



Research Article

Enterprise Architecture of the Blockchain Platform

Anna KACZMARCZYK¹ and Monika SITARSKA-BUBA²

¹IBM Global Services Delivery Centre Polska, Wroclaw, Poland

²Wroclaw University of Economics and Business, Wroclaw, Poland

Correspondence should be addressed to: Monika SITARSKA-BUBA; monika.sitarska-buba@ue.wroc.pl

Received date: 6 April 2020; Accepted date: 23 July 2020; Published date: 22 September 2020

Academic Editor: Dariusz Wawrzyniak

Copyright © 2020. Anna KACZMARCZYK and Monika SITARSKA-BUBA. Distributed under Creative Commons Attribution 4.0 International CC-BY 4.0

The project is financed by the Ministry of Science and Higher Education in Poland under the programme "Regional Initiative of Excellence" 2019 – 2022, project number 015/RID/2018/19, total funding amount 10 721 040,00 PLN.

Abstract

The main purpose of the paper is to discuss the nature of the enterprise architecture of the blockchain platform (EAoBP). The authors also highlighted how the main technology challenges for enterprises are addressed through the proposed solution. The paper consists of the introduction and 3 chapters. Chapter 2 presents related works about the blockchain technology and defines the platform concept. The architecture layers which are required to build the enterprise blockchain platforms are described in the 3rd chapter. The 4th chapter constitutes the implementation aspects of the EAoBP. The permissioned blockchain systems leverage a cross-organizational collaboration model, what constitutes cooperation within the network without 3rd party authorities. The open source character of the implementation technology and the clear guidance of the scope of each layer clarified in the article should help businesses in applying the concept.

Keywords: Blockchain, enterprise architecture of the blockchain platform (EAoBP), Distributed Ledger Technology (DLT), platform, Hyperledger Fabric, architecture layers

Introduction

The blockchain concept constitutes new opportunities for enterprises and enterprise networks nowadays. The first

blockchain network created by Satoshi Nakomoto in 2008 is dedicated and limited to manage transactions behind the BITCOIN cryptocurrency. The open character of the

network and the anonymous character of the peers made the business usability of the

blockchain technology questionable. Despite the business weaknesses, the concept was so promising that many of the authorities concluded it as disruptive for business models and processes nowadays, (Risius, 2017 and Beck, et al. 2017). Huge commercial potential industries like Amazon, IBM, Microsoft Azure, Hewlett Packard, Oracle and SAP started working on the new technology (Onik, et al. 2019). In a short time, the blockchain has been generalized to the distributed ledger systems that process all types of transactions within the network far beyond cryptocurrencies (Swan, 2015, Sitarska-Buba, 2018, Wörner, et al. 2016 and Hofmann, 2018).

Blockchain is not a completely new technology, it is rather just a new mechanism utilising existing multifaceted technologies together – such as distributed ledger technology (DLT), mathematical hashing, distributed networks, asymmetric encryption techniques, digital signatures and programming (Onik, et al. 2019 and Badr, et al. 2018). The Blockchain technology brings the possibility to embed a cross-organizational collaboration model, (joining entities that already cooperate into chains, and eliminating redundancy of transactions storage through a common distributed ledger (Norta, 2016).

The goal of the article is to present the enterprise architecture of the blockchain platform and highlight how main technology challenges for enterprises are addressed through the proposed solution. Chapter 2 presents related works about the blockchain technology and defines the platform concept. The architecture layers which are required to build the enterprise blockchain platforms are described in the 3rd chapter. The 4th chapter describes the implementation aspects of the EAoBP.

Blockchain Technology and Platform Concept

The first generation of blockchains, which were public (permissionless), consists of

distributed nodes working together in a peer-to-peer model (e.g. Bitcoin, Ethereum). Anyone can join and leave the public blockchain ecosystem at any time, enjoying the full access to read and write (Onik, et al. 2019). Blockchain systems operate under the governance model to build trust between participants on a shared network. (Wu, 2019). Each participant's (node) has equal rights in approving the transaction. The transaction is an elementary component of the Blockchain system. This model rejects the creation of a central authority needed to approve the transaction. The authentication is processing within the network by each node. The transaction is asymmetrically encrypted and marked with a one-way hash function, which is collision-resistant and irreversible (the transaction cannot be played back, knowing only its shortcut).

The new transaction is transmitted into the blockchain network, which means that each node receives information about adding a new entry at the same time, in order to either confirm or reject it. The decision to add a new block should be made autonomously by each of the nodes based on the accepted consensus mechanism (e.g. Proof of Work (PoW), Practical Byzantine Fault Tolerance (PBFT)). If a consensus is reached, the new block is added to the current system. A newly added block will store the hash of the previous block, which allows to keep the data structure in the system.

The introduction of smart contracts starts the second generation of blockchain systems (Blockchain 2.0). Smart contracts were introduced as semi-autonomous programs running on the blockchain. (Omohundro, 2014). The consensus is implemented in the form of smart contracts, which are programmable rules/codes allowing transactions to result from the execution of user-defined programs (Rimba, et al. 2018). Moreover, smart contracts are responsible for ensuring that all new transactions are compliant with the agreed consensus. (Tschorsch, et al. 2016). It even allows parties who do not fully trust each other to conduct and reliably control mutual transactions without relying on the services

of any trusted middle men (Rimba, et al. 2018). Smart contracts cover the agreed consensus within the network business rules and business agreements, and are used to build trust within the network.

Only the smart contracts implementation enabled the embedding of cross-organization collaboration models that were executed through private (permissioned) and federated (hybrid/consortium) blockchains. In the private blockchain, the access is restricted, and read and write access are controlled based on the roles of the nodes or other restrictions as defined by the protocol (Onik, et al. 2019). The Federated blockchain is moderated according to the consortium need, the access can be restricted, or reading/writing rights will be limited and defined as prioris. The flexibility proposed by the federated blockchains create the optimal environment to build cross-organization collaboration models, addressing real business needs.

The synergy effect of usage in well known technologies like DLT, mathematical hashing, distributed networks, asymmetric encryption techniques, digital signatures and programming makes it possible to create a new generation of IT systems characterized by features like **immutability** (resistance towards the modification of data) and **non-repudiation**. Systems are also **forgery resistant**; certain researchers believe that even quantum computers are not able to change transactions (process the fraud) within a distributed network (Singhal, 2018). Public blockchain systems are fully **democratic**, which allows to create a Regulator role or build internal channels to limit the transaction exchange within (HF01 2020). The way a data structure is defined and data are stored, blockchain systems are **double-spent resistant**. Another very important feature of the blockchain technology is the **consistent state of the ledger which is** achieved through implementing the proper consensus mechanism (Singhal, 2018). If the ledger is consistent and immutable, the whole system is **auditable**, because all transactions (past and current) are stored. The peer-to-peer processing makes

blockchain systems resilient. Even if a single node is lost, the security and consistency will not be threatened because the same ledger copy is stored by all other nodes.

On top of the above described features, the blockchain technology enables **digital tokens** to be distributed around the network participants. In the Blockchain world, tokens have emerged as the artefact of choice to represent assets, a utility or a claim on something inherent to a specific blockchain project. Tokens exist due to their usefulness of representing something digitally (Pilkington, 2015 and Oliveira, et al. 2018). Researchers identify three main types of tokens: **cryptocurrency**, **utility tokens** (used as an internal payment method, a reward for reaching a consensus, a workload performance reward, a voting right confirmation or as a digital asset) and **tokenised security** (equity or funding tokens). The equity token grants its holder equity-related earnings, such as profit-sharing, application rents or platform fees, and the funding tokens are defined in the initial coin offerings (ICOs) process to represent a long-term investment from the holder's perspective and a financing vehicle for the project's team (Oliveira, et al. 2018). Cryptocurrency and utility tokens are mostly used in permissionless blockchains, where the lack of trust nudges them towards the platform's distributed consensus (Lewis, 2015). In opposition to that, the permissioned blockchain lacks the need to issue tokens out of a mere choice or pure funding aspirations (Blockchain Hub, 2017, and Lewis, 2015). Before the implementation of any tokens within commercial (permissioned) blockchain systems, their usage and business values should be discussed first.

There are several limits identified for the blockchain technology that have to be addressed during the business implementation. According to the authors, the most critical limits are the transaction throughput and the transaction latency. For the bitcoin, the average **transaction throughput** (number of transactions processed per second) is between 3.3 and 4.8 TPS (Blockchain, 2020, Croman, et al. 2016 and @wandererli, 2019). Compared to

the payment systems, like Visa, where there is around 2000 TPS rate, as Croman, et al. (2016) mentioned, it is clear that the bitcoin will not replace the payment transaction systems. **Transaction latency** can be understood as the time needed to add a new transaction within the system. The latency time is dependent on the consensus mechanism implemented in the network. In the Bitcoin chain, where the PoW consensus is implemented, 10 minutes are needed to add a new block to the system. Blocks are relatively small, around 1MB (@wandererli, 2019). So, huge latency is not acceptable in transaction systems, which means that the scalability of the system is questionable according to the business usage.

Technology itself will not help developers build blockchain based systems. Scientists emphasize that the industry should also provide a **platform**, that is considered as the development framework to create multiple applications (Pillai, et al. 2017). Developers should be able to write their own application codes using specific components of the platform. Not only technical challenges like security, performance, data integrity, privacy and scalability should be addressed (Yli-Huumo, et al. 2016), but also quality aspects should be taken into consideration like usability for developers and suitability for the integration within the network (Pillai, et al., 2017).

Enterprise architecture of the blockchain platform (EAoBP)

This section proposes the enterprise architecture of the blockchain platform in details, presenting all the required layers.

The limits of the blockchain systems, described in the previous chapter, made the pure architecture not implementable in the enterprise environment. Based on the research, the following requirements need to be considered for the enterprise implementation of a Blockchain network:

Participants must be identified/identifiable – the enterprise usage of the Blockchain platform requires the participants to be fully identifiable to

keep the transaction trustworthy without a 3rd party authorisation.

Networks need to be permissioned – in the business reality, the network is not open for everyone. It is limited to the identified participants who were invited to be part of it. The permission mechanism should be easily implementable.

High transaction throughput performance - one of the weaknesses of the public networks is the transaction execution time, which can take up to 10 minutes to process a single transaction (@wandererli, 2019). There must be a condition to implement the acceptable transaction execution time.

Low latency of transaction confirmation – each transaction should be confirmed within the blockchain network as soon as possible. Delays or too high latency lead to low efficiency of the network and loss of trust by participants.

Privacy and confidentiality of transactions and data pertaining to business transactions– enterprise networks will not share their data worldwide, they will require their data to be kept private and confidential within and outside the network (as mentioned in IBM 2020, Forrester 2018 and HF02 2020).

The authors defined the enterprise architecture of the Blockchain platform that meets the business requirements and trays to address the constrains and limits of the public blockchain network (Fig. 1).

They proposed the Blockchain 2.0 system architecture, which consists of five layers. Each layer plays a different role and is responsible for the execution of a specific functionality that determines Blockchain 2.0 as a whole (Singhal, 2018). The authors agree that the application, execution, semantic, propagation and consensus layers are critical to build a blockchain platform.

The **application layer** is responsible for the communication with the end-users, providing them with specific business

functions and IT services, and allowing them to process transactions in accordance with the defined business rules. Due to the peer-to-peer processing model, the recommended development/programming frameworks are those which allow to create applications hosted on the web servers, where new features are developed at the server level and the communication with users is managed through API. Moreover, applications should support a proper identity management and a workflow management.

The **execution layer** is responsible for executing the instructions that are called by the application layer. The same set of instructions must be executed by each node independently to claim a new transaction. Through instructions, single scripts, algorithms or programs such as smart contracts are understood. The deterministic execution of a specific instruction on the same input dataset and under the same restrictive conditions always provides the same output dataset for all nodes. These features of the blockchain technology ensure data consistency, **immutability** and **trust** within the distributed ledger.

The **semantic layer** defines the logical structure of the blockchain system. Each transaction, correct or not, is processed at the execution layer. The semantic layer is responsible for the validation, and consequently, the approval or rejection of the transaction in the system. The semantic layer constitutes the definition of transaction's validation rules, data models and data structure. In general, the blockchain structure is a timestamped list of blocks, where blocks are connected through a hash function (Wörner, et al., 2016). It means that data are hash pointers that encrypt transactions of a given block. Each block stores its hash function and remembers the hash function of its predecessor up to the generic block (Drescher, 2017). At the semantic layer, system developers implement smart contracts, which are autonomous algorithms or mini-programs performing additional operations written in their codes during the transaction execution (Klinger, et al., 2017). The extensive use of smart

contracts allows for the creation of new virtual goods that constitute a business value in a specific Blockchain system.

The **propagation layer** is responsible for the definition of communication and synchronization within the blockchain platform. The blockchain network is a peer-to-peer network, where each node is autonomous and there is no central authority approving the transactions. For the public chain, it is necessary to ensure the visibility of all nodes in the chain as well as the rules for adding new nodes so that they become equivalent members in the network. The next step is to manage the synchronization process between nodes. In Bitcoin blockchain, when the new block is generated, it is immediately validated within the entire network. If this block passes the correct validation, it is synchronized throughout the network. Transaction throughput and latency are the most critical weaknesses of the public chain that make a business value of the whole solution questionable.

For example, this issue has been addressed in Hyperledger Fabric by dividing the workload of the nodes between endorsing and committing peers and transaction ordering nodes, which will be further discussed in chapter 4 (HP01 2020).

Another positive deviation in private chains is the possibility to create a role of a central authority (regulator), whose approval will confirm the creation of a new transaction in the network. There are business models, especially in the government area where a regulator is needed but all other blockchain features can be used to create an added value for the network participants.

The **consensus layer** is the most important and basic layer to meet the general assumption of the blockchain technology. This layer defines the consensus on the basis of which transactions or blocks within the entire network are approved. The basic goal of each blockchain network is to achieve a consistent state of the ledger. Each blockchain system may implement and execute a different consensus algorithm, but for the assumption, the result is to validate

one common version of the registry within the network without the participation of the central authority. The security, trust and immutability of a given network is determined by the effectiveness of the consensus algorithm.

For the commercial usage of blockchain systems that often requires the

implementation of shared business processes, additional aspects affecting the architecture must be considered. The authors propose to extend the traditional list of layers through permission, data privacy and integration layers. The enterprise architecture of the Blockchain platform is presented in figure 1.

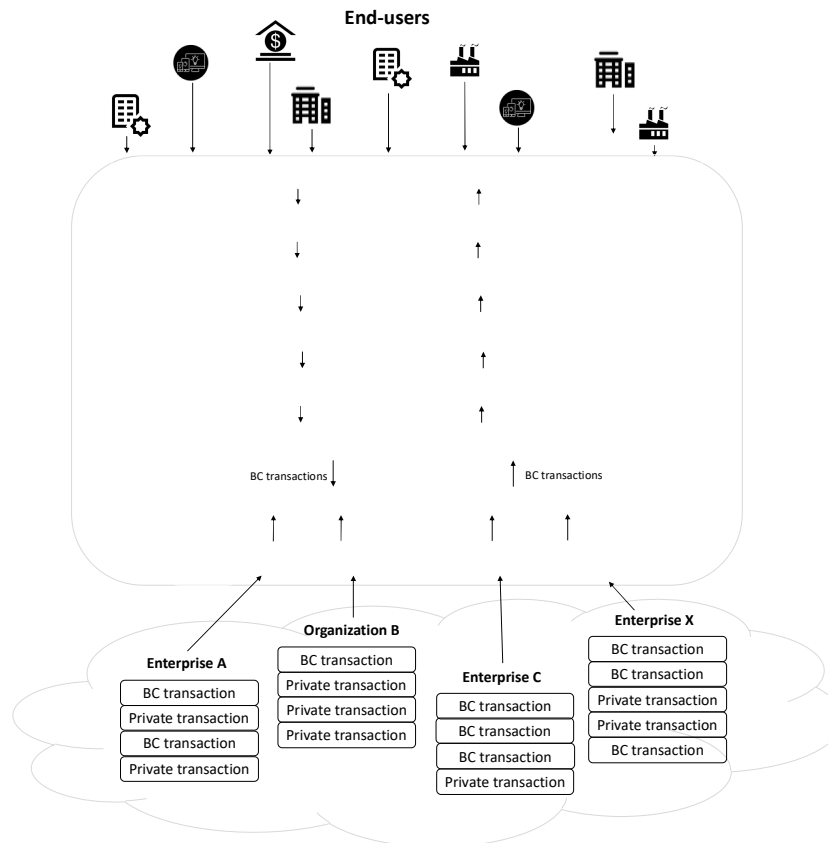


Fig. 1: Enterprise architecture of the Blockchain platform (EAoBP)

Source: own research, based on (Sitarska-Buba 2018)

EAoBP will be mostly dedicated to participants of the business networks that already cooperate. They have a need to create a distributed transaction ledger and share their business results within the network. To meet this request, the authors defined a **permission layer** that is responsible for the definition of the access rules for network participants. The business entity will be allowed to access the blockchain network only when other participants agree or based on invitations

only. The way the permission layer will be automated is up to the business agreements between the current participants. There are examples of the Blockchain implementation where the networks are fully private, as in the following polish cases: Durable Medium, KIR and e-Voting, KDPW. Those examples, further described in the next chapter, confirmed the need for a permission layer definition. The implementation of the permission layer can be executed in traditional contracts signed between

individual companies or implemented in a blockchain code.

The permission layer has also been highlighted at the end-user level. It is the natural consequence of the closed access for nodes that is further distributed to application users. If the blockchain platform is private, the access for the users is private as well. The access could be granted based on the invitation that has to be confirmed by the authority within the chain or by the network itself. In the second case, the invitation code could use a consensus mechanism that is already implemented and manage each access as a specific type of the transaction.

Going deeper into the blockchain platform layers, the authors identified the **data privacy layer** that provides participants with the possibility to identify and limit transactions that will be processed within the blockchain system (on-chain and off-chain distribution) (Xiwei, et al., 2016 and Xiwei, et al., 2017). This requirement is not only related to the data privacy regulation defined by the European Union (GDPR). This layer was created to ensure the flexibility for participants to define an access level for a specific type of transactions exchange between nodes. For example, Hyperledger Fabric v.2.0 provides a private data collection mechanism which allows to exchange specific data only between a priorly defined nodes. Peer-to-peer data distribution is still used but nodes send transactions only to the organization that is authorized to see them (HF01 2020).

Enterprises that decided to create blockchain platforms usually build them above other IT systems and platforms that already exist in their organizations. Different backend systems, frontend platforms and data hosting environments have contributed to define the **integration layer**. This layer is responsible for working out a common technology platform where nodes will be hosted and maintained. Within this layer, the nodes will create the integration code responsible for the transaction extracted from the internal IT systems, translate them into a blockchain

transaction and distribute them around the network based on the data privacy protocol.

Implementation of the EAoBP based on the IBM Blockchain platform

The authors decided to present the implementation example of the EAoBP based on the IBM Blockchain platform and Hyperledger Fabric v2.0, which is an open source blockchain framework designed for business.

The main reason for this choice was that the Research Everest Group assessed IBM Blockchain Services as a Leader in a field of 30 service providers in the Blockchain Services (PEAK Matrix Assessment 2020). Everest specifically noted IBM's strength in the integrated services and solutions, the global delivery footprint and the vast network of partners across different industries, and the ability to consortia cooperation and governance (Doshi, et al., 2019).

IBM Blockchain platform is integrated with the Hyperledger Fabric framework. The Hyperledger or the Hyperledger project that started in December 2015 is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by the Linux Foundation, including leaders in finance, banking, Internet of Things, supply chains, manufacturing and Technology. The Hyperledger Fabric was the first of the Hyperledger projects. The cooperation between IBM and Linux Foundation was so efficient because Hyperledger Fabric enterprise-grade permissioned a distributed ledger technology (DLT) platform, designed for use in enterprise contexts (HF02 2020). **The permission layer** is an integrated part of the solution, where all participants are well known and authorized to be part of the consortium. Entities that are part of the network with common business goal, cannot trust each other, therefore consensus mechanisms like crash fault tolerant (CFT) or byzantine fault tolerant (BFT) are provided.

RAFT is a crash fault tolerant (CFT) ordering service based on an implementation of Raft

protocol. Raft follows a “leader and follower” model, where a leader node is elected (per channel) and its decisions are replicated by the followers (HF03 2020). RAFT consensus is highly recommended by Hyperledger Fabric these days.

The Data Privacy layer is provided by Hyperledger Fabric through a channel architecture and a private data feature mentioned in the previous chapter. Using the channels, participants of the network can establish a sub-network (private data collection) where members can see a selected set of transactions. The private data collection allows data exchange between selected members of a channel, providing the same protection as channels without the need of creating and maintaining a separate channel (HF02 2020).

Consensus, semantic, propagation and execution layers are constituted by a smart contract’s implementation and an execute-order-validate approach. Chaincodes (smart contracts) are processed according to a new sequence (HF02 2020):

Execute a transaction and check its correctness, thereby endorse it,
Order transactions via a consensus protocol, and
Validate transactions against an application-specific endorsement policy before committing them to the ledger.

The predefined endorsement policy specifies how many nodes are needed to meet the consensus or how many are needed to vouch for the correct execution of a given smart contract. The endorsement policy is defined for each specific blockchain network, which means that the channel architecture, channel leader election rules and the regulator role are established separately. This rule brings us to the position that each transaction needs to be executed (endorsed) only by the subset of the peer nodes necessary to satisfy the transaction’s endorsement policy. This allows for a parallel execution, increasing the overall performance and scale of the system (HF02 2020).

A significantly processing transaction increases the overall performance of the platform. Based on the newest results published by (Gorenflo, et al., 2019), the platform is able to support up to 20000 transactions per second (TPS).

The Hyperledger Fabric is ready to use a development framework that provides implementable modules for each blockchain solution like:

Ordering service establishes a consensus on the order of transactions and then broadcasts blocks to peers,

Membership service provider is responsible for associating entities in the network with cryptographic identities,

An optional peer-to-peer **gossip service** disseminates the blocks output by ordering the service to other peers,

Smart contracts (“chaincodes”) run within a container environment (e.g. Docker) for isolation,

The ledger can be configured to support a variety of DBMSs,

Endorsement and validation policy enforcement that can be independently configured per application (HF02 2020),

This is the perfect example of the EAoBP application layer.

Creating a new blockchain solution by IBM, provides an integration layer that helps to integrate data transformation and business services within cloud, on-prem or hybrid environments.

To create an effective blockchain solution for a business, there are at least three must have conditions defined by IBM. First of all, the group of enterprises should have a **real business problem** that can be addressed only through a blockchain based system. The Blockchain ecosystem requires building a network of organizations that are interested in resolving this business problem. The last condition is a need of trust that has to be created by the blockchain system. Taking the above conditions into consideration, IBM successfully implement the blockchain solution in different business areas proving the efficiency and the future necessity of the technology.

Food Trust is one of the most successful blockchain projects from IBM. It is a food supply chain based on the blockchain technology. It was designed as a private, permissioned blockchain network for monitoring food supply from farms to consumer baskets. As early as 2016, Big Blue and Walmart began testing the blockchain technology to reduce the time of tracking goods. A proof of the concept was done by the Tsinghua University of Beijing focusing on China's massive pork market, it was found that the tracking time reduced from days to minutes. The result is a customizable suite of solutions that can optimize the process of distribution, monitor food safety and freshness, minimize waste or health risks, trace exact proveniences of the food and securely store the required certifications. Walmart issued a mandate to all its suppliers of leafy greens stating that they had to get on to the blockchain by the end of September 2019 as a deadline. The Food Trust application is also a source of crucial information for consumers themselves who can finally learn about their food from a secure source which is the blockchain based immutable record. Other leaders and competitors in the food sector are currently joining the solution and testing the application for their needs. The system is also very attractive for restaurants and all other food service providers who care about the credible information on their food.

KIR, the infrastructure institution of the Polish banking sector, and IBM created a platform prototype (Reliable Documents Sharing) for a durable medium deliberately based on a generally available open source blockchain technology solution (KIR 2020). KIR chose the Hyperledger Fabric 1.1 framework from the Linux Foundation as the basis for its platform, and an electronic stamp tool that developed itself (IBM2, 2020). The prototype durable data carrier has been designed to help banks adapt their internal systems to the requirements of the EU Directive 2007/64 / EC on payment services in the internal market in the field of customer communication, by digitizing the publication, approval and search processes. KIR has built a prototype platform for the

entire banking sector in Poland, whose task is to provide an online service aimed at verifying the existence and originality of both public and private documents, published by banks for users.

KIR's durable medium blockchain solution acts as a secure database for banks and their customers that is not controlled by any single party. The platform provides a proof-of-existence service that enables users to register and verify documents through timestamped operations stored on a distributed ledger (IBM2, 2020). This ensures that every exchange of information receives an electronic timestamp and a unique cryptographic signature, which means that any subsequent changes to the information entered are immediately visible to the relevant users of the blockchain. This means that the entire lifecycle of documents issued and exchanged by banks and their clients can be traced and audited by all the parties with access to the blockchain platform (IBM2, 2020). The above mentioned features indicate that all the blockchain technology assumptions have been met by that implementation.

The Central Bank of the Republic of Azerbaijan and IBM developed a **Digital Identification System** based on Hyperledger Fabric to verify the reliability of the documents related to both the individuals and legal entities for use with banks, credit providers and similar organizations. The system will simplify and automate the "Know Your Customer" validation process and will be used by both clients and credit organizations in serving citizens of Azerbaijan.

IBM designed for KDPW an **eVoting** platform for the Capital Market in the National Depository for Securities in Poland. It supports general meetings of public companies, including voting using digital devices. The eVoting application is integrated with the KDPW application used for providing issuers with lists of persons entitled to participate in general meetings (KDPW 2020).

Conclusion

The main idea of this paper is the enterprise architecture of the blockchain platform. The authors identified 8 layers that define the architecture, highlighting that permission, data privacy and integration layers are required in the business implementation of blockchain solutions. Those layers constitute the permissioned blockchain platform that is implementable at the execution level.

The applicability of the platform was verified based on the IBM Blockchain platform and Hyperledger Fabric. A new approach of transaction processing (execute-order-validate) available in the current Hyperledger Fabric code significantly increases the solution scalability up to 20.000 TPS. The achieved result establishes the position of blockchain systems within the enterprise solutions, implementing an effectively cross-organizational collaboration model.

References

- @wandererli(2019), The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed. [Online], [retrieved April 14, 2020], <https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44>
- Badr B., Wu Xun, Horrocks R., (2018), *Blockchain By Example*, Packt Publishing, ISBN: 9781788475686
- Beck R., Mueller-Bloch C. (2017), Blockchain as radical innovation: a framework for engaging with distributed ledgers. In: 50th Hawaii international conference on system sciences, Waikoloa. [Online], [retrieved March 14, 2020], <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1684&context=hicss-50>
- Blockchain 2020, Transaction Rate Per Second. [Online], [retrieved April 14, 2020], <https://www.blockchain.com/charts/transactions-per-second>
- BlockchainHub, (2017), Cryptographic Tokens. [Online], [retrieved April 30, 2020], <https://blockchainhub.net/tokens/>
- Croman K. et al. (2016) On Scaling Decentralized Blockchains. In: Clark J., Meiklejohn S., Ryan P., Wallach D., Brenner M., Rohloff K. (eds) *Financial Cryptography and Data Security*. FC 2016. Lecture Notes in Computer Science, vol 9604. Springer, Berlin, Heidelberg
- Doshi R., Kalawatia S., Menon S. (2019), Everest Group PEAK Matrix™ for Enterprise Blockchain Services 2020. [Online], [retrieved March 14, 2020], <https://www2.everestgrp.com/report-action/EGR-2019-33-R-3461/Marketing?SearchTerms=blockchain>
- Drescher D., (2017), *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Apress, ISBN: 9781484226049
- Forrester (2018), *Emerging Technology Projection: The Total Economic Impact™ Of IBM Blockchain*. [Online], [retrieved April 14, 2020], <https://www.ibm.com/downloads/cas/QJ4XA0MD>
- Gorenflo Ch., Lee S., Golab L., Keshav S., (2019), FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second, in: Conference: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). [Online], [retrieved April 14, 2020], <https://arxiv.org/pdf/1901.00910.pdf>
- HF01, Hyperledger Fabric (2020), What's new in Hyperledger Fabric v2.0?[Online], [retrieved April 14, 2020], <https://hyperledger-fabric.readthedocs.io/en/latest/private-data/private-data.html>
- HF02, Hyperledger Fabric 2020, Introduction. [Online], [retrieved April 14, 2020], <https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html>
- HF03, Hyperledger Fabric 2020, Configuring and operating a Raft ordering service. [Online], [retrieved April 14, 2020], https://hyperledger-fabric.readthedocs.io/en/release-2.0/raft_configuration.html
- Hofmann E., Strewé UM, Bosia N., (2018), *Supply chain finance and blockchain technology: the case of reverse securitisation*, Springer

- International Publishing AG, ISSN 2193-1739
- IBM (2020), IBM Institute for Business Value. [Online], [retrieved April 14, 2020], <https://www.ibm.com/thought-leadership/institute-business-value/technology/blockchain>
 - IBM2 (2020), KIR. [Online], [retrieved April 14, 2020] <https://www.ibm.com/case-studies/kir-blockchain-financial-services-payments>
 - KDPW (2020), eVoting. [Online], [retrieved April 3, 2020], <https://blockchain.kdpw.pl/>
 - KIR (2020), Durable medium. [Online], [retrieved April 14, 2020], <https://www.kir.pl/en/clients/durable-medium/>
 - Klinger B., Szczepański J., (2017), Blockchain - historia, cechy i główne obszary zastosowań. [Online], [retrieved April 14, 2020], <http://czasopisma.uksw.edu.pl/index.php/cwc/article/view/1858/1682> (accessed 03.04.2020)
 - Lewis, A., (2015), A gentle introduction to digital tokens. [Online], [retrieved April 30, 2020], <https://bitsonblocks.net/2015/09/28/a-gentle-introduction-to-digital-tokens/>
 - Norta A., (2016), Establishing Distributed Governance Infrastructures for Enacting Cross-Organization Collaborations. [Online], [retrieved April 14, 2020], <https://www.researchgate.net/publication/301641987>
 - Oliveira L.,Zavolokina L. Bauer I., Schwabe G., (2018). To Token or not to Token:Tools for Understanding Blockchain Tokens. In: International Conference of Information Systems (ICIS2018), San Francisco, USA, 12 December 2018 - 16 December 2018. [Online], [retrieved April 29, 2020], <https://doi.org/10.5167/uzh-157908>
 - Omohundro, S. (2014). Cryptocurrencies, smart contracts, and artificial intelligence. *AI Matters*, 1(2), 19–21. [Online], [retrieved April 14, 2020], <https://doi.org/10.1145/2685328.2685334>
 - Onik Md Mehedi Hassan, Miraz Mahdi H., (2019), Performance Analytical Comparison of Blockchain-as-a-Service (BaaS) Platforms, In: International Conference for Emerging Technologies in Computing, iCETiC 2019: Emerging Technologies in Computing. [Online], [retrieved April 14, 2020], https://link.springer.com/chapter/10.1007/978-3-030-23943-5_1
 - Piech K, et al. (2016), Leksykon pojęć na temat technologii Blockchain i kryptowalut. [Online], [retrieved April 14, 2020], https://www.gov.pl/documents/31305/0/leksykon_pojec_na_temat_techologii_blockchain_i_kryptowalut.pdf/77392774-1180-79ab-4dd5-089ffab37602
 - Pillai B., Muthukkumarasamy V., Biswas K., 2017, Challenges in Designing a Blockchain Platform. [Online], [retrieved April 14, 2020], https://www.researchgate.net/profile/Kamanashis-Biswas/publication/317617799_Challenges_in_Designing_a_Blockchain_Platform/links/5943ccad45851525f890a0a9/Challenges-in-Designing-a-Blockchain-Platform.pdf
 - Rimba, P., Tran, A.B., Weber, I. et al. (2018), Quantifying the Cost of Distrust: Comparing Blockchain and Cloud Services for Business Process Execution. *Inf Syst Front.* [Online], [retrieved April 14, 2020], <https://doi.org/10.1007/s10796-018-9876-1>
 - Risius M., Spohrer K. (2017), A Blockchain Research Framework, In: *Bus Inf SystEng* 59(6):385–409. [Online], [retrieved April 14, 2020], <https://doi.org/10.1007/s12599-017-0506-0>
 - Singhal B., Dhameja G., Panda P.S., (2018) Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Apress
 - Sitarska-Buba M., (2018), Architecture of the blockchain 2.0. In: *InformatykaEkonomiczna* 4 (50), ISSN 1507-3858
 - Swam M., (2015), *Blockchain*, O'Reilly Media, Inc., ISBN: 9781491920497
 - Tschorsch, F., Scheuermann, B. (2016). *Bitcoin and beyond: A, technical survey*

- on decentralized digital currencies, In: IEEE Communications Surveys & Tutorials IACR Cryptology. [Online], [retrieved April 14, 2020], <https://ieeexplore.ieee.org/abstract/document/7423672/citations#citations>
- Wörner D., Von Bomhard T., Schreier YP., BilgeriD.,(2016), The Bitcoin Ecosystem: Disruption Beyond Financial Services?, Research Papers. 33. [Online], [retrieved April 3, 2020], http://aisel.aisnet.org/ecis2016_rp/33
 - Wu Brian, (2019), Blockchain Performance and Scalability – Hyperledger Fabric. [Online], [retrieved April 14, 2020], <https://blog.bybit.com/research-and-analysis/blockchain-performance-and-scalability-hyperledger-fabric/>
 - Xiwei Xu, Pautasso C., Zhu L., Gramoli V., Ponomarev A., Chen Sh., (2016), The Blockchain as a Software Connector. [Online], [retrieved April 14, 2020], <https://ieeexplore.ieee.org/abstract/document/7516828>
 - Xiwei Xu, Weber I., Staples M, Zhu L., Bosch J, Bass L, Pautasso C., Rimba P., 2017, A Taxonomy of Blockchain-Based Systems for Architecture Design. [Online], [retrieved April 14, 2020], <https://ieeexplore.ieee.org/document/7930224>
 - Yli-Huumo J., Ko, D., Choi, S., Park, S., Smolander, K. (2016). Where Is Current Research on Blockchain Technology?. [Online], [retrieved April 14, 2020], <https://doi.org/10.1371/journal.pone.0163477> (accessed 02.04.2020).