital Id)
- Scalability
- Turing completeness
- Functional/Imperative available languages
- If it as Native Currency
- Genesis (source coingecko)
- Number of contributors (source coingecko - Nov 14, 2018)
- Number of Reddit Subscribers (source coingecko - Nov 14, 2018)
- Blockchain Protocol Main Goal
- Number of Running ICO
- Coin Economy
- Cost of 51% Attack
- Governance
- Industrial Partnership

Contacts

Paolo Gianturco | Equity Partner
Business Operations & FinTech leader
Deloitte Consulting S.r.l.
pgianturco@deloitte.it

Gabriele Tamburini | Manager
Business Operation & Blockchain
Deloitte Consulting S.r.l.
gtamburini@deloitte.it

Marco Mione | Manager
FinTech Team
Deloitte Consulting S.r.l.
mmione@deloitte.it

Guzzoni Emanuele | Manager
Banking & Capital Markets
Deloitte Consulting S.r.l.
eguzzoni@deloitte.it

A special thanks for their contributions in the making of this research goes to:
Emilio Barucci, **Francesco Bruschi**, **Daniele Marazzina** and **Vincenzo Rana** of the Dipartimento di Matematica of the Politecnico di Milano.

Deloitte.

Deloitte Creative Team - Italia | SG.049.20