BLOCKCHAIN

TÜRKİYE

CONCEPTUAL ARCHITECTURE FOR BLOCKCHAIN

Blockchain Turkey Platform, Social Impact and Training Working Group Report

MAY 2019

TBV

TÜRKİYE BİLİŞİM VAKFI

BLOCKCHAIN TÜRKİYE

CONCEPTUAL ARCHITECTURE FOR BLOCKCHAIN

Blockchain Turkey Platform, Social Impact and Training Working Group Report

MAY 2019

***

Design and Graphic Works
TERMİNAL MEDYA LTD. ŞTİ.
Maslak Mah. Bilim Sokak No: 5 SUN Plaza Kat: 13 Sarıyer/İSTANBUL
0(212) 367 4988 ve 0(532)643 6959

Editor
ÖZLEM ÖZKAN

Graphic Works
GÜLİSTAN ŞENOL

Printing
SET POZİTİF MATBAACILIK
Maslak Mah. Ahi Evran Cad. Rentaş İş Mrkz.
A Blok No: 62 Sarıyer/İSTANBUL
0(212) 286 4933

Social Impactand and Training

DISCLAIMER

"This report prepared by the "Social Impact and Training Working Group" of Blockchain Turkey Platform operating under Turkish Informatics Foundation has been prepared to to offer solutions for solving the problems encountered in the management of this report provide chain is for informational purposes only, people and institutions binding recommendations or opinions does not qualify. This report contains information from publicly available sources and is not guaranteed to be up-to-date and complete. All information and opinions given in this report may change in time. Within this context, this report has no responsibilities or obligations against individuals reading its content or any third parties."

CONTENTS

Presentation 5

Contributing Institutions 6

Preface 7

Executive Summary 9

1. Introduction 10

2. Vision and Strategy 14

3. Business Architecture Domain 17

4. Data Architecture Domain 21

5. Application Architecture Domain 24

6. Technology Architecture Domain 27

Contributors 32

References 33

TÜRKİYE BİLİŞİM VAKFI

Turkish Informatics Foundation (TBV) *was founded with the aim of transforming Turkey into an information society by contributing to the development of the required infrastructure and increasing the share of information technology in the country's economy by pursuing economic and social studies, undertaking scientific R&D, creating relevant projects and ensuring their application.*

BLOCKCHAIN
TÜRKİYE

The Blockchain Turkey Platform *was founded with the aim of creating a sustainable blockchain ecosystem in Turkey and alleviating the difficulties in the new modes of conducting business by creating a sharing platform, both led by the Turkish Informatics Foundation (TBV).*

PRESENTATION

Faruk Eczacıbaşı
Turkish Informatics Foundation (TBV)
Chairman of the Board

When we founded Turkish Informatics Foundation (TBV) in 1995, it had a simple mission: Leverage information and communications technologies to increase the country's productivity. Call it Industry 4.0 or the information society, the world has entered a period of acceleration, forcing us to change our thinking.

Blockchain is likely to be one of the most transformative products of this new line of thinking and further experience is needed for it to be properly understood and applied. As in every new technology, blockchain needs to evolve from the experimental stage, which involves conceptual thinking, to the pilot stage and on to the final product.

Blockchain's dependence on collaboration, which manifests itself in settings such as inter-industry consortia and other platforms, sets it apart from other technologies. Blockchain gives prominence to ecosystems, especially those that create value through collaboration instead of comprising individual companies with their own products.

Accordingly, as Turkish Informatics Foundation, we took action on 8 June 2011. We launched the blockchain Turkey Platform (BCTR) to increase the prevalence of, awareness about and usage of blockchain in Turkey and to identify blockchain's strategic priorities. BCTR is a sharing platform which aims to alleviate the difficulties in the new ways of conducting business by creating a sustainable blockchain ecosystem.

I sincerely hope that, as the world migrates from the "build and sell" business model - to which we've grown accustomed since the invention of the steam machine - to the "co-create & presume" way of thinking, this platform and its work are beneficial for our country.

CONTRIBUTING INSTITUTIONS

BKM
BANKALARARASI
KART MERKEZİ

Garanti BBVA

softtech

TÜBİTAK
BİLGEM

PREFACE

Barış Özistek

Chairman of the
Board of Directors of
Boğaziçi Ventures

One of the most distinctive characteristics of blockchain is the need for multiple participants. This feature has both advantages and disadvantages in different aspects. When you read the contents of the report, you will see how different competencies and technologies need to come together in order to solve problems using blockchain technology effectively. We believe what's important is to get the maximum benefit from the advantages and also eliminate the disadvantages as much as possible. Right at this point, blockchain Turkey Platform (BCTR) has filled a critical gap and created a very productive environment for the need of working-together, which is in the nature of blockchain, by bringing together many organizations and individuals from different sectors and interests all around Turkey.

In order to acquire the right gains, the BCTR platform carries out its works by handling the blockchain technology and the paradigm shift created by its effect, through multidimensional working areas created both vertically and horizontally. While sectoral value fields are evaluated vertically, this technology and the change of paradigms are studied with different aspects horizontally.

Technology working group, one of the horizontal workgroup, aims to contribute to the definition, development and dissemination of this technology by tackling blockchain from a technical perspective. In this context, it started its studies by making a technical definition for blockchain and formed the conceptual architecture in this report as the first output. Just like any other newly developed and emerging technology, there is a confusion in both the scope and alternative components. Considering blockchain as a solution and defining it with only a conceptual systematic and independent of its current areas of use would help to relieve this confusion. In addition to this gain, it will be beneficial to create a common language for all stakeholders in the blockchain ecosystem and to create a common instrument of assessment for both strategy determination and choosing among alternatives.

Unlike conventional industries, the world of technology constantly offers us new opportunities and capabilities. Turkey can catch up with the change that will come along with the blockchain technology, or even may be a leading actor. In this sense, I congratulate the BCTR Technology working group who prepared this report, which I believe will be of great benefit to all readers, and extend my gratitude to all the working group stakeholders who contributed, to the valuable companies and the BCTR platform who provided this opportunity.

Best regards.

EXECUTIVE SUMMARY

Among the most important obstacles preventing the further spreading blockchain-based use cases, we can name both the inadequacy in understanding the intrinsic characteristics of this new technology and the confusion caused by this problem coming to fore also through an implementation of this technology.

In overcoming this problem, it will be useful to initially see blockchain as a solution and then to be able to assess strategies and alternatives for this solution on the basis of a common framework. For this purpose, it was aimed to create a reference architecture definition for blockchain. It is expected, therefore, that it will be beneficial regarding the following matters: "Providing a common infrastructure for comparing different solution alternatives showing up within the scope of blockchain", "A clear determination of the definitions and scope areas of each alternative", "A framework that will be used in conformity assessment of blockchain for solving real world problems", and "Creating a common language for all stakeholders from different interest and knowledge levels who will work within this system/solution". Architectural definition is a practice that is used to define the organization of the basic components of a system. Depending on the complexity of the systems, these organizations can be defined at different levels of detail; we will be content with the conceptual architecture definition, which is the highest level of detail within this version of the report. Definition at conceptual level consists of classifying system components based on certain domains of interest (domains/addressed embraced in the report are indicated as vision/strategy and requirements, business, data, application and infrastructure). It is important here that the system components to be identified are expressed only in a conceptual terminology, regardless of the specific terminology custom to the particular use, technology, or implementation. Similarly, the vertical hierarchies to be determined between the components are generic, regardless of specific uses or designs. Another aspect of architectural definition is perspectives. By foreseeing that there will not be a particular need for certain perspectives at conceptual level, we advanced with a holistic point of view.

1. INTRODUCTION

Especially after the explosion of interest in crypto currencies, blockchain as a technology underneath created a curiosity and agenda in every sector. However, it would be safe to call Bitcoin a concept and solution that even many decision makers from both business and technology still have difficulties in interpreting it correctly. Underneath these difficulties, in addition to the fact that blockchain's factual characteristics differ from a technological invention, it is possible to show the confusion that is due to the application of the agenda itself. For whatever the reason might be, considering blockchain as a solution and defining it with only a conceptual systematic and independent (neutrally) of its current implementations and practices would help to relieve this confusion.

In order to realize this aim, we will try to create a conceptual architecture that is specific to blockchain. Architectural definition is a practice that is used to define the organization of the components of a system. Depending on the complexity of the systems, these organizations can be defined at different levels of detail. We will be content with the conceptual architecture definition, which is the highest level of detail within this version of the report. However, it is planned to expand on this conceptual definition in future studies.

Definition at conceptual level consists of classifying system components based on certain fields (for example; data, application, strategy etc.). It is important here that the system components to be identified are expressed only in a conceptual terminology, regardless of the specific terminology for the particular use, technology, or implementation. Similarly, the vertical hierarchies to be determined between the components would be generic, regardless of specific uses or designs. Another aspect of architectural definition is perspectives. By foreseeing that there will not be a particular need for certain perspectives at conceptual level, we will advance with a holistic point of view. However, as the level of detail increases, there will, of course, be a need to make this definition specifically from different perspectives (application, data, infrastructure, etc.).

An architectural definition for a system (or solution) would be beneficial in the following matters: providing a common ground for comparing different solution options showing up within the scope of this system; a clear determination of the definitions and scope of each option; a framework that will be used in conformity assessment for problems; and creating a common language for all stakeholders from different interest and knowledge levels who will work within this system/solution. Therefore, this report aims to define a conceptual framework and terminology that is specific to blockchain.

Although the concept of distributed ledger (DLT) and blockchain are often

used interchangeably, it would be correct to call blockchain a specialized DLT. The key element that distinguishes blockchain from other DLTs is the use of a data structure in which transaction records are organized into blocks and these blocks are cryptographically linked to each other.

As will be discussed later, the value propositions of the blockchain concept are formed based on conflicting requirements and constraints. Therefore, it is not possible to present all the propositions in a single solution and there is a need to make a trade-off between alternatives. There are many different types of blockchain implementations formed according to these preferences. The architectural definition to be made in this report will allow the scope of these different solutions to be formed comparatively over a common framework.

While evaluating the use of blockchain for a problem, one of the various blockchain options is usually focused on and it is proceeded with a black-and-white decision. However, instead of solving the whole problem with blockchain, it is often more effective to use more than one blockchain approaches for the solution by focusing on sub-problems (for example, the notary/audit function can be implemented by including the use of public network in a basic scenario of a private network). At this point, it will be important to compare the value propositions of all alternatives over a common framework.

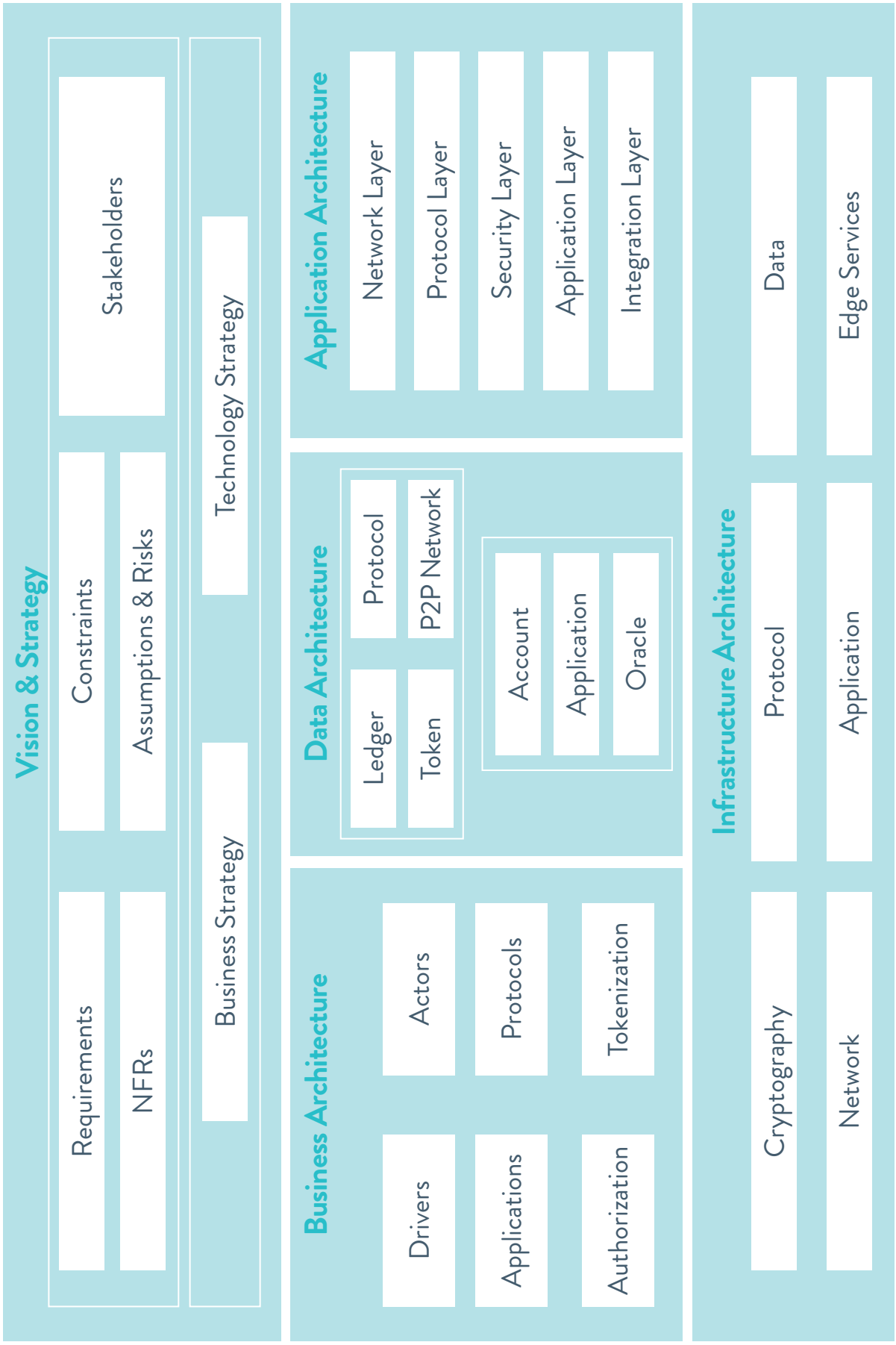
The strategy to consider blockchain as a solution for problems should also include the consideration of many non-functional requirements. Of course, gaining the maximum value from the use of blockchain is the main goal, but due to the constraints of such requirements, it will often be more realistic to follow a strategy of an evolutionary use and adoption. As in the case of Bitcoin, uses in the public network design offer disruptive value propositions, however, its adaptation and expansion to current conjecture still require many uncertainties and sub-problems to be solved. Describing this evolutionary process from scratch with clear scopes would again require a common framework.

Blockchain technology, which has the potential to transform the Internet, changes the way that business is done at the corporate level and introduces new use cases. Today, many companies and consortiums continue their R&D processes and pilot studies related to the use cases that they have reconstructed. Blockchain technology continues to expand its ecosystem with emerging protocols and practices and to be embraced by an ever-growing audience. Today, blockchain platforms focus on three important elements that can be listed as scalability, interoperability and privacy in order to take their technology further. The sectoral distribution of tools, services and infrastructures used and the use cases and applications built on platforms have today focused on social media, instant messaging, content management, advertisement and e-commerce sectors in the domain of B2C.

Distributed applications that we encounter in the B2C domain, where public chains are often used, are likely to replace platforms that we can today call data subjects. In the domain of B2B, we see the tracking, verification and proofing practices that are built with the support of smart contracts in private chains in private chains where relationships between institutions are managed. In the financial sector, we can see the applications that are designed to replace today's services and that include the new value concept to their structures. Blockchain technology can simplify the management of reliable information and facilitate government agencies' access and use of critical public sector data while maintaining the security of this information. Data stored in a public or private blockchain cannot be modified or deleted by a single user; instead, they are verified and managed using automation and governance protocols. In the data sector, which is reshaped within the framework of these features, we encounter blockchain practices where personal data is evaluated from a different perspective and artificial intelligence technology is included.

The rest of the report describes the conceptual architectural definition created. The diagram describing this definition is shown in Figure 1. As it can be understood from this diagram, the system definition has been created by making a classification on 5 main areas in parallel with the general architectural practice and detailed descriptions are provided for each of them later in this paper.

Figure 1 **High-level Blockchain Conceptual Architecture**



2. ARCHITECTURAL VISION & STRATEGY

Blockchain is a special type of the decentralized digital ledger (registry) concept. This is implemented by a technology that ensures that the records remain unalterable by ensuring that the records are confirmed and stored as peer-to-peer copies and in coordination on computers on a peer-to-peer (P2P) network. In this way, it performs its vision to operate in a secure, inalterable, transparent, democratic and controllable manner.

This vision has emerged to meet a number of requirements, and these requirements are addressed by some principles that are common for all blockchain protocols. These are the need for more than one stakeholders to be able to write records in the common and reliable state (data) storage environment, a lack of confidence or hierarchy among such actors who are able to add records, a rejection or unnecessity of a mediator or central authority, rejecting intentional or unintentional alterations of records, and users in ecosystem having an anonymity at a level that is to be determined based on the fiction.

In addition to these functional requirements, non-functional requirements are also considered as important decision points that affect the performance of blockchain solutions. In the technical context, these can be listed as scalability, speed and throughput, system reliability (fork problem, vulnerabilities in common decision-making mechanisms, etc.), integration and interoperability with other systems, maturity/standardization level of technique and process, and efficiency (costs such as power and time, etc.). However, addressing non-functional requirements only in a technical context would be restrictive, which would make it difficult to make realistic decisions. For this reason, it is important to evaluate some requirements in terms of political, economic, cultural and sociological aspects while designing solutions within the blockchain concept; the degree of compliance with regulations and administrative policies, risk factors related to cultural and social behavior (trust, sociopathy, the need for change, etc.), and the need for cooperation can be listed among such requirements.

As can be seen, the decision to use blockchain requires many assessments. In other words, it is wrong to think that blockchain as a silver bullet. Because, in addition to these requirements, the solution also includes some risks and assumptions. Therefore, the factors such as the expected developments in quantum computing in risk assessment, malicious users and uses, the governance of the software and the adaptation of the users to the changes should be considered as well.

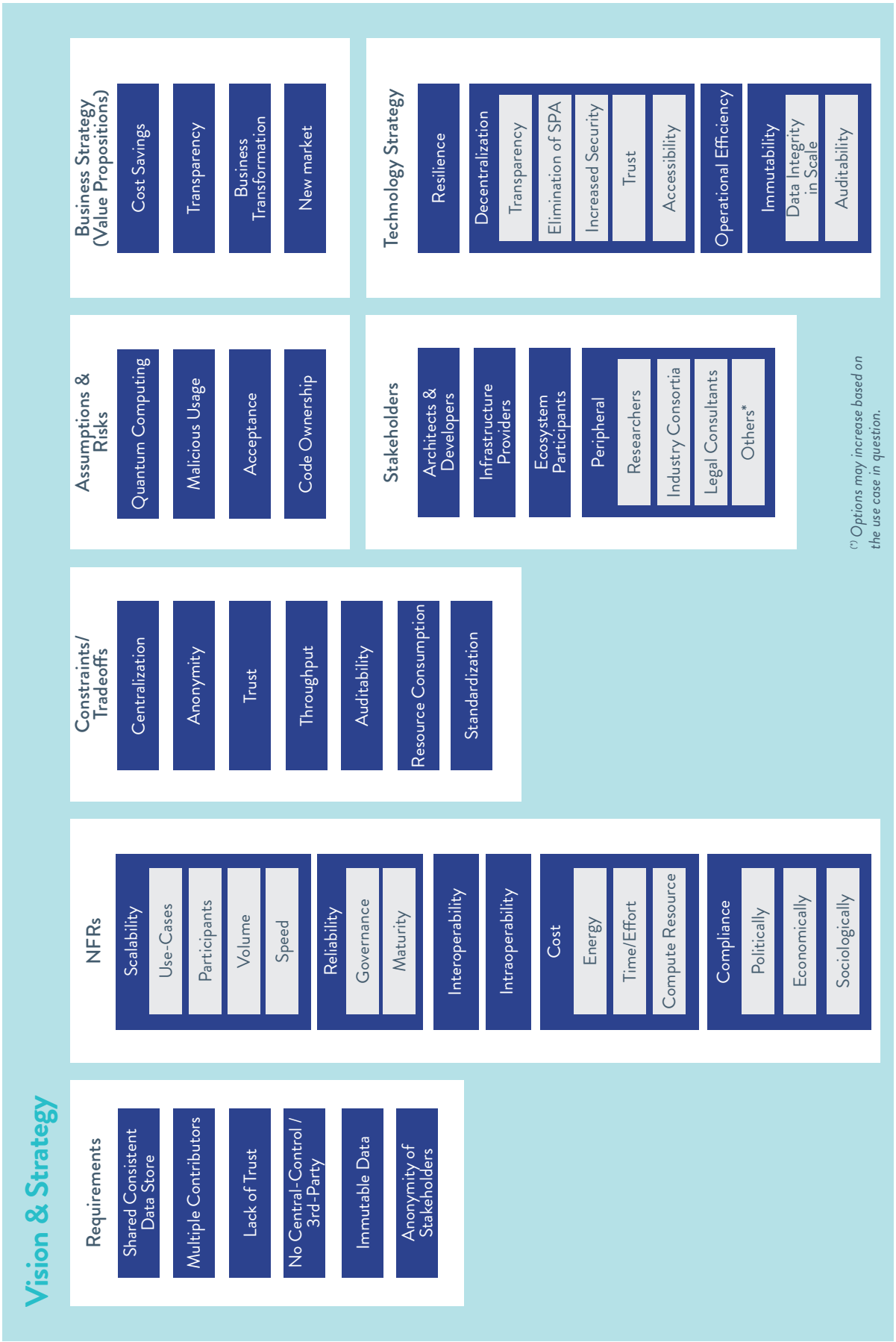
The decision to use blockchain as a solution is often for realizing the

strategies for institutions and organizations, such as cost saving, increasing the auditability, transforming an existing line/process of business or creating an entirely new line of business and its market.

In addition to these commercial strategies, they are also used specific to the technology strategy for the following gains: Providing resilience by spreading the single point of failure; transparency, security, confidentiality and operational productivity through eliminating the central authority; auditability and conformity thanks to guaranteeing the inalterability of data.

The concept of blockchain can be implemented to have different characteristics according to the configurations of the aforementioned architectural structures and components. However, even though their characteristics are different, the key stakeholders involved in all implementations are generally common and are composed of architects and developers, infrastructure providers, ecosystem participants (network users), researchers and other environmental stakeholders.

Figure 2 **Architectural Vision and Requirements Domain**



3. BUSINESS ARCHITECTURE DOMAIN

Technological advancements and innovations are constantly developing and expanding. Individuals and institutions should be aware of progress. The paradigm shift brought along by blockchain maintains this evolution in the line of a different perspective. Although the technology behind blockchain is conceptually similar to a database, there are basic concepts that need to be understood in order to properly interpret the technology. Smart contracts, a decentralized consensus, cryptographic proof, inalterable chain structure and the evolution of value are prominent among these concepts. This exciting data processing paradigm plays a critical role in the development of distributed applications. This section will address the paradigm shift that comes along with blockchain technology from a business architecture perspective.

While technological developments continuing to touch people's lives at different points in the course of time, they also brought along the change with the new paradigms that it offered. In a rapidly digitalizing world, while the data is becoming a valuable workable mine, the communication tools have shortened distances, making people's interactions with each other instantaneous. In this context, individual rights have also evolved, and increased their scope and now reached a structure that includes digital indicators. Blockchain technology appears to be a unique tool to interpret and give a meaning to this paradigm change in a healthy way. Blockchain technology proves its potential in shaping the future with its different applications today, providing a decentralized and fully reliable environment dominated by digital values.

The transformation of money, one of the most used tools for centuries, that it had until today has been a source of inspiration for many concepts. The evolving value in art, law and many more fields has become more digitalized day by day. Considering this matter from the perspective of blockchain technology, we see that the assets have evolved into cryptocurrencies, tokens and digital records.

Blockchain technology, also called the Trust Machine, touches the concepts of privacy, transparency and prosperity as well while restoring this phenomenon. Blockchain has an inalterable, verifiable and sustainable structure thanks to the science of cryptography, which derives its power from mathematics.

The actors who play a role in the world of blockchain are using key pairs to express themselves. Users can interact through the public key on the network while maintaining their privacy with the private key. In addition to these, the wallets of users may contain tokens that represent identification data. Another concept represented by blockchain philosophy is the equality

arising from decentralization. Blockchain technology, which uses consensus algorithms to create a decentralized democratic environment, ensures that the entire network is equal.

The power of smart contracts will be utilized at the stage where this equality becomes independent of individuals/institutions and is evolved into autonomous management, audit and legal systems. Smart contracts, which are a set of coded rules, accelerate many processes of today, reducing costs and human-induced errors.

Blockchain, a matter of ecosystem, is expanding its field of use with protocols that continue to evolve. Its growing field of use increases the number of core roles serving the technology day by day. Miners taking on the load of processing in order to maintain existing platforms, alongside users and investors, developer communities working to provide a more advanced experience, stock exchanges involved in the exchange of cryptocurrencies, wallets that ensure the secure storage of assets, regulators/law units supervising the introduction of this technology into our lives and the following process, and organizations that come together to ensure better adoption of blockchain by the end user can be listed as core roles of the ecosystem that constitutes today's blockchain technology.

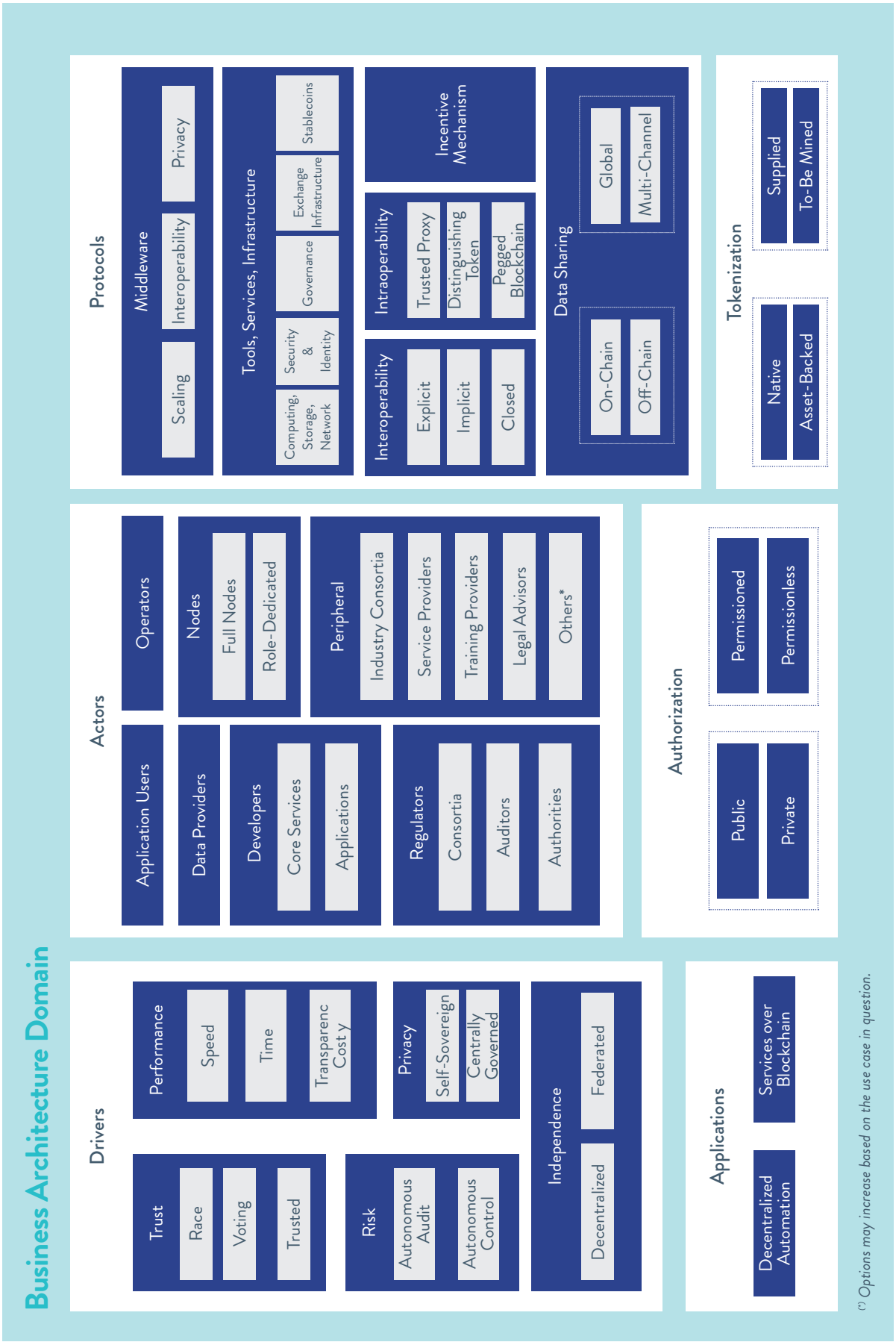
In order to use blockchain technology more efficiently in today's areas of use, some restrictions must be overcome. The transaction capacity that a blockchain network can process is called scalability. A scalable system must be able to process all transactions on the network without being affected by network stress. Scalability is one of the most important problems for existing blockchain protocols, and we keep encountering solutions at different layers. On-chain solutions require a modification in the code base on the primary layer of blockchain. An example for this can be to increase the block size limit from 1 MB to 10 MB, or to reduce the block generation time from 10 minutes to 5 minutes. It should not be overlooked that changes in the structural properties of blockchain may require hard-fork.

Second-layer scalability solutions, on the other hand, concentrate on saving space and reducing network congestion. These solutions, called off-chains, refer to the secondary layers built on blockchain protocols and often appear as side chains and channels. There are mechanisms that facilitate the process of reaching a consensus for a greater scalability and in order to process more transactions. Various projects have developed and managed these consensus mechanisms that can be an applicable solution to the scalability problem. The main scalable consensus models can be listed as Delegated Proof-of- Stake, Byzantine Fault Tolerance (BFT) and Proof of Authority. Blockchain technology is a subset of a general DLT due to its distributed architecture. By organizing the information (transactions), there are other distributed ledgers that do not use the same data structure in chain and consecutive blocks.

The most popular form of such distributed ledgers is a technology called Directed Acyclic Graphics (DAG). Interoperability offers a completely new structure for blockchain ecosystem. The problem of interoperability between blockchain systems is due to that the protocols do not speak the same language with each other. Functionality competences of smart contracts, transaction plans and differences in consensus algorithms are some of the factors that dissociate this language.

In order to overcome this problem, a public protocol solution that facilitates the universal communication between each blockchain system is required. Multi-channel frameworks are the environments that help facilitating open communication and transfer of both assets and data across multiple blockchains over a broader network. A standard ecosystem in which each blockchain is part of a larger system can be created with these structures. There are some researches today for frameworks with the competency that would allow the Internet concept of blockchains.

Figure 3 **Business Architecture Domain**



4. DATA ATCHITECTURE DOMAIN

Although there are blockchain solutions with different characteristics in response to different needs, the basic entities to be included in the data model for many blockchain networks are common.

The main component of blockchain, which is a special concept of distributed ledger within the concept of DLT, is this Ledger that is available and shared for common use. Ledger consists of blocks that are kept in the chain data structure, specific to blockchain. A block is a data structure that is used to hold a certain number of transactions together, as is evident from its their name. The first ring of the chain data structure has a special structure, as it is different from other rings in terms of its method of generation, and is defined as the Genesis block.

A transaction basically includes updates on the generation and status of a defined asset. This asset is identified as unique to each blockchain solution and is called a Token. As well as a token can represent a real-world asset, it might also have been generated purely fictionally in order to ensure the functioning within the blockchain. These details are described in the Token definition. In addition to this, a Token refers to the data at different levels depending on the definition of the asset it represents, which can be kept off-chain rather than on-chain as the size of the data increases or access restrictions take place.

The processes that will procure the gains that blockchain conceptually promises are defined within the system architecture that is called a Protocol. As a matter of fact, the main asset that differentiates blockchain solutions is the Protocol selected; that is, it defines the rules of the game. Despite the differences, all protocols involve some common processes; transaction submission, transaction validation and consensus. Among these processes, especially consensus should be addressed more because of its complexity and high impact factor.

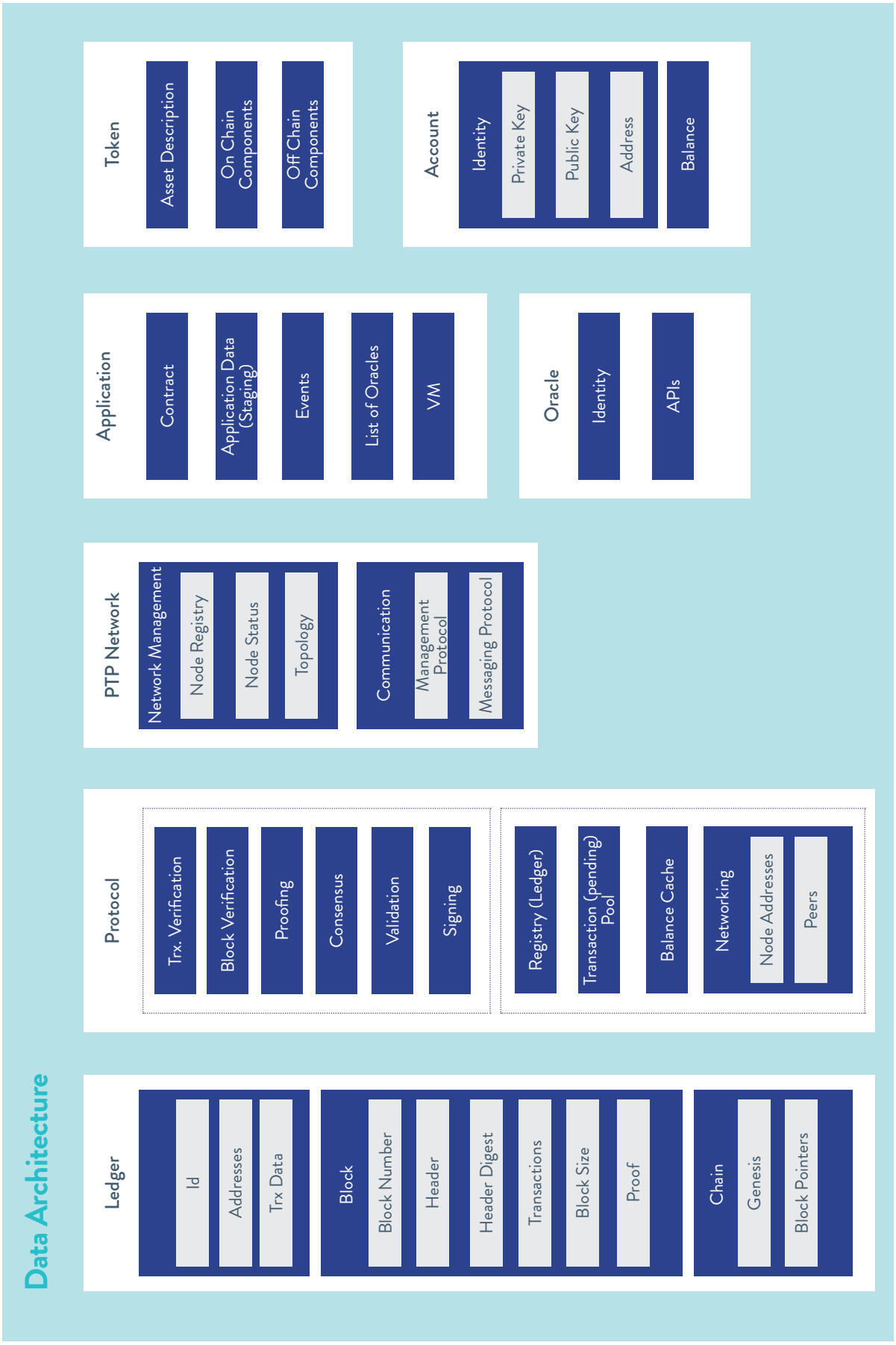
Consensus basically involves two sub-processes; mining or voting based on its type, and verification. Both sub-processes perform so many cryptographic transactions and require data structures related to these transactions. A protocol also defines the data sets that it should work on while carrying out the processes. As it might be guessed, the first data component is the Ledger. Although it is physically identical, this Ledger can conceptually be distinguished as its local copy at the place of processing. Another data structure is the transaction list that processes will use to create a new record. In addition, the balance information of the assets in the system to be utilized in the verification process is kept in a cache- like environment that can be accessed quickly.

The main infrastructure, in which the processes described in the protocol

will be operated, will be a distributed network, but as per blockchain's design principle, it will be peer-to-peer (P2P). A P2P network requires data structures to operate functions related to its own network infrastructure, and also uses separate data structures to perform its communication services.

Blockchain is used as a technological solution to address real-world problems. The applications created based on these problems and their users also take place in the ecosystem with separate data structures. Users are basically defined by an identity and assets they own. On the other hand, applications require different data structures based on numerous application types. While the state and function definitions are sufficient in relatively simpler applications such as contracts, distributed application components require more resources. Some of these resources may even come from interactions with systems outside the ecosystem, which are specifically referred to as Oracle. In the context of the data structure alone, in addition to complexity, applications require more resources in the context of computing requirements, including temporary data sets to be used during computations.

Figure 4 **Data Architecture Domain**



5. APPLICATION ARCHITECTURE DOMAIN

As well as the ones with a customized blockchain application architecture stack usually contain different compositions, they usually consist of six main layers. Main layers can be listed as follows: Network layer, protocol layer, security layer, application (services) layer, integration layer. The network layer consists of a peer-to-peer (P2P) network protocol application that allows blockchain nodes to communicate with each other. Handshake mechanisms and elimination of authorized accesses are embraced within this layer. The peer-to-peer blockchain network prevents any user from controlling the main infrastructure or disabling the entire system. All users on the network are subject to the same protocols. This is why the protocols are the set of rules that governs the network. Blockchain protocols often include rules regarding consensus, transactional validity, and network participation. In addition to basic network functions, additional features are offered for corporate services in private blockchain applications. In addition to these additional features, many network layer solutions are supported by side functions; such as anti-spam filtering and secure messaging infrastructure.

Core functions consist of a consensus mechanism between blockchain nodes for the acceptance of new blocks. The execution or operating sub-layer is a virtual machine that hosts a command set and computing capabilities. The storage and ledger sub-layer is used to store the status of smart contracts and blockchain. Identifying digital assets, sending transactions, processing current transactions, verifying blocks, generating blocks, publishing blocks, and signing blocks are considered common core layer services of blockchain protocols.

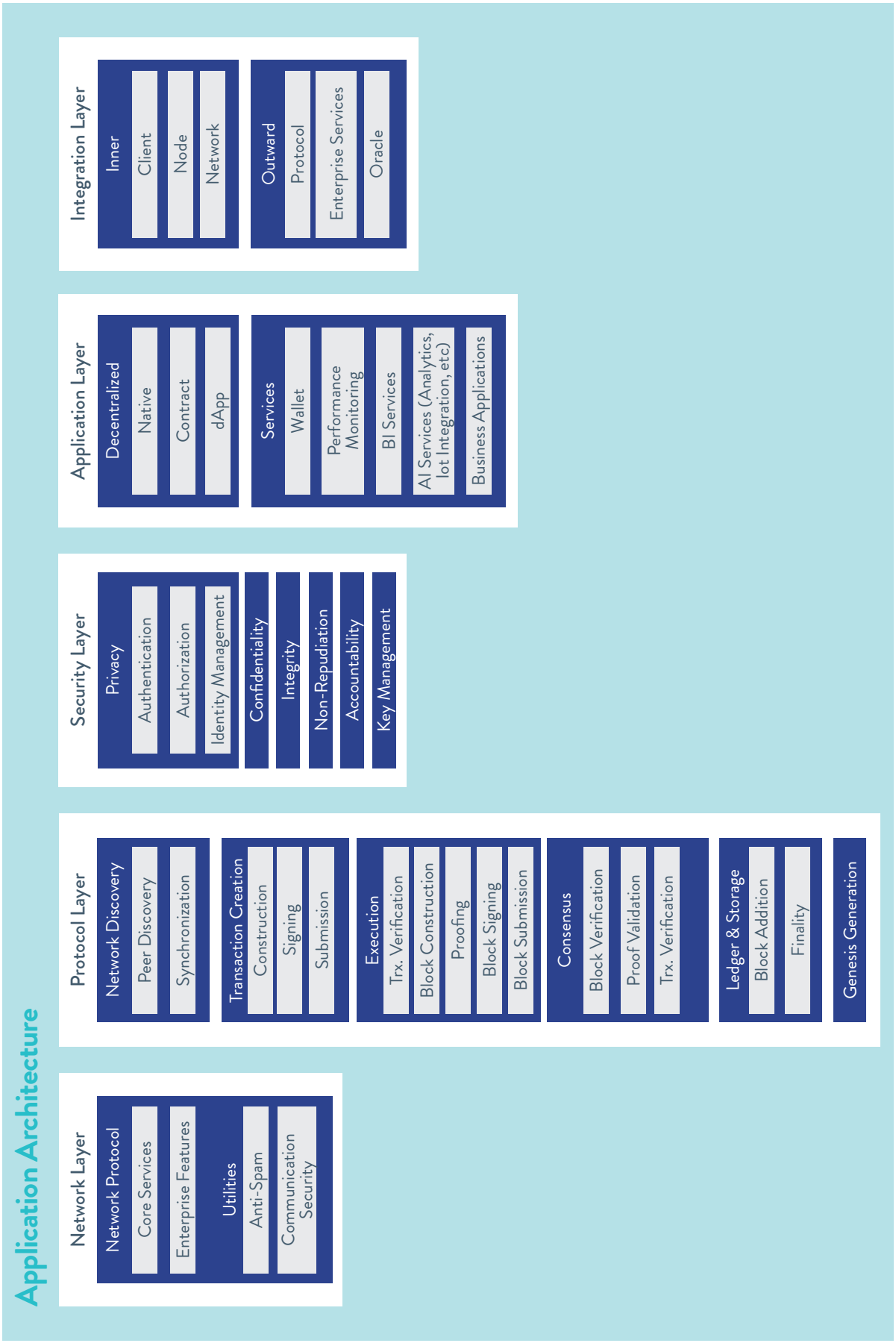
Blockchain technologies used at the enterprise level focus on two important concepts that are not found in public blockchain protocols; permission based structures and sensitive (private) transactions. A blockchain that requires permission consists of a network in which nodes are managed only by “trusted” participants and only authorized users can participate in transactions. The purpose of private transactions is usually to prevent unauthorized users from accessing business logic. This is why the privacy and leveling layer applies the rules of privacy and authority level required for the distribution of blocks. Account management, role-based authorization and permission management are performed at this layer. The security layers of the applications may vary depending on the structure of the blockchain. It is aimed to ensure the conditions of verification, privacy, integrity, accountability and undeniability in all chains. In chain structures requiring permission, the concepts of authorization and identity management should be added to existing security components.

The application (Services) layer is the primary user interface that works

on top of the protocol and network layers. A virtual machine that runs instructions as to the logical operations given in smart contracts is also included in this layer. The layer has two main actors; operators and users. Application operators are those who manage applications that connect to one or more blockchains and provide specific services to users. Examples of these applications include high-level services such as node monitoring applications, chain dashboards, wallets, and other ecosystem applications. Application users are those who indirectly interact with the network through the interface of an application.

The integration layer basically performs functions in two contexts; the interactions of the components within blockchain and the interactions required for the cooperation of blockchain with the outside world. These interactions are carried out, in accordance with the generic valid requirements and standards, independent of the details of the interacting system as much as possible due to the robustness principle.

Figure 5 **Application Architecture Domain**



6. TECHNOLOGY ARCHITECTURE DOMAIN

Blockchain can be defined from infrastructure perspective through investigations on these topics; cryptography, networking technologies, protocols, edge services, data infrastructure, and application design & runtime components.

In terms of network technology (P2P network), blockchain systems can be considered to consist of a combination of three sub-protocols:

>> **Transaction Protocol** includes business layer activities such as cryptocurrency generation by mining, destruction of cryptocurrencies, verification of transactions, and management of digital data.

>> **Consensus Protocol,** is the protocol that blockchain nodes operate among themselves to ensure that accurate and consistent data is written to the ledger. It is a vital component that ensures blockchain's inalterability and prevents illegal transfers. The underlying principle of alternative technologies on this subject generally involves the activities of the nodes having different levels of vote in making collaborative decisions according to their various competencies or attributes (hash power, amount of cryptocurrencies, identity, storage space, etc.). Those are mainly: PoW, PoS, DPoS, PoC, PoE, PoET, PoA, PoB, PoI, BFT, PBFT and DBFT. Multi-core computers and GPU, FPGA and ASIC-based hardware are used for especially consensus transactions.

>> **Network Protocol** is widely used in Gossip protocols. It performs fast spreading of transactions among blockchain nodes, finding peer nodes, downloading blockchain data, and publishing blocks on the network.

Within the scope of Security and Crypto Technologies, various components are used to provide the security function, which is the most important vision of blockchain. Particularly various components of cryptography are used in different combinations for this purpose. Hash and Digital signature components in the example we met with Bitcoin are the building blocks used in almost all blockchain implementations. Hash is used to ensure the inalterability of blocks, and to provide consensus in the block generation process. Digital signature is used primarily to verify the origin of transactions. Various versions of Hash and Digital signature are preferred based on their desired security and performance levels. The majority use Elliptic Curve Cryptography (ECC) technology. In addition to this, Hash-Based signature technology, which is known to be resistant to quantum crypto, is also used.

Within the scope of providing privacy in the blockchain, the targets of providing anonymity and untraceability, hiding contents in transactions, and hiding status data are tried to be met at different levels. Given the nature

of blockchain, the difficulty in meeting privacy targets is understandable, considering that data is copied and processed on all nodes.

In addition to these basic components, when it is aimed to add privacy capabilities, the number of building blocks that can be used and combinations of usage increase. Zero Knowledge(*) Proofs (SNARKS, Bulletproof, etc.), commitments, accumulators, symmetric cryptography and homomorphic cryptography technologies are used to ensure that transactions (comparison, validation, addition, subtraction, etc.) are performed with hidden states of the data instead of itself. Special signing technologies (Ring-signature and derivatives, Multi-signature, Blind Signature, etc.) are used for privacy enhancing purposes such as hiding the identities of the initiators of a transaction and hiding the signed data etc. Threshold Signature or Threshold Cryptography technology is used to allow multiple people to initiate transactions. While building blocks for the security of a blockchain (verification of integrity and origin of transactions) are pre-defined as on-chain, we may also encounter off-chain components among the ones with privacy purpose.

In permissioned blockchains, the registration of users to the system and the authentication of transactions are performed by components called Membership Service. In general, PKI technologies are used, and certificates are issued to authorized users/nodes. IDEMIX technology used in the Hyperledger platform can be given as an example for this type of services.

Commonly used hardware components in this class are HSM (Hardware Security Module) and SGX (Software Guard Extensions) modules. SGX is especially on blockchain nodes in cases where the codes that process sensitive data must be run in a protected environment. HSM is used on blockchain nodes in cases where sensitive data such as keys should be stored and used in order to provide security (E.g. Quorum platform). Usually, USB-based hardware modules are used as wallets.

Within the scope of Ledger and Data, the technologies related to the organization and processing of data in blockchain are addressed.

Smart Contract is a component that is used for processing data within blockchain. What allows smart contracts to be available in the blockchain is the technology called Virtual Machine.

As explained in previous chapters, the data are stored both in and out of the blockchain. Two types of data are stored in blockchain. One of them is transactions, and the other is the state information governed by transactions. In addition to the blockchain systems that work with data where the data spread inside transactions are used (UTXO Model), there are systems operating based on state data that are updated cumulatively with transactions (Account Model). The Key-Value database, a NoSQL database type, is the most widely used technology for storing state data in a smart contract (on-chain).

(*) ZKP -- Zero Knowledge Proof

In blockchain, there are tokens that are modeled at a higher level and stored in the smart contract, in addition to the native tokens that miners generate and/or that are paid for transaction fees. Technologies that can be used for these high-end tokens are being developed as well. ERC-20 and ERC-721 type tokens working on Ethereum blockchain are the most widely used standards in this field. While the codes describe how a token works, the databases are basically tables of rows and columns that track who has how many tokens.

Sharding, sidechain, state channel and channel technologies are available in terms of the technologies ensuring the Ledger scalability. Sharding is a traditional database scaling technology that breaks down the database and places each part on a different server.

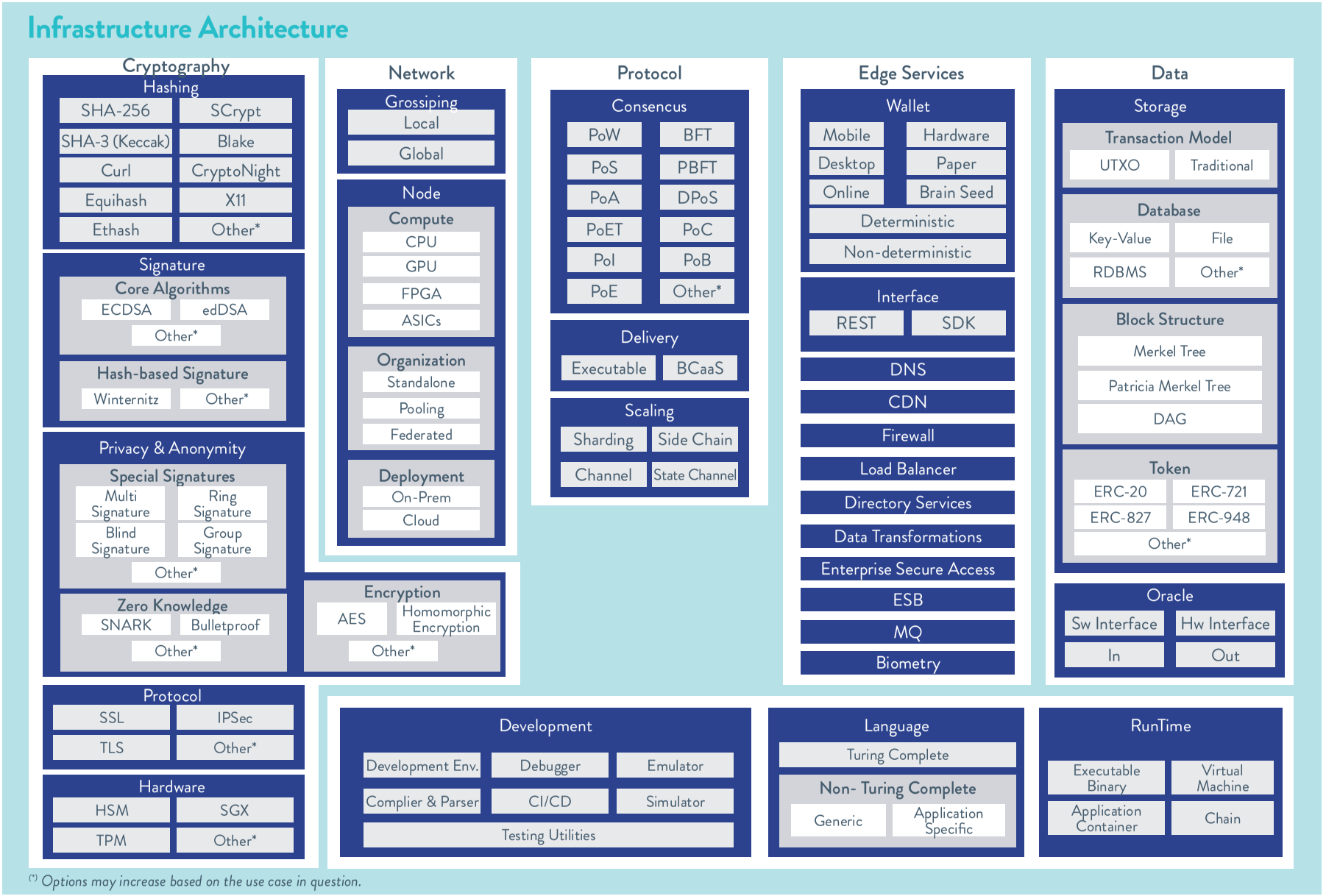
Its purpose is to eliminate the need for a “full node”, which stores the exact state of the network and every transaction that takes place. Instead, each node stores a subset of this data and validates only these operations. If a node needs to receive information regarding processes or blocks that it does not store, it finds another node possessing the information it needs. It can be applied to blockchain systems using PoS consensus. Sidechain is a scalability enhancement technology based on allowing digital assets to pass between blockchains. The concept of Channel refers to the generation of virtual sub-blockchains on the same blockchain platform. With channel memberships, both the access control and the processes in the same blockchain environment on different data sets are ensured. State channel scalability technology is a term that can be confused with the concept of channel or the concept of sidechain.

State channel refers to scalability, low cost, high speed, privacy and other blockchain integration goals, and carrying out some of the transactions off-chain and reflecting their results to the blockchain. Lightning Network for Bitcoin and SpankChain for Ethereum etc. samples are used.

Blockchain systems use Oracle technologies to exchange data with the external components out of the blockchain. Their task is to locate and verify the real-world data (currency exchange rate, weather forecast, a match result, flight information etc.) and to send them into blockchain in order to use them in smart contracts. These components might have been implemented as software and hardware oracles based on the interface connecting to the real world. Software components mostly use the data provided on the Internet environment and by APIs. Hardware oracle components can allow receiving physical data such as from RFID sensors or barcode readers etc. While Oracle components are generally used to provide external world data into blockchain (inbound oracle), they can also be used to provide data (outbound oracle) to the outside world based on the regarding status within the blockchain.

(For example, triggering to open a lock in physical world when there is a certain amount of money accumulated in the person’s blockchain account.)

Edge technologies refer to both the services and the components allowing the blockchain to interact with external components and stakeholders. The concept of a wallet as a client software is the components that host user identity and blockchain access information, and some of which may also interact with blockchain. They might be implemented by different technologies: Online, Mobile, Desktop, Hardware and Paper wallets. Wallet technologies are classified in Hot and Cold Wallet types based on their usage. The classification of deterministic and non-deterministic wallet types is based on whether the generation of private keys of the wallet is independent or not. In order to interact with blockchain, various APIs are used based on the type of the blockchain. The most common type is Rest API. The JSON format used in blockchain and these API services are of building block technologies. The Edge services layer also includes component technologies such as firewall, directory service, and various proxy services. Message queues, ESB, microservice, etc. technologies are used for the integration of applications on this layer. Application Technologies can be divided into classes related to the development, testing and execution of applications for blockchain. Smart contract and edge applications developed using various languages and IDEs such as Java, Phyton, JavaScript, Go and Solidity are validated using testnets or blockchain simulators/emulators. Virtual Machine components on a blockchain node are used to run Smart Contracts.



(*) *Options may increase based on the use case in question.*

Figure 6 **Infrastructural Architecture Domain**

CONTRIBUTORS

Enes Türk

Bankalararası Kart Merkezi A.Ş.

Aydın Akyol

Garanti Bankası

İbrahim Kara

Softtech

Taner Dursun

Fatih Birinci

Tübitak Bilgem

REFERENCES

1. Tasca, Paolo & Thanabalasingham, Thayabaran. (2017). Ontology of Blockchain Technologies. Principles of Identification and Classification. SSRN Electronic Journal. 10.2139/ssrn.2977811.
2. C. Ballandies, Mark & Dapp, Marcus & Pournaras, Evangelos. (2018). Decrypting Distributed Ledger Design - Taxonomy, Classification and Blockchain Community Evaluation.
3. Dylan J. Yaga, Peter M. Mell, Nik Roby, Karen Scarfone (2018). Blockchain Technology Overview. NIST Interagency/Internal Report (NISTIR) – 8202.
4. Andreas Ellervee, Raimundas Matulevicius, Nicolas Mayer (2017). A Comprehensive Reference Model for Blockchain-based Distributed Ledger Technology. ER Forum/Demos: 306-319.
5. Xu, Xiwei & Weber, Ingo & Staples, Mark & Zhu, Liming & Bosch, Jan & Bass, Len & Pautasso, Cesare & Rimba, Paul. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. 10.1109/ICSA.2017.33.
6. Enterprise Ethereum Alliance - Enterprise Ethereum Client Specification V2 (2018). https://entethalliance.org/technical-documents.
7. Architecture reference (2019). https://hyperledger-fabric.readthedocs.io/en/release-1.4/architecture.html
8. IBM Blockchain developer portal: https://developer.ibm.com/tutorials/category/blockchain/
9. Business Innovation Through Blockchain - The B3 Perspective - Vincenzo Morabito (2017)
10. Fat Protocols – Joel Monegro (2016): https://www.usv.com/blog/fat-protocols

BLOCKCHAIN

TÜRKİYE

TBV

TÜRKİYE BİLİŞİM VAKFI