BİGA PROJECT

TAKAS İSTANBUL

FinTechHub
TAKAS İSTANBUL

TAKAS İSTANBUL

FinTechHub TAKASİSTANBUL

PHYSICALLY-BACKED GOLD, COMPLIANT WITH REGULATIONS AND OFFERING MAXIMUM PRIVACY AND SECURITY

24h SECURE TRANSFER

Gökhan ELİBOL

Deputy General Manager Board
Member at Takasbank

We are proud to announce BiGA, the world's first physical gold-backed blockchain-based transfer system which is built by Takasbank. Today's global economic trends come with intense competition. In particular, developments seen in financial technologies gradually becomes more crucial.

Having adopted progress and development as its main objective since the very first day of its foundation, our Bank carries out its activities with a focus on contributions to the Turkish economy. What is more, our Bank has been also serving as an On-Site R&D Center within the brand FinTechHub Takas Istanbul since 2017.

The central position of Takasbank in Turkish Capital Markets and our R&D mission have triggered us to work on blockchain technologies.

Special attention is given to collaborations with start-ups and universities, giving R&D incentives to our employees. Meetings with the regulatory authorities and international organizations in order to enrich fintech ecosystem.

BiGA is a reference project that is intended to become a milestone in the adoption of blockchain technologies by financial institutions. BiGA is under international patenting process with its innovative features. Especially, BiGA is expected to have contributions on Istanbul Financial Center.
I would like to express my gratitude to the Chairman of our Executive Board, our Bank's employees and all the stakeholders of the project for their contributions and support in the BiGA Project.

TABLE OF CONTENTS

8 ABSTRACT

10 INTRODUCTION

12 ABOUT TAKASBANK

16 TAKASBANK BLOCKCHAIN VISION

19 SCOPE OF THE PROJECT

- GOLD TRANSFER SYSTEM (GTS) PROJECT
- GTS-BIGA INTEGRATION
- TRANSFER
- RECONCILIATION
- ISSUANCE
- REDEEM

26 TECHNICAL BACKGROUND OF THE PROJECT

- HYPERLEDGER
- QUORUM
- ZERO-KNOWLEDGE PROOF
- OTHER TECHNOLOGIES

30 **FUNCTIONAL DESIGN**

- BIGA WITH HYPERLEDGER PLATFORM
- BIGA WITH QUORUM PLATFORM

36 **BİGA PROJECT TEST RESULTS**

- TEST SCENARIOS
- TEST RESULTS
- BIGA FUNCTIONS TEST RESULTS

40 **TECHNICAL OUTPUTS**

- OPERATING PRINCIPLES OF DISTRIBUTED SYSTEMS
- DIFFERENT BLOCKCHAIN INFRASTRUCTURES
- CONSENSUS ALGORITHMS
- CRYPTOGRAPHIC ALGORITHMS
- BLOCKCHAIN ACCOUNT STRUCTURES
- PRE-COMPILED CONTRACTS:

44 **BUSINESS OUTPUTS**

- ASSET TRANSFER
- BUSINESS CONTINUITY
- PAYMENT SYSTEM INFRASTRUCTURE

46 LESSONS LEARNED AND RECOMMENDATIONS

48 FUTURE PLANS

- CHANGING THE ZERO-KNOWLEDGE PROOF ALGORITHM
- REMOVAL OF THE QUORUM MAKER DEPENDENCY
- CHANGING THE CONSENSUS ALGORITHM
- SECRET KEY RECOVERY SCENARIOS
- CONCEALMENT OF THE PARTIES INVOLVED IN TRANSFER
- UPDATEABLE SMART CONTRACT
- DEVELOPMENT WITH HYPERLEDGER FABRIC PLATFORM
- KNOW YOUR CUSTOMER STUDIES
- WALLET APPLICATION FOR PERSONAL USE
- EVALUATION OF SOME EXTREME SCENARIOS

52 CONCLUSION

53 PROJECT TEAM

54 THANKS

55 ABBREVIATIONS / TERMS OF GLOSSARY

58 APPENDICES

65 REFERENCES

ABSTRACT

Popularity of blockchain technology has been growing among financial institutions recently, particularly those with central positions, which led many foremost institutions to explore possible applications of this brand new technology. Having knowledge and experience on blockchain technology is one of the strategic goals of Takasbank since it is discovered that it may have a disruptive effect on financial sector. With this strategy, Takasbank R&D Center closely studies blockchain technology for more than three years. Existing studies indicate that the blockchain technologies are not yet mature enough to be used in the financial sector.

It is clear that further development is needed to adopt this technology in the financial sector in addition to existing technologies and that such activities can be made within Takasbank. A special attention must be given to the functions such as usage of decentralized ledger technologies and digitalization of physically-backed assets, which are in line with the regulations and privacy expectations of transaction owners, and through which transactions can be monitored by authorities. The idea to develop a platform using the blockchain technology was born in 2017 within Takasbank. In the mentioned study, a platform allowing for transfer of physically-backed digital gold between the parties through the blockchain technology is established. Not only the distributed ledger technology is used, but also the privacy of transactions is protected.

Transactions with full privacy, having backed by physical assets, without independent value and the capability of execution in line with regulations are the features differentiating this project from many other projects announced across the world. In this study, developments are made with two distinct blockchain infrastructures outstanding with different technical capabilities.

As a result, a multi-party testing process is initiated with five Banks. Tests are conducted with Albaraka Türk Participation Bank, Garanti BBVA, Kuveyt Türk Participation Bank, Vakıfbank and Ziraat Bank. The functionality of BiGA was observed to have 100% success rate.

This document is prepared to give information about the development process of the BiGA Project.

The offered BiGA Digital Gold is ensured to have equivalence to one gram gold which can be transferred among stakeholders in a controlled and privacy-focused manner. The proper functioning and competence of the technology are tested and technological uncertainties are observed. Moreover, it is aimed to pioneer the other studies and efforts in the financial sector. The document provides information on both the technical infrastructure and the business model of the project.

INTRODUCTION

The BiGA Project is initiated by Takasbank Blockchain Work Group within Takasbank. As of then, the developments within the blockchain technologies are followed up and the projects that could be implemented under Takasbank are evaluated.

On the other hand, Takasbank achieved its On-Site R&D Center status in 2017. With the R&D vision, blockchain studies are carried on with project design. Takasbank has efforts on these studies from executive level. This includes hosting blockchain-related organizations and ensuring active participation in blockchain focused events. Takasbank has made contributions to blockchain technologies in the financial ecosystem through various meetings and exchange of information with the start-ups in the blockchain ecosystem developing in Turkey.

The idea that Gold Transfer System Project (GTS), whose technical infrastructure is developed with traditional methods, can be developed by using blockchain technology while it was still in the design stage had emerged. Therefore, the efforts for BiGA Project that can be considered as the blockchain version of the Gold Transfer System are initiated. In this paper, we present details of the first phase of BiGA.

BiGA

One Gram Gold

BiGA
1 GRAM ALTIN KARŞILIĞI ŞİFRELİ DİJİTAL VARLIK
ENCRYPTED DIGITAL ASSET EQUIVALENT TO 1 GRAM GOLD
İSTANBUL CLEARING SETTLEMENT AND CUSTODY BANK INC.
İSTANBUL TAKAS VE SAKLAMA BANKASI A.Ş.
1GRAM
GOLD

TAKAS İSTANBUL

FinTechHub
TAKASİSTANBUL

ABOUT TAKASBANK

Having a strategic importance in respect of the banking and capital markets of our country, Istanbul Takas ve Saklama Bankası A.Ş. (Istanbul Clearing, Settlement and Custody Bank Inc.) (Takasbank) has the license and authorities as the "Central Clearing and Settlement Institution", the "Custodian for Pension Funds", the "National Numbering Agency", the "Central Counterparty Institution", the "Payment and Securities Settlement System" and the "Investment Bank". In this context, it is the only institution that is constantly supervised and audited by the Capital Markets Board (CMB), the Central Bank of Republic of Turkey (CBRT), and the Banking Regulation and Supervision Agency (BRSA).

The main objective of Istanbul Clearing, Settlement and Custody Bank Inc. is to increase the competitive power of our country's markets by providing settlement and custody services and performing financial services and any and all kinds of economic activities under the related laws. Authorized by the CMB as the Central Clearing and Settlement Institution of our Country, Takasbank provides settlement, collateral and cash management services to the other markets in our country (Commodity Exchange, Energy Market), including, in particular, the markets under the structure of Borsa Istanbul A.Ş. Currently providing "Central Counterparty" (CCP) services in the Securities Lending Market, Borsa Istanbul Money Market, Equity Market, Derivatives Market and Foreign Exchange SWAP Market; Takasbank warrants the execution of transactions under the scope of its CCP activities; and in this context, it conducts a comprehensive risk management activity with its advanced technological infrastructure. In addition, Takasbank Money Market, one of the organized money markets in our Country, which brings together the financial institutions supplying and demanding funds and allows for execution of transactions with a term of not more than 6 months, thus creating the comparable market interest rates, is also a platform operated by Takasbank.

On the other hand, Takasbank, one of the institutions that received an operating license from the CBRT and was authorized as a payment and securities settlement system within the framework of the "Law no. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions" (Law), is defined as a "Critical Bank" due to the strategic importance in the banking and capital markets within the EFT-ESTS system.

Takasbank has expanded its activity areas to international platforms as well with the ”Cash Settlement and Collateral Service”, ”Global Settlement and Custody Service” and ”Local Settlement and Custody Service” that it provides through the securities and cash correspondent accounts established abroad and its SWIFT membership.

Serving as a bridge between the money and capital markets by providing reliable, fast wand cost-effective cash transfer service, Takasbank offers clearing and settlement services for the markets operating under the structure of Borsa Istanbul within the framework of the Capital Market and Borsa Istanbul legislation through online connection with the organized markets in a fully-automated environment.

Takasbank has, in years, expanded its range of banking products with instruments including cash and non-cash credit facilities and aiming to support the completion of settlement. In addition to the cash credit facilities that it extends, it conducts its banking activities and executes clearing and settlement transactions of Turkish Capital Markets supported with cash and non-cash credit facilities like Takasbank Money Market (TMM), Turkey Electronic Fund Trading Platform (TEFAS) and Securities Lending Market (SLM) operated by it, by minimizing the risks, providing liquidity for the market and aiming error-free and timely completion of settlement.

In addition, TapuTakas System (Title Deed Transfer System) was designed under the protocol signed with the General Directorate of Land Registry and Cadastre to create time, workforce and cost advantages for all parties via a modern, secure and technological infrastructure through:

- Simultaneous exchange of the real estate and the related cash sales cost;
- Elimination of the trust issues of parties;
- Elimination of cash carrying risks;
- Ease of fast transfer at low cost;

in order to prevent the problems experienced by buyers and sellers at the time of exchange of property rights and the purchase-sale cost.

Takasbank Check Clearing System allowing for payment of checks on account between bank branches and through which all functions are managed from a single center was established by adding to the clearing and settlement transactions, the collateral management function previously not included in the check clearing services, under article 5 of the Regulation on Check Clearing Transactions.

Takasbank was authorized as the central settlement bank in order to ensure continuous cash flow in the market through timely and accurate execution of payments and operation of collateral mechanism for the Electricity and Natural Gas Markets in the energy market.

Offering cross-border services to market participants as well, Takasbank also represents Turkey in global organizations under its capacity as the international settlement agency. Activities related with many projects are continued with the aim of developing the technological infrastructure in line with Takasbank's vision to become a preferred institution in international markets.

Takasbank provides access to foreign securities traded in over 65 markets globally through its current overseas custody network. Under this service, Takasbank provides for the safekeeping of capital market instruments through its accounts held with international settlement and custody institutions abroad (Euroclear and Clearstream) or global depository institutions (Citibank). Our Bank also offers the services covering appraisal, control, reconciliation and reporting to the CMB in relation to the assets of Collective Investment Schemes and Personal Pension Funds, which are provided as a service supporting and strengthening the CMB's supervision and audit function.

Authorized by the Capital Markets Board as the portfolio custody institution on 24 July 2014, our Bank provides portfolio custody services for securities mutual funds, securities investment trusts, exchange traded funds, real estate investment funds, and venture capital investment funds.

Our Bank also became an on-site R&D Center on 21 April 2017 upon the approval of the Ministry of Science, Industry and Technology of the Republic of Turkey under the Law No. 5746.

The "PERSON-TO-PERSON, ACCOUNT-TO-ACCOUNT" Gold Transfer System, one of the most important components of Istanbul International Finance Center Project, the software and system of which were developed by our Bank and which will function with the participation of

Banks, was commissioned by Takasbank, starting to provide services to the system-member banks and customers as of 16 July 2018. Offering important contributions to finance and capital markets through its risk, cash, settlement and collateral management services, Takasbank put into the service of our national economy, an organized Foreign Exchange SWAP Market jointly with Borsa İstanbul A.Ş. as of January 2018. Having become an important alternative to the Over-The-Counter (OTC) Markets at which Foreign SWAP transactions are intensively executed, Borsa Istanbul Foreign Exchange SWAP Market provides its participants with a secure environment in which they can execute their transactions without assuming counterparty credit risk through the CCP service offered.

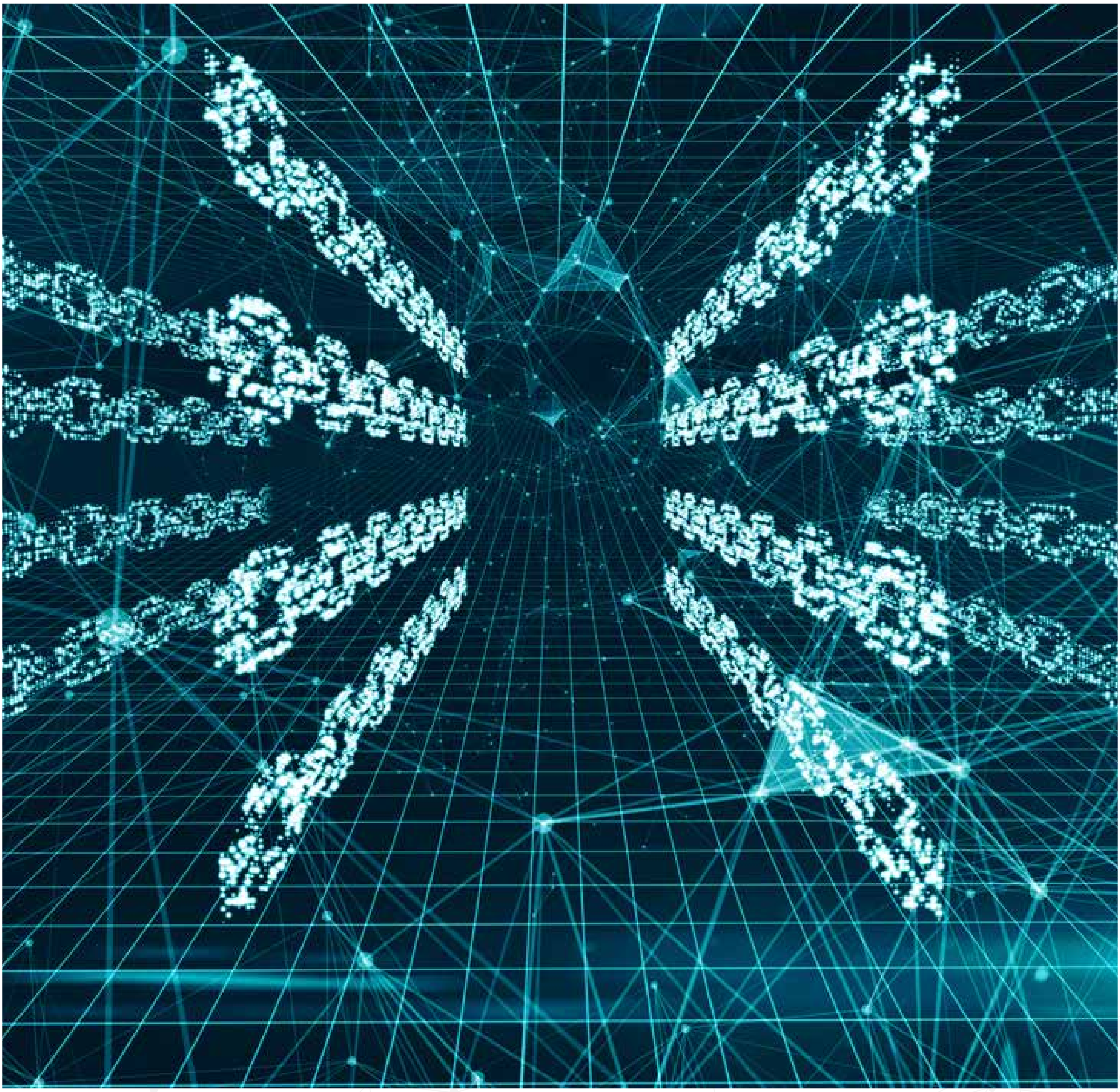
Through the said projects and comprehensive activities conducted, Takasbank not only actively supports

A BRIDGE BETWEEN MONEY AND CAPITAL MARKETS

the IFM Project, but also strengthens its position in domestic and international markets; thus, aiming to achieve its target of becoming a pacemaker institution among international settlement and custody institutions.

TAKASBANK BLOCKCHAIN VISION

Takasbank's blockchain R&D studies go back to as early as 2016 in order to comprehend state of the art in financial technologies. These activities become concrete with a specialist's dissertation published in Takasbank. At the same time, a work group on blockchain is formed to keep up with blockchain developments. The work group starts by grasping the philosophy of blockchain and then focuses on the impacts of this technology on Takasbank's role in financial markets. With trailblazing vision of Takasbank in financial technologies, innovative technologies are constantly under watch by Takasbank staff.



Takasbank is awarded with the title of On-Site R&D Center in April 2017 and FinTechHub Takas Istanbul brand name is registered. The companies and researchers working on blockchain are contacted in order to collaborate with the fintech ecosystem in this area.

Takasbank staff are encouraged to conduct their academic studies in the field of blockchain. Consultations with the regulatory and supervisory public authorities in the finance sector are made, and support agreements are reached with public research agencies.

The "Digital Transformation in Financial Markets and Blockchain Workshop" organized in Takasbank, which was the first in this field, attracting high attention of the senior-level participants from public and private companies in the Banking and Capital Markets, was held in October 2017. A panel specific for senior-level executives was organized in Takasbank in November 2017 with the contributions of a large bank with international activities under the scope of overseas collaborations. In addition, Takasbank contributed in many conferences, workshops and panels as a sponsor or by providing speakers.

As a result, blockchain platforms that can be used in the finance sector are identified and the knowledge on such platforms is obtained by studying different business scenarios for each platform. After all, by having comprehensive knowledge on blockchain, it is concluded that it is impossible to implement blockchain in financial sector with current regulations and a different approach is needed. Due to this reason, studies on zero-knowledge algorithms are initiated.

Takasbank has set as strategic goal, for the upcoming period, to be responsible for the analysis, design, infrastructure, continuous development and management of the Security Transfer Platform planned to be established using the blockchain infrastructure.

BiGA
İSTANBUL TAKAS VE SAKLAMA BANKASI A.Ş.
1 GRAM ALTIN KARŞILIĞI ŞİFRELİ DİJİTAL VARLIK
ENCRYPTED DIGITAL ASSET EQUIVALENT TO 1 GRAM GOLD
ISTANBUL CLEARING, SETTLEMENT AND CUSTODY BANK INC.

SCOPE OF THE PROJECT

The main objective of the project is to establish an infrastructure that allows transfer of dematerialized gold with certain standards, using blockchain technology. The physical equivalents of the gold kept in safe custody in the BİST vaults.

When the existing blockchain projects are examined, it is seen that digital assets are not backed by an underlying physical asset. In addition, there is a high volatility observed in their values in the markets that are not yet regulated. Also, existing digital assets are not based on a physical asset. In order to avoid unexpected fluctuations in market value, each digital asset of current financial sector, is predefined on physical basis in blockchain-based solutions. Thus, a digital asset is to be build which is safe from speculations.

BiGA is the first asset that is to be produced with this regard on blockchain platform which is integrated with the Gold Transfer System, that is a first in the world.

Under the project, the integration with the GTS managing the processes of storage of physical gold in vaults and dematerialization of gold is completed. Then, it is possible to digitalize dematerialized gold and convert them into BiGA's. Therefore, an end-to-end integral structure is established between the physical asset and digitalized asset. It is ensured that the transfer, reconciliation and reporting of digital assets could be realized through the blockchain infrastructure developed. The infrastructure is designed in a functional manner, allowing for digitalization and transfer of other assets as well.

Overview

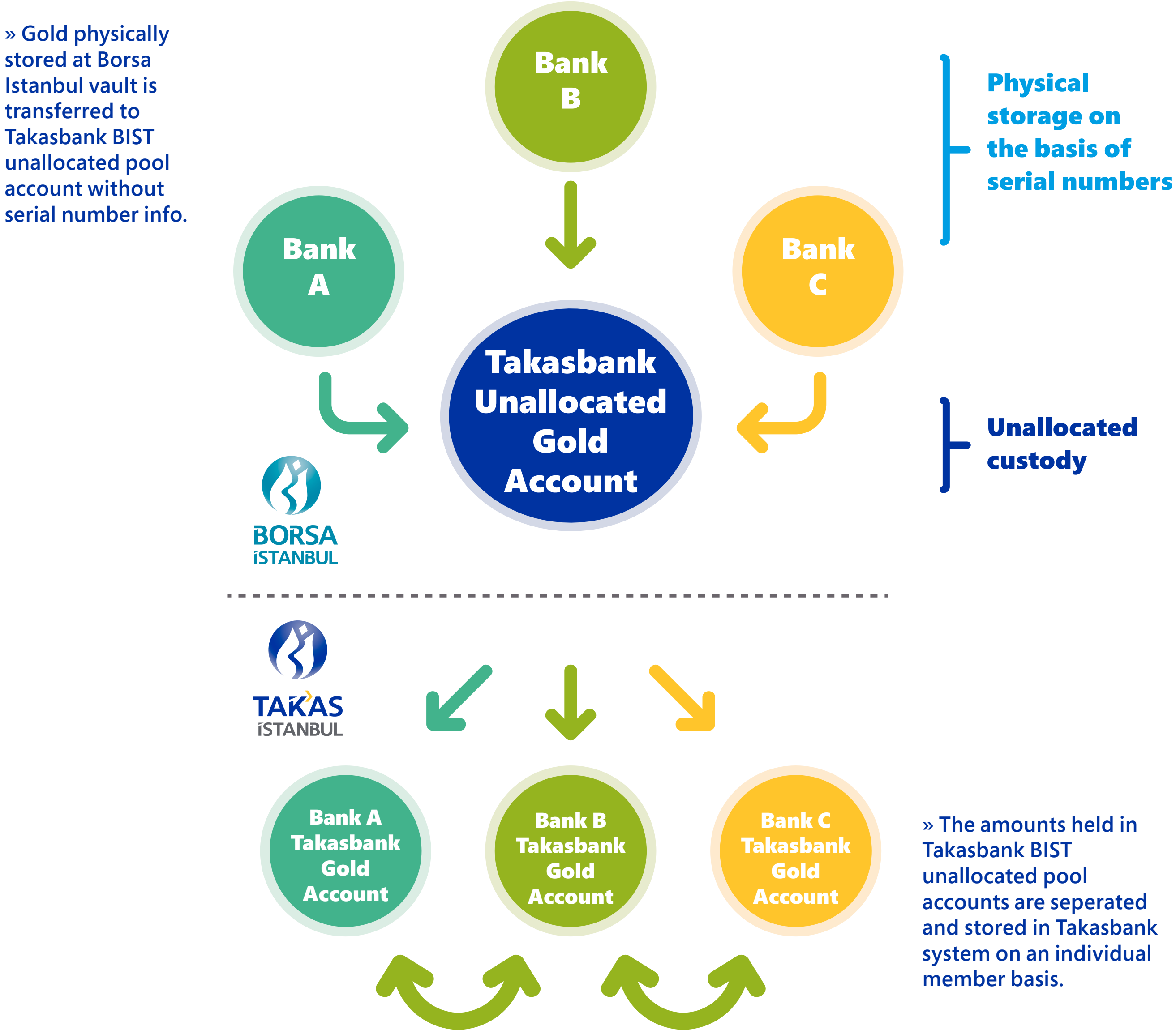
In this system, three main capabilities such as issuance, redeem and transfer are offered for the digital assets. Furthermore, additional abilities, for example, integration between the blockchain system and the GTS, reconciliation, monitoring and reporting features are also provided.

Gold Transfer System (GTS) Project

The "Gold Transfer System" is announced service by Takasbank on 16 July 2018 which enables interbank transfer of gold balances held within banks in a dematerialized manner. Hence, gold savings in the economic system is expected to increase and pave the way for its usage as a financial instrument in the Turkish financial market.

The Gold Transfer System is comprised of certain transactions. Firstly, physical gold safely stored at Borsa Istanbul vaults are dematerialized by Takasbank.

Gold physically stored at Borsa Istanbul vaults is transferred to Takasbank BIST unallocated pool account without serial number info. BIST holds them in the accounts of banks opened in the name of Takasbank within the country, and their electronic transfer between the accounts. GTS enables the accountholders to transfer their gold savings among themselves as if they make transfer in currencies. In brief, the EFT of gold is realized with this system.



» Gold physically stored at Borsa Istanbul vault is transferred to Takasbank BIST unallocated pool account without serial number info.

Physical storage on the basis of serial numbers

Unallocated custody

» The amounts held in Takasbank BIST unallocated pool accounts are seperated and stored in Takasbank system on an individual member basis.

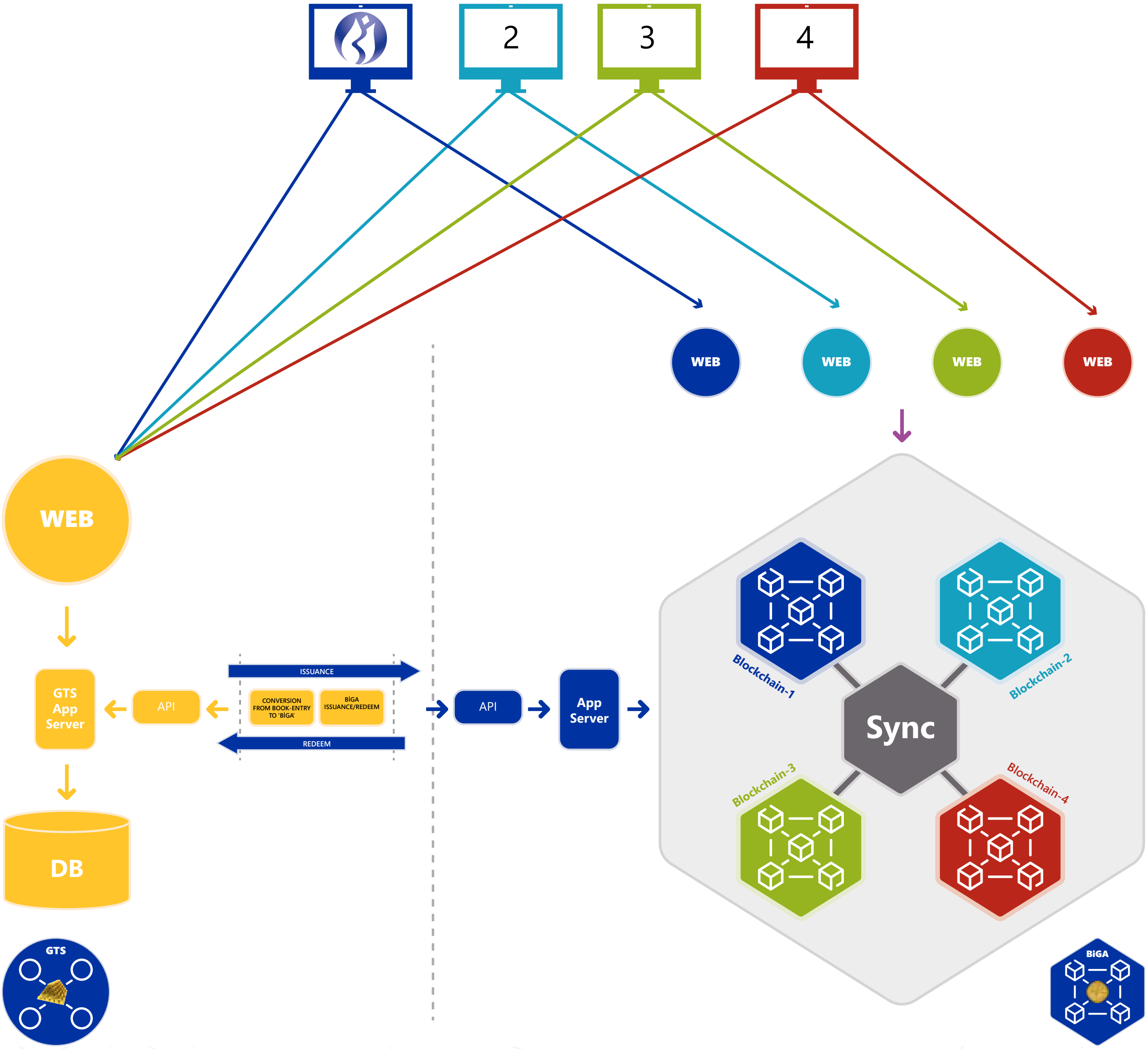
Bank B
Bank A
Bank C
Takasbank Unallocated Gold Account
BORSA İSTANBUL
TAKAS İSTANBUL
Bank A Takasbank Gold Account
Bank B Takasbank Gold Account
Bank C Takasbank Gold Account

Takasbank Dematerialized Gold Storage and Transfer System

GTS-BiGA Integration

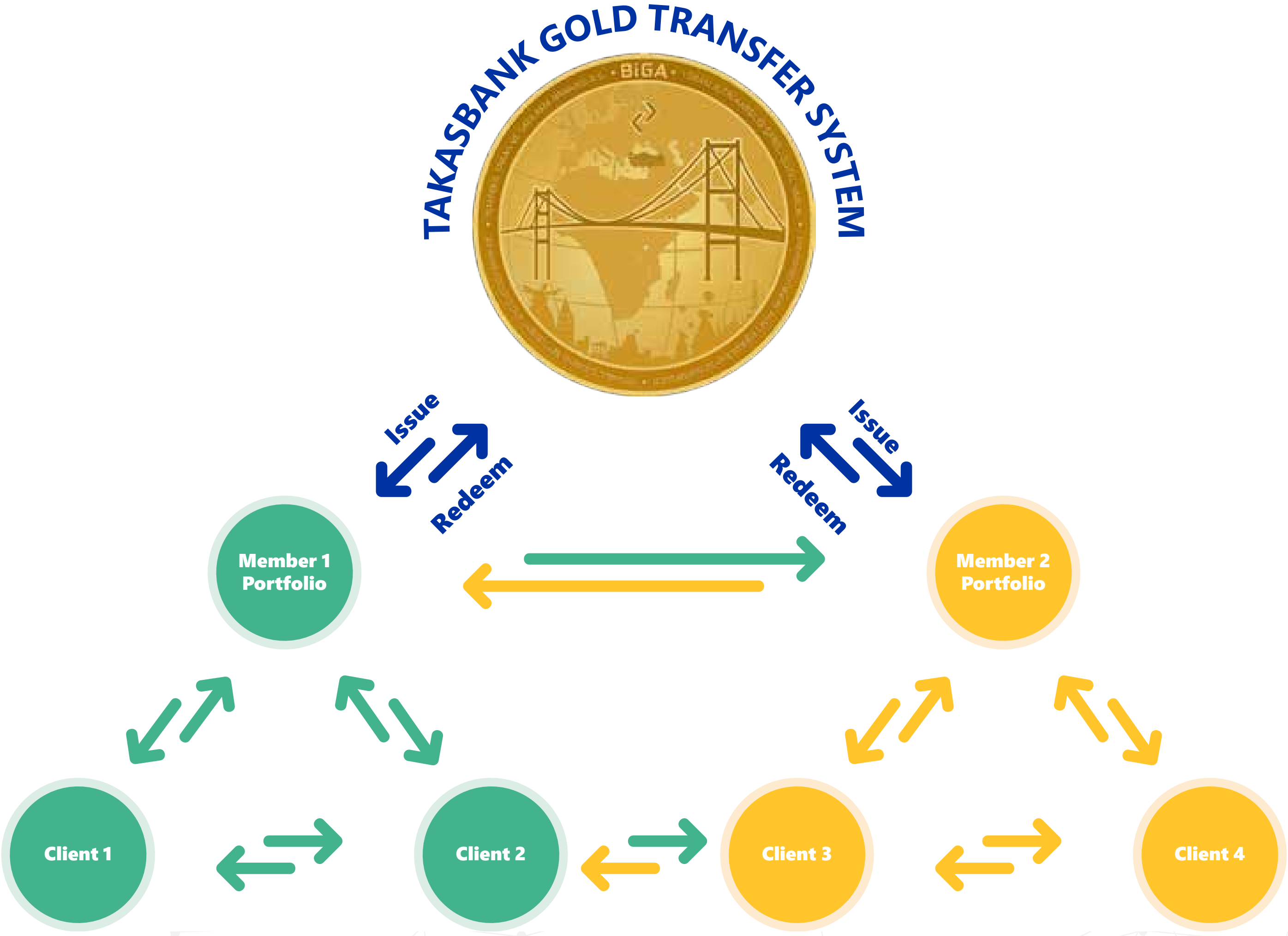
With the GTS Project, golds physically stored at Borsa Istanbul vaults are converted into dematerialized gold and then, dematerialized gold is converted to BiGAs. Thereby, each digital asset is produced with reference to its physical basis. The transformation and reconciliation between the digital asset and physical asset are made.

End users may conduct their transactions through a bank. Thus, users may change their BiGA assets over the bank (node) and convert them into dematerialized gold at any time.



Transfer

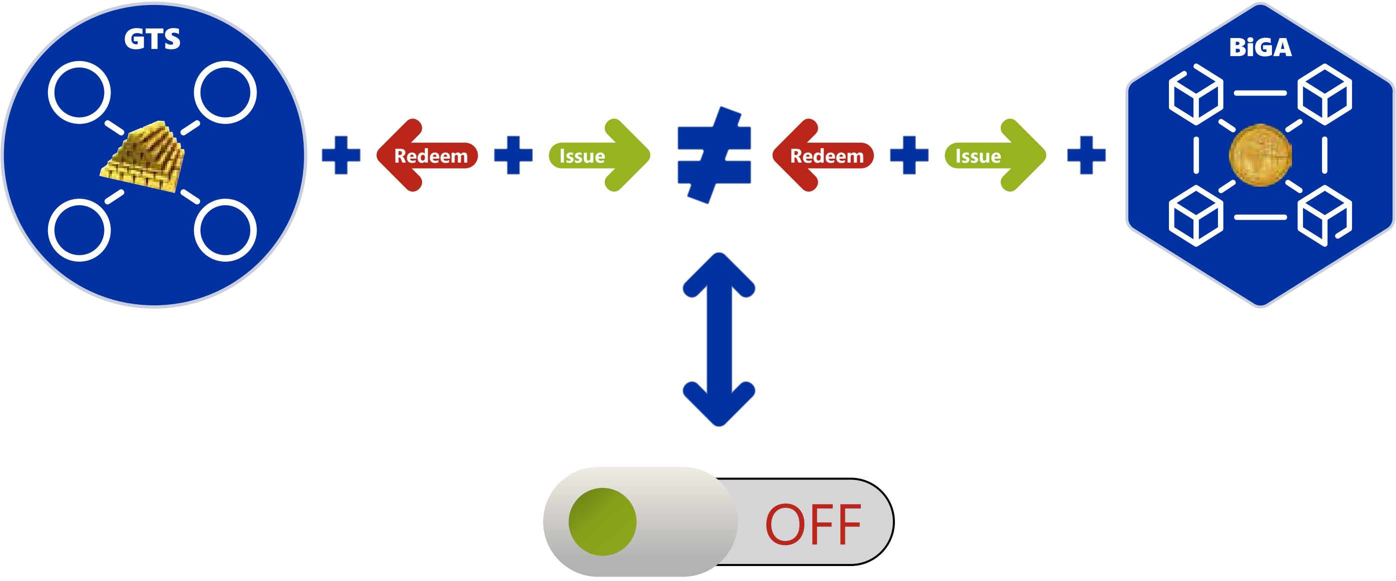
End-users can transfer their BiGA assets that are created on a 7-day/24-hour basis among BiGA accounts. The institutions participating in the system are each defined as a node on the blockchain network. These nodes constantly keep a copy of the data on the blockchain network in their most recent versions. During the transactions, BiGA amounts subject to transfer are sent encrypted and these values are stored encrypted on the blockchain. Therefore, nobody can know the amount transferred except for the users that are the parties to the transfer. In addition, the regulatory authority can also oversee any record any time. However, the other parties may approve the accuracy of the transaction while seeing nothing about actual transaction. The related encrypted balances on the blockchain are revised as a result of the approved transfer transactions. This verification process is further explained in detail in the technical section of the document.



Reconciliation

Regular controls are made in order to guarantee that the system runs in a consistent manner without any errors. The main objective of each control is to ensure that the total of the assets on the GTS and the assets held on the blockchain is equal to the total of the amount of gold physically stored in vaults at any time.

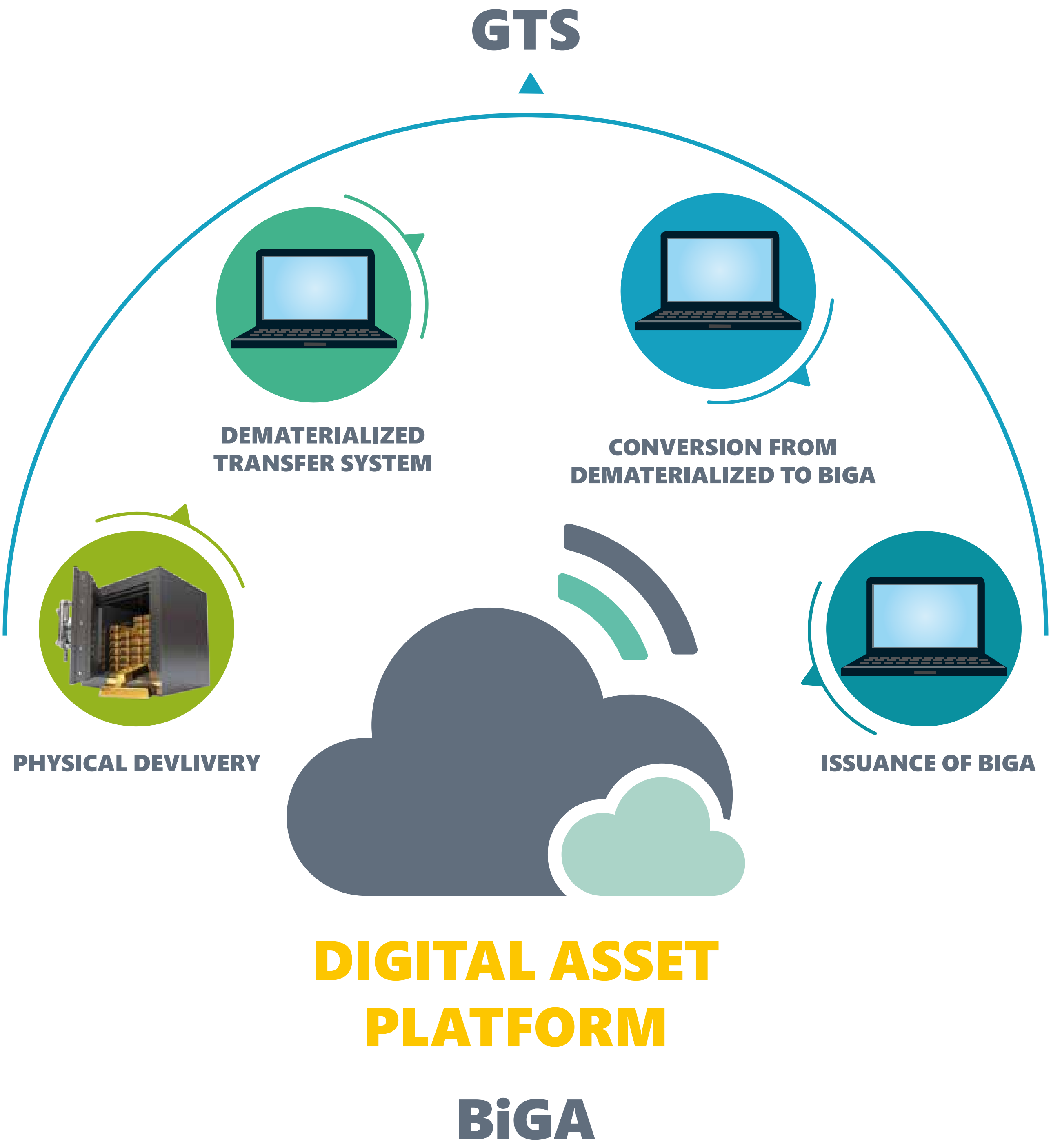
In case of any inconsistency due to any extraordinary cases; issuance, redeem and transfers are automatically suspended. After the related error is detected and fixed, the system is enabled again.



Physically-Backed Blockchain-Based New-Generation Transfer System

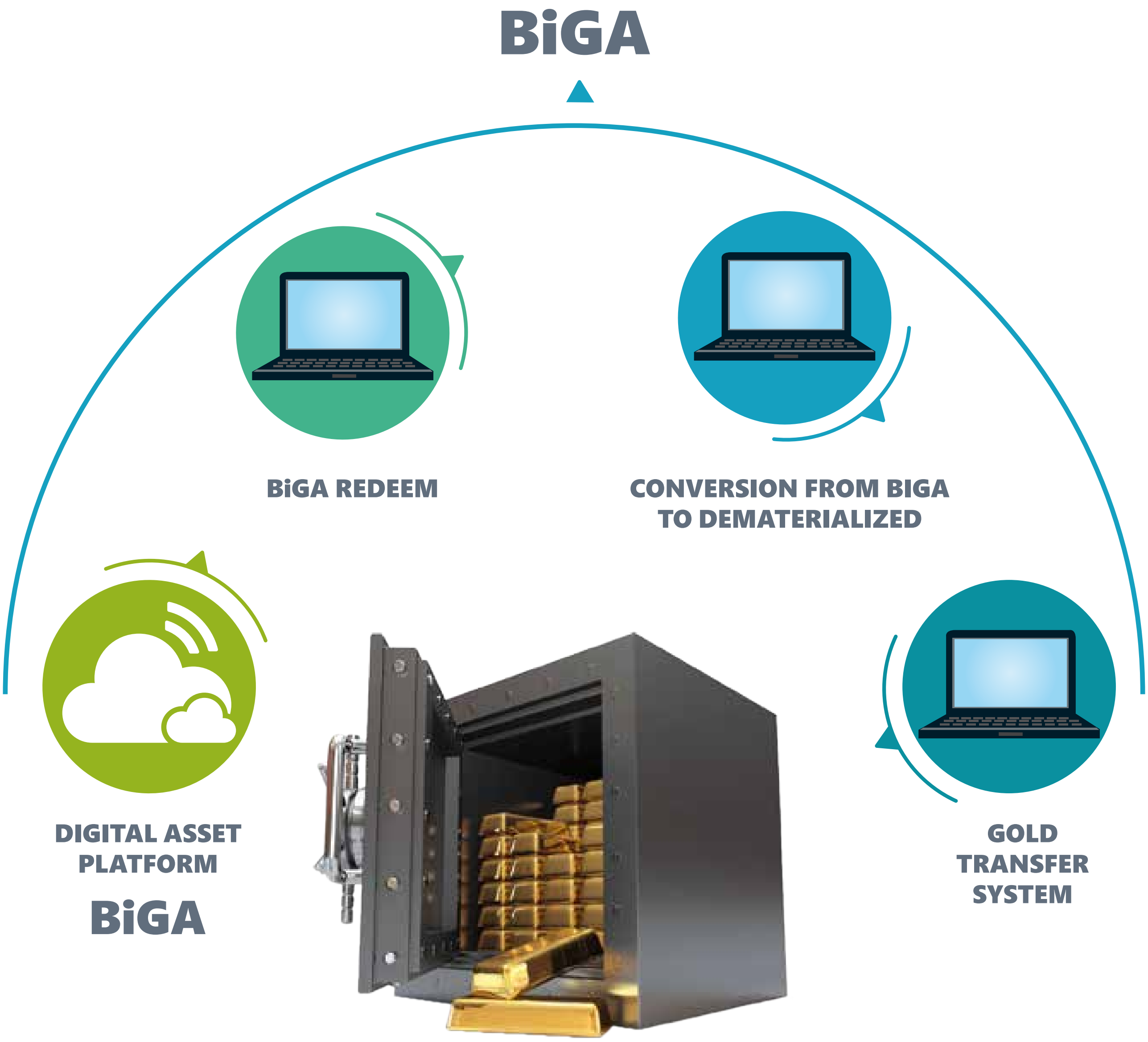
Issuance

The user who is a member of Takasbank Gold Transfer System dematerializes his 995/1000 pure LBMA-compliant gold physically stored in BIST vaults. The user then transfers the issuance of 1 BiGA in return for 1 Gram dematerialized gold to its accounts held on the Gold-Backed Digital Asset Platform. Issuance of the gold are made within the time frame specified in accordance with the operating rules of the GTS.

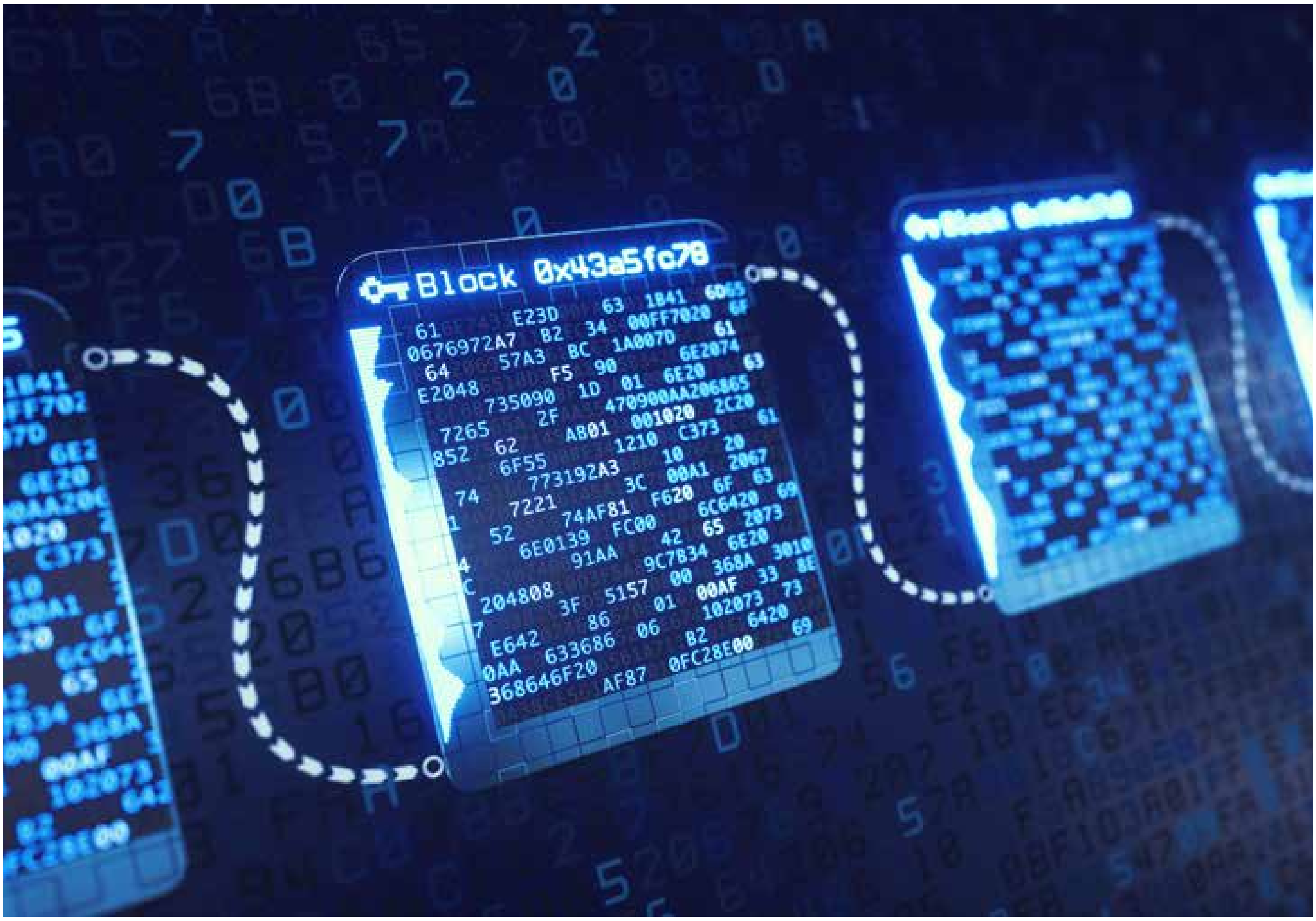

GTS
DEMATERIALIZED TRANSFER SYSTEM
CONVERSION FROM DEMATERIALIZED TO BIGA
PHYSICAL DEVLIVERY
ISSUANCE OF BIGA
DIGITAL ASSET PLATFORM
BiGA

Redeem

The user converts its BiGAs, which are held in its accounts, to dematerialized gold, thus ensuring that they are out of the system. The user converts 1 BiGA on the Gold-Backed Digital Asset Platform to 1 Gram dematerialized gold and then, transfers the amount to its accounts on GTS. Redeem process is realized within the time frames specified in accordance with the operating rules of the GTS.



PHYSICAL EXIT



TECHNICAL BACKGROUND OF THE PROJECT

The technical studies for the project are initiated in the last quarter of 2017. Firstly, efforts are initiated with Hyperledger Fabric 1.0 platform. At this stage, cooperation is established with a fintech company with case studies in this field for both introduction to blockchain technical studies and contributing to the fintech ecosystem. Moreover, while starting the related activities, collaboration is made with TÜBİTAK BİLGEM Blockchain Research Laboratory concerning Zero-Knowledge requirements. Thus, the ecosystem and the technical foundations of the project are established with the expertise of different disciplines brought together.

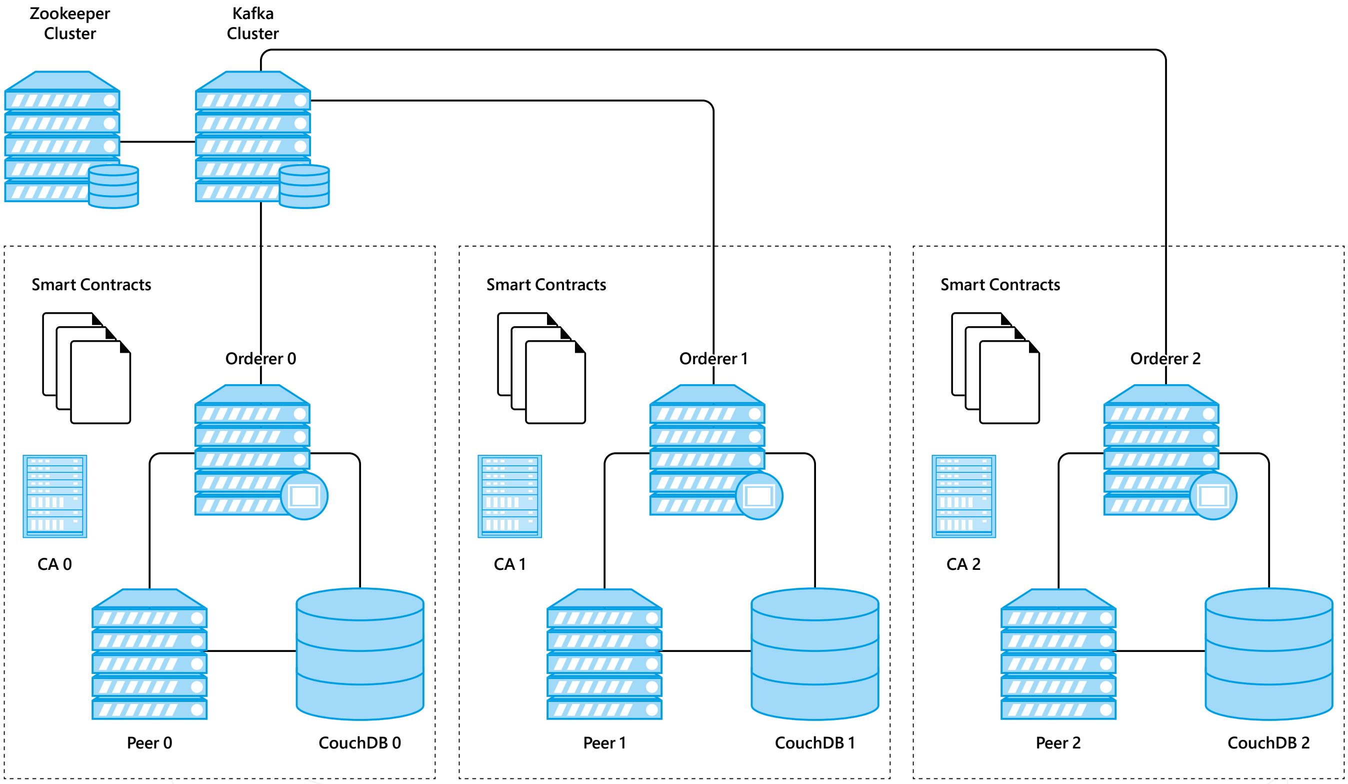
The project is continued solely with the efforts of Takasbank employees in the following stages. The used blockchain infrastructure is Hyperledger Fabric and then later continues with Quorum platform. These studies are not conducted merely on blockchain platforms. For instance, new-generation technologies like Docker are frequently used in this project.

Information on the technical components used in the project and the experiences are provided in this section.

Hyperledger

Hyperledger is an open-source platform supported by Linux Foundation. It is the first platform without requiring use of cryptocurrency, on which transactions are conducted through smart contracts (chaincode). It quickly becomes popular in corporate research projects. Hyperledger service layer is considered in three main logical categories. These include membership services, blockchain services and chaincode services.

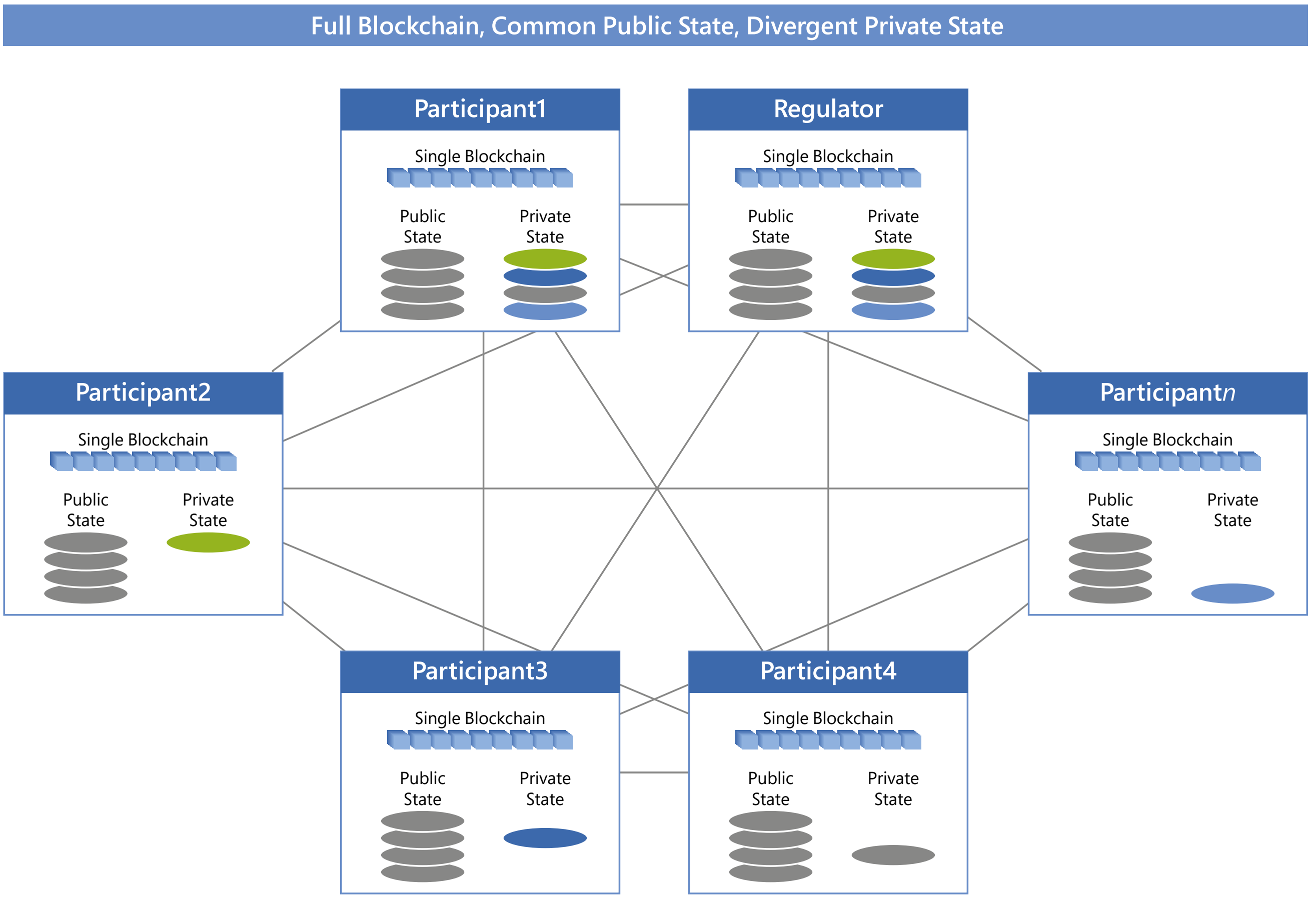
While membership services provide services related with identity, privacy, etc.; blockchain services manage the blockchain and consensus structure together with the P2P protocol built in them. Chaincode services allow for management and operation of smart contracts within Hyperledger infrastructure. In addition, event-driven bidirectional interactions are ensured within the service layer together with a communication layer located at a lower level. Although these terms and structures may sound quite confusing at first step, Hyperledger is tested in many Blockchain R&D projects since it contains the fundamental elements needed by the business world. Hyperledger supports five different projects, instead of creating a single blockchain framework. The one that stands out among these projects is the Fabric. Thanks to its modular architecture, modules can be replaced as required with the plug-and-play philosophy. In addition, there are Iroha, Sawtooth, Burrow and Indy Hyperledger projects.



Source: https://medium.com/@abhinav.garg_90821/hyperledger-fabric-multi-orgs-multi-nodes-with-kafka-zookeeper-and-swarm-cluster-946a94dade0f

Quorum

It is an open-source platform released by J.P. Morgan in 2015 as a result of the modification of the structure of Ethereum for the purpose of its usage in financial markets. While this platform facilitates business processes and the process of overcoming legal restrictions, it is used to produce new-generation transaction applications based on trust, accountability and transparency. Since it also has Ethereum infrastructure, it offers the advantages provided by this platform as well. Its fast consensus algorithm running with high precision in spite of its permissioned structure, and its capability to allow for execution of transparent and private transactions are considered as its key properties. The developments to be made in Ethereum infrastructure are easily reflected to Quorum. The network produced using this platform can be set up very quickly.



Source: Quorumwhitepapper-https://github.com/jpmorganchase/quorumdocs/blob/master/Quorum%20White-paper%20v0.1.pdf

Zero-Knowledge Proof

Zero-Knowledge proof is a model to solve proof problems, one of the most common in the field of cryptology. It is a proof method produced with the motto of "How can I prove that I know the information without revealing the information to the counterparty?". Cryptologic functions run in the background and their assumptions are used to prove the information.

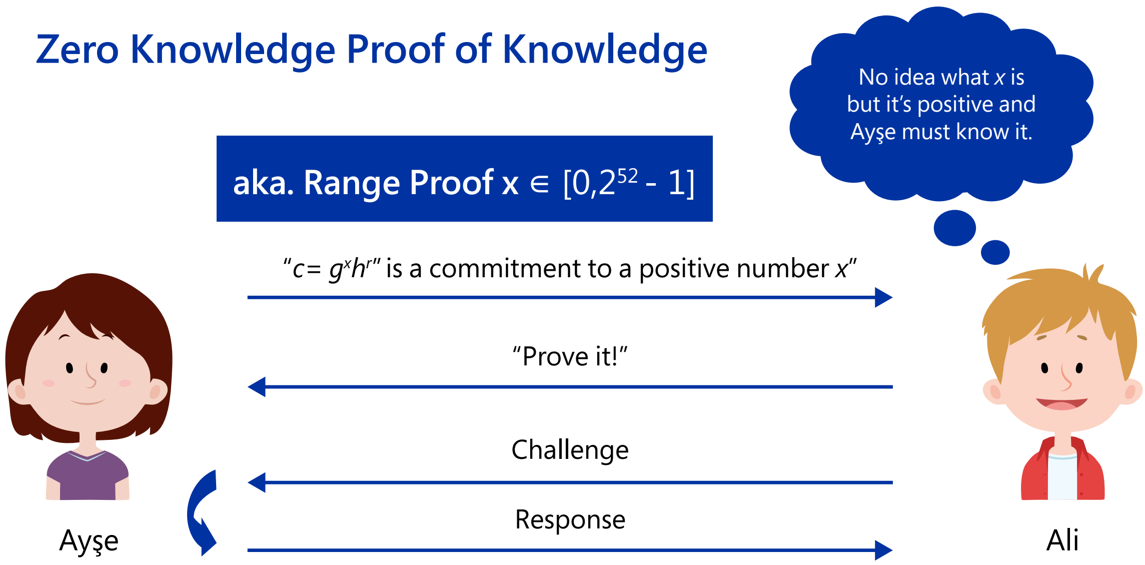
Zero-Knowledge proof must satisfy the following three parameters:

- **Completeness**: If the proof given is true and complete, the receiver will be convinced that the giver knows the information.
- **Soundness:** If the proof is not false, the giver persuades the receiver without cheating.
- **Zero Knowledge:** If the statement is true, the receiver will understand it. The giver's knowledge is proven with the example given to the receiver.

Completeness and Soundness are properties of more general interactive communication with the receiver. Zero Knowledge can be stated as the proof method.

Zero-Knowledge proof is not a proof in the mathematical sense of the term. In this method, the information is used for the purpose of proving to the receiver through manipulation.

The usage of blockchain technologies in their current state especially in financial areas is considered to be quite difficult due to regulation requirements. The facts that the data are constantly kept updated in all nodes and every incoming transaction is approved by nodes and that the information about the persons executing the transactions and the related transaction amounts are kept open on all nodes are considered to pose serious obstacles against the usage of this technology in the finance and satisfaction of the regulation requirements. Zero-Knowledge Proof model offers a resolution of such issues.



Zero Knowledge Proof of Knowledge

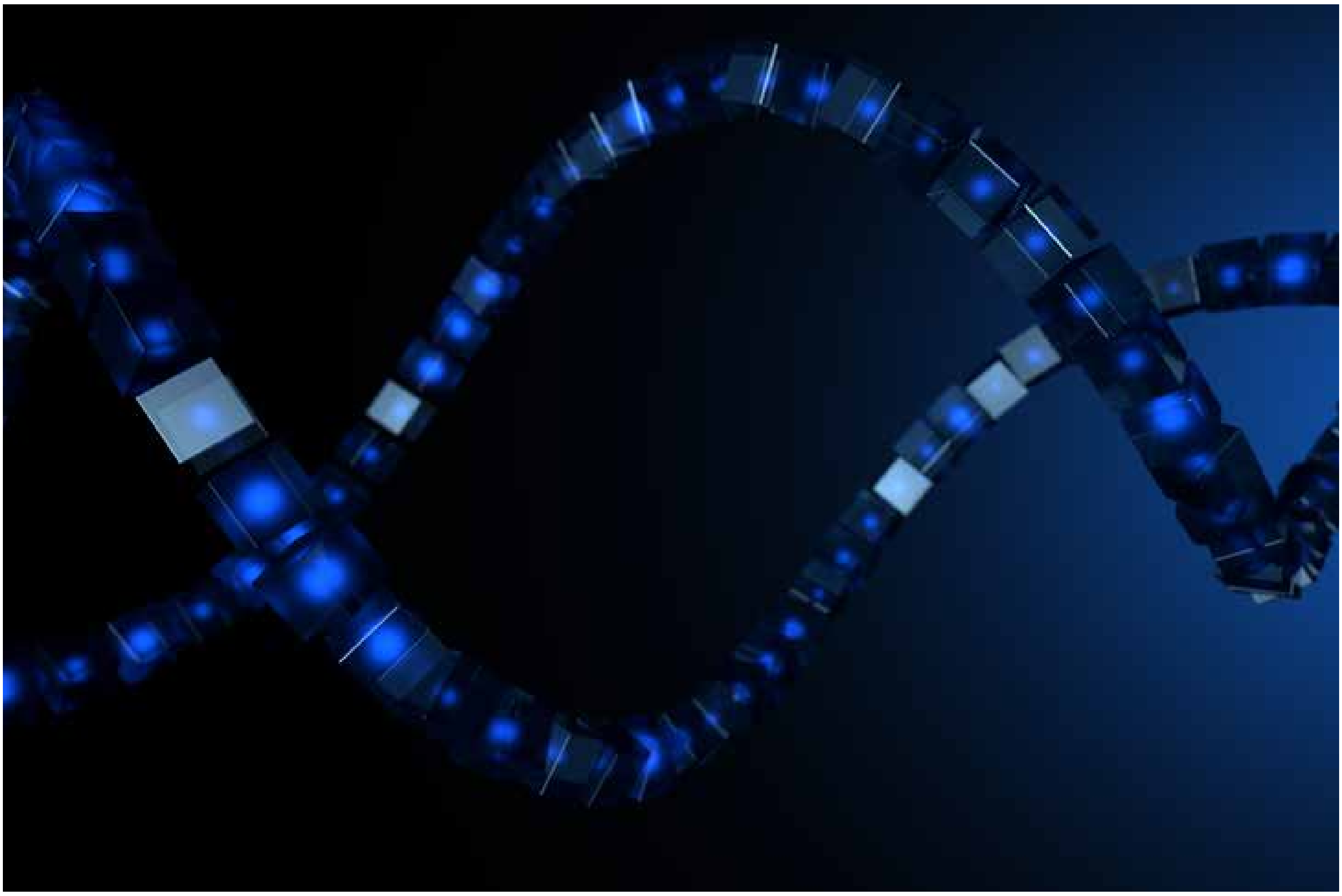
No idea what x is but it's positive and Ayşe must know it.
aka. Range Proof x ∈ [0,2^{52} - 1]
"$c= g^x h^r$" is a commitment to a positive number x"
"Prove it!"
Challenge
Response
Ayşe
Ali

Kaynak: https://hackernoon.com/bulletproofs-the-new-kid-in-blockchain-security-land-e730fc0efe14

Other Technologies

Innovative technologies for software development processes are also used in the project. These technologies are as follows:

- **Programming languages:** Java, Go, JavaScript, AngularJS, Solidity
- **Supporting solutions:** Quorum Maker
- **Container technology:** Docker
- **Operating system:** Linux
- **Application server:** WildFly
- **Database:** PostgreSQL, CouchDB



FUNCTIONAL DESIGN

Although there are various alternatives for different platforms and technologies in BiGA Project, studies are focused on Hyperledger Fabric and Quorum platforms due to their aforementioned capabilities. Since a closed-loop system and a structure to which only the nodes to be authorized by the platform administrator can be added are planned, platforms with permissioned structures are selected (permissioned blockchain).

In the permissioned blockchains, only the specified nodes can create blocks with specific rights and participate in the consensus. In permission-less blockchain, every chain has contribution in the consensus and block generation. Private blockchain structure determine the persons with whom the information is shared with. In private blockchain, the network is not open to everyone. Only those joining the network can access to the blockchain data. In a public blockchain, the network is open to access by all nodes. BiGA has a blockchain network that is in the permissioned and private category.
When current blockchain technologies are intended to use in the financial instruments, the infrastructure provided in practice has two major restrictions.

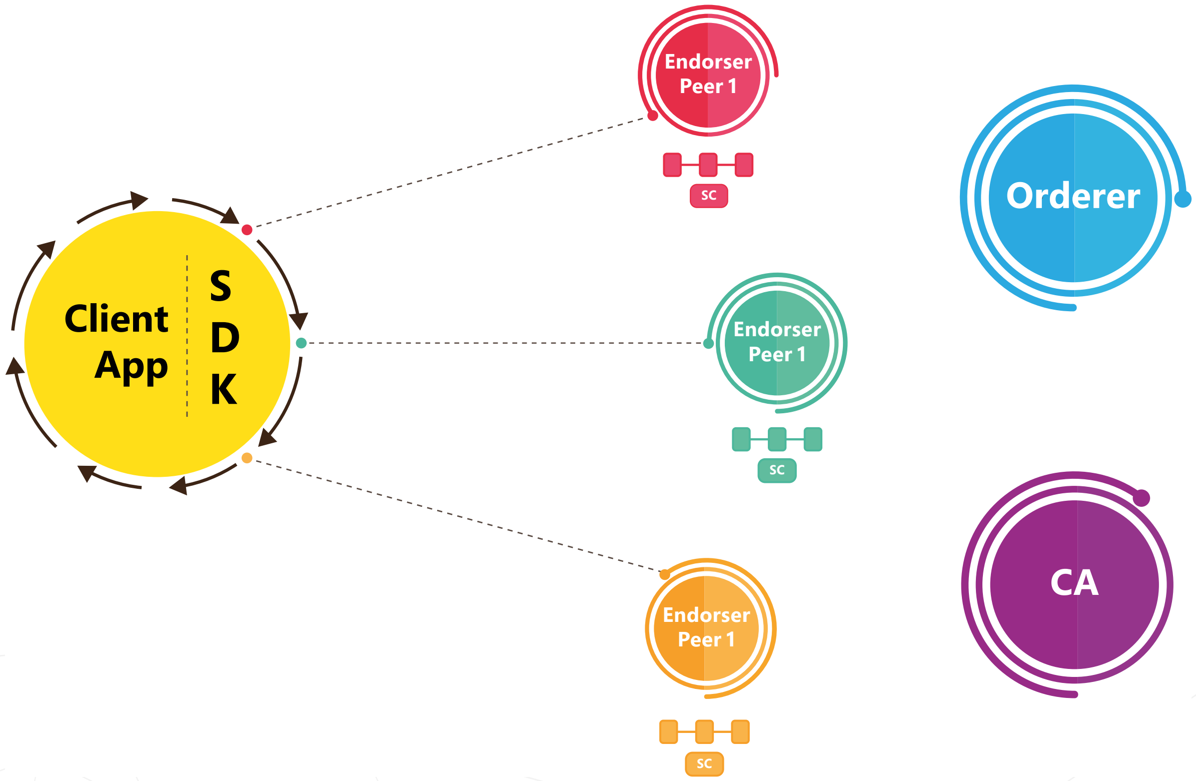
One of the restrictions is the privacy. In case that all transactions are visible on blockchain; in addition to the involved parties, the other nodes can also view the transaction detail. The other restriction is the failure of control and audit of transactions by the relevant authority in case that the transactions are fully closed and private.

BiGA Project offers a solution to these two restrictions. This design covers the solution in which the involved nodes can view the related transactions, the other nodes in the system can validate the accuracy of the transaction and transfer even though they cannot view any data, and the authorized node can also view the transaction detail. The technical provision of this architectural design covers the method of adding zero-knowledge proof algorithms to the current blockchain platforms.

BiGA with Hyperledger platform

The BiGA Project with Hyperledger platform presents a design in which every nodes on the blockchain network are designed as endorser nodes. The application server, database and the related services of each node in BiGA are defined.

A separate wallet is not designed in BiGA Project. Users' account structures and the related transactions are conducted by the related node on the blockchain through REST services located on the server. CouchDB is used as the database for storage of state details. There is at least one channel by default on the blockchain network built with Hyperledger Fabric. Apart from these structures, an organization, a CA (Certificate Authority) and an orderer are used.



The general view of the design for BiGA is specified in the below figure. A Single organization and a single channel structure are used in this design. BiGA Project Hyperledger Platform studies are developed with smart contracts. The use of smart contracts allowed for entry and definition of other values on the infrastructure. The smart contracts on Hyperledger Fabric are developed with Go.

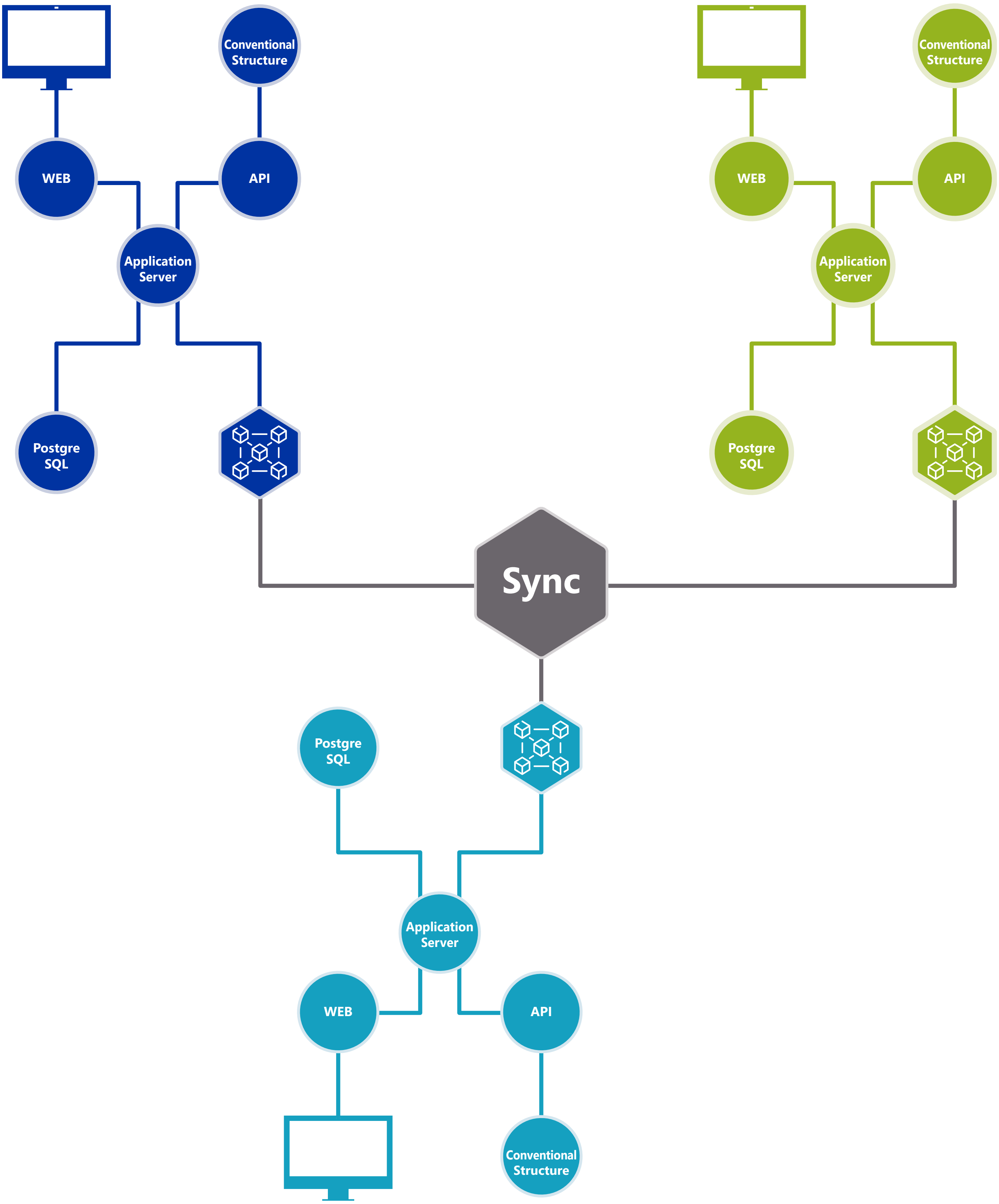
A separate server is built for each node and configured to run in different environments. There is no integration made between the nodes except for the blockchain network. Thus, a real network environment could be created.

Since the project is a closed-loop proof-of-concept project, cloud environment is preferred as the infrastructure in order to more efficiently use the development and testing period. In addition, no personal data are stored on the blockchain network under any circumstances.

During the early stages of the Project with Hyperledger, the following items are used:

- **Fabric Configuration:** Making the definitions like the organization, peers, channel, etc., production of certificates, creation of docker images;
- **Smart contract:** Making the related development in Go language;
- **Chaincode Deploy:** Loading chaincode and channel properties onto the servers;
- Generation of the client java application with Fabric SDK;
- **Installation scripts:** Editing of cloud-formation scripts;
- **API Layer:** Creation of the service layer for Rest API;
- Making the web-based developments for Usage, Reporting and Monitoring functions.

BiGA has proved that alternative financial instruments can be deployed on single blockchain.



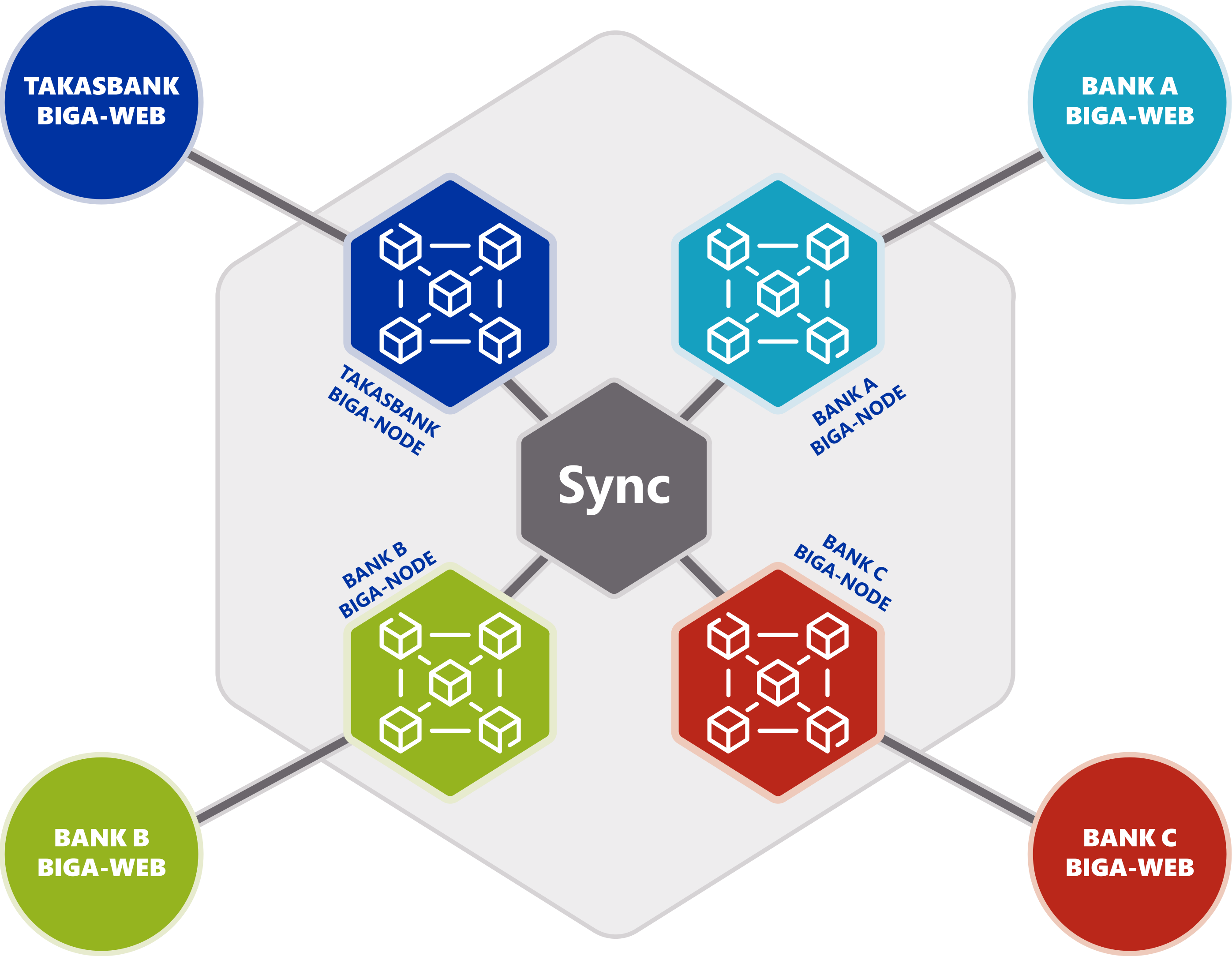
BiGA Hyperledger Design

BiGA with Quorum Platform

Ethereum is another blockchain infrastructure that is used while designing BiGA Project. At the beginning, it is concluded that the plain Ethereum infrastructure is not adequate for corporate usage; and that it is more suitable for public use. In this context, it is considered appropriate to use Quorum, permissioned blockchain infrastructure developed by J.P. Morgan, which is the version of Ethereum blockchain infrastructure customized for corporate applications.

The business logic required for BiGA Project is produced with smart contracts. Solidity, the most popular programming language, is used to write Ethereum-based smart contracts. A Java-based integration application is developed to ensure communication with such smart contracts; and Web3j library is used in this application. In addition, the open-source Quorum-Maker project developed by Synechrorn-Finlabs is used to rapidly set up and configure Quorum blockchain network.

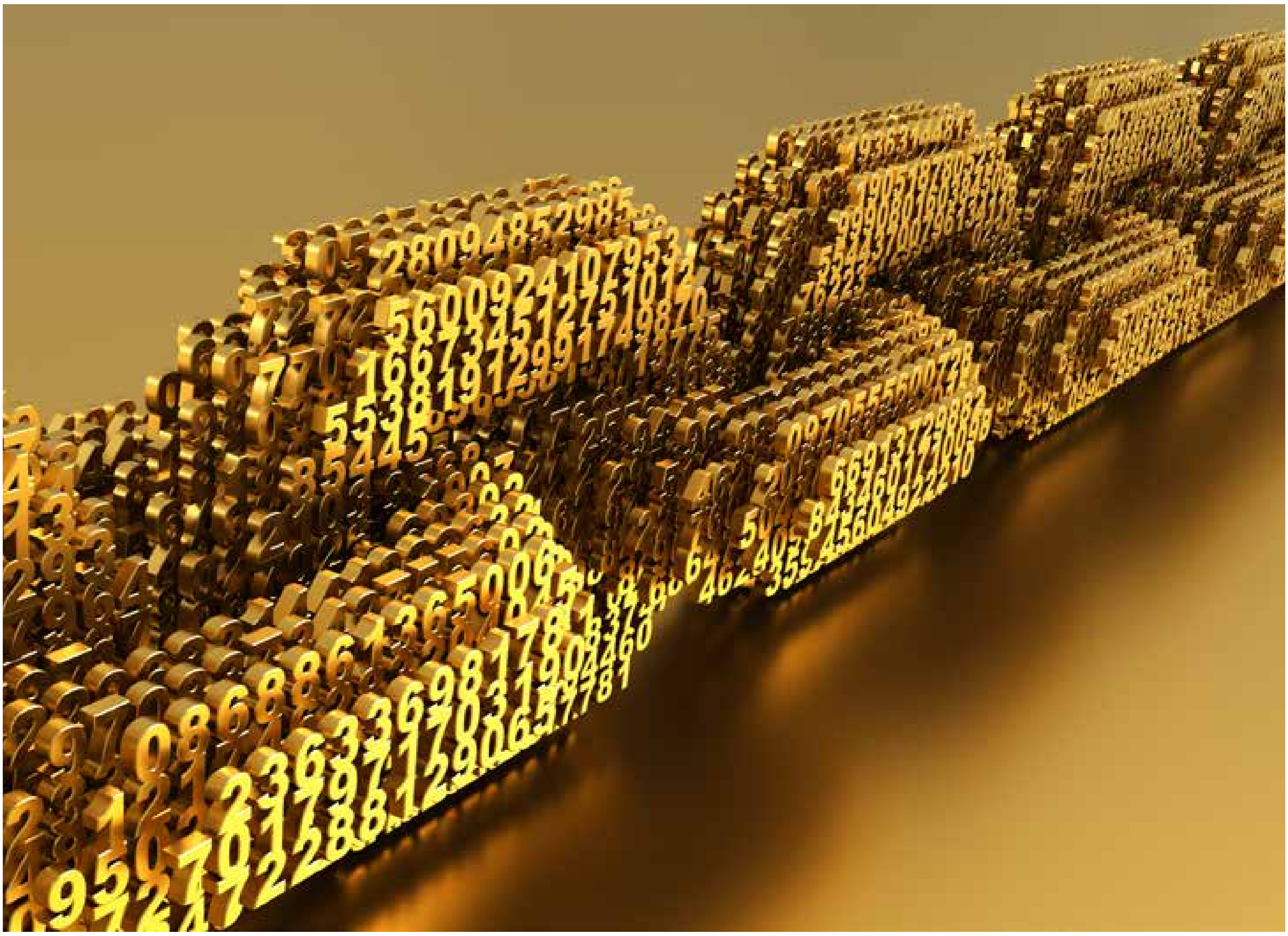
Takasbank BiGA Blockchain Network



During the development of BiGA Project, it is determined that Quorum blockchain infrastructure and Quorum-Maker tool do not completely meet the project requirements. Therefore, some customizations are made by creating forks in Quorum and Quorum Maker projects in order to meet such requirements and they are adapted to BiGA Project.

One of the R&D focuses of BiGA Project is to ensure privacy of transactions conducted on the blockchain network. Currently, there are some blockchain technologies ensuring transfer privacy (Zcash, Monero, etc.). However, these technologies work with the principle of full confidentiality/ privacy and cannot be monitored by anybody except for the parties involved. This eliminates the possibility of review and control of transfers by regulatory authorities. In order to solve this problem, it is aimed to develop a blockchain infrastructure compliant with the regulations and ensuring privacy for the parties that are not subject to the transfer. Thus, it is ensured that all the transactions could be validated by all nodes through zero-knowledge proofs without knowing the contents and that only the regulatory authority could monitor all transfers in the system.

Different cryptographic proof algorithms are tested in order to meet these requirements. The party that conducts a transaction on Quorum network has to encrypt all data related with the transaction, to create some cryptographic proofs for the related transaction, and to post and publish such encrypted data and proofs on the network. These transactions published on the network must be cryptographically verified on all nodes via smart contracts and processed as a result of such verification. Cryptographic verifications requiring high performance may be carried out by smart contracts on the nodes. Since smart contracts run on EVM (Ethereum Virtual Machine) layer, they create high costs in terms of both performance and scale. In order to meet these requirements, such activities are added to Ethereum Pre-Compiled smart contracts running outside EVM and developed with Go programming language. These smart contracts running on EVM execute the verification of cryptographic proofs by means of Pre-Compiled contracts. The related block is created on the blockchain according to the result of the transaction. Quorum and Quorum Maker tool are customized and forked to build the cryptographic proof verification mechanism on the Quorum infrastructure. RAFT is used as the consensus algorithm during the initial phase of the project. It is planned to be changed with other consensus algorithms in the following stages of the project.



BiGA PROJECT TEST RESULTS

The BiGA Project multi-party testing process is started upon completion of the blockchain and GTS integration. Firstly, BiGA Project is introduced and the related information is shared with the banks currently using Takasbank GTS system. Five banks including Albaraka Türk Participation Bank, Garanti BBVA, Kuveyt Türk Participation Bank, VakıfBank and Ziraat Bank participated in the tests.

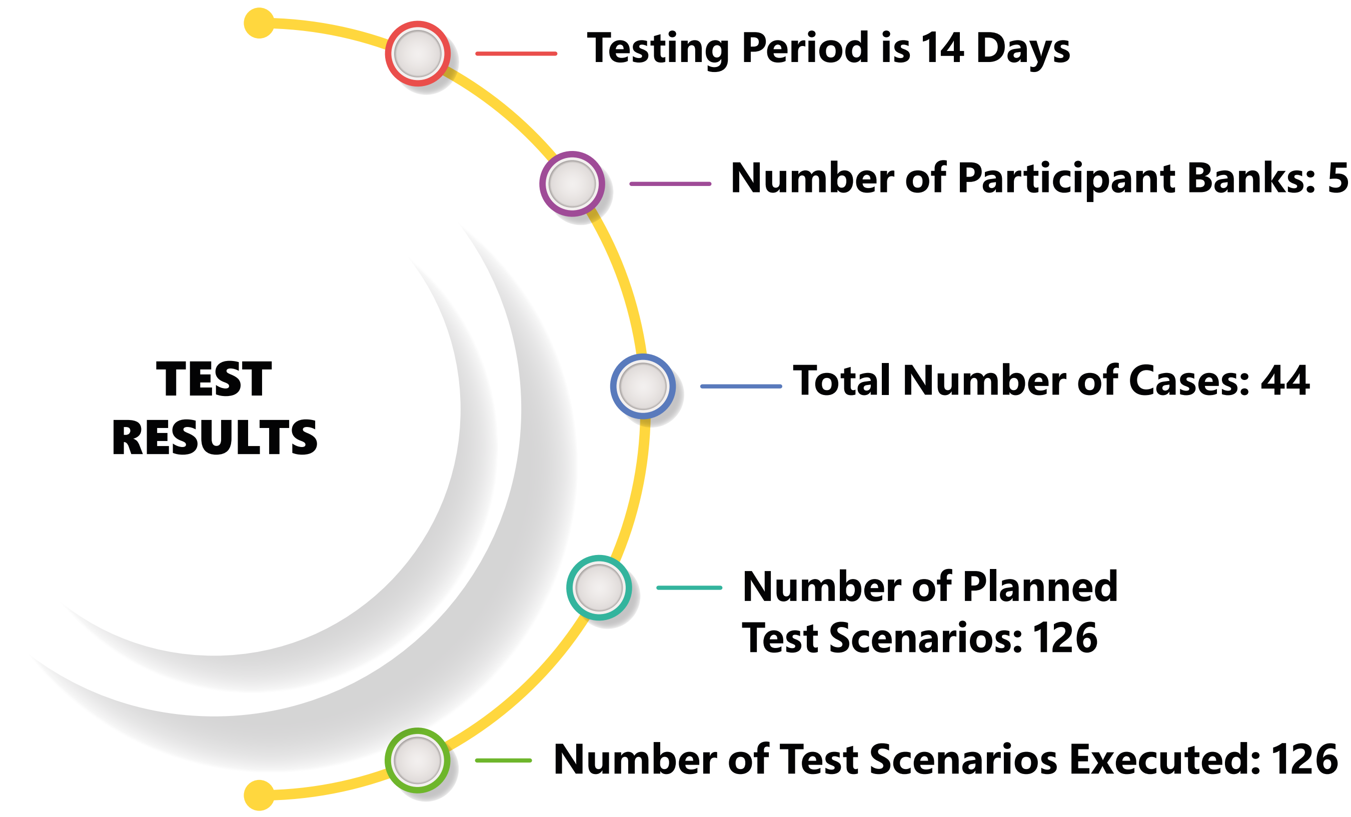
Test scenarios

The following items are tested.

- Blockchain node installation script
- Setting up the blockchain network and participation to the blockchain network
- Blockchain web installation script
- Blockchain wallet operations
- Creation of transactions and monitoring of blocks on blockchain
- Smart contracts
- Balances that can be viewed by the related parties with only Zero Knowledge
- Takasbank Gold Transfer System Screens and Integrations

Test results

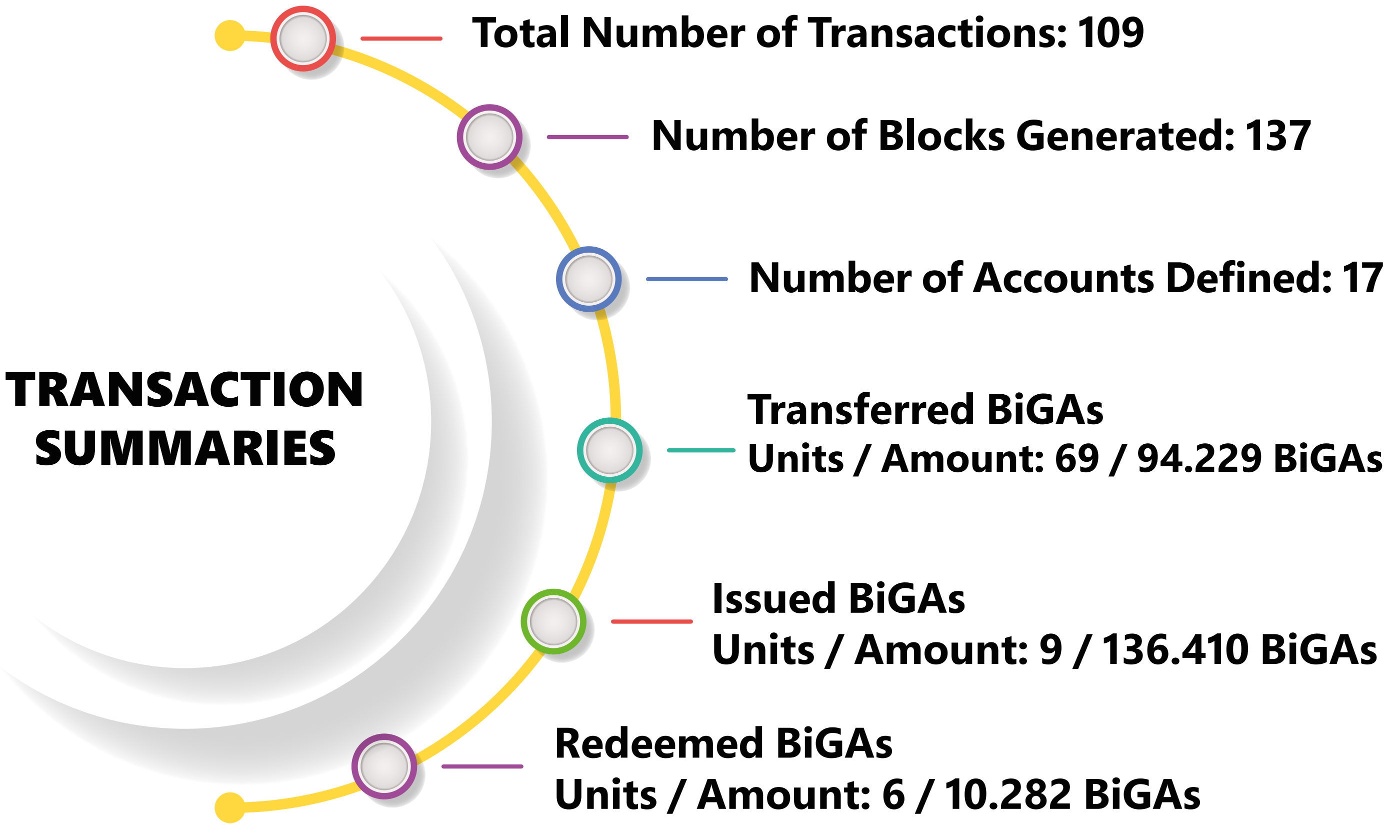
Test results are summarized in the table below.



TEST RESULTS

- Testing Period is 14 Days
- Number of Participant Banks: 5
- Total Number of Cases: 44
- Number of Planned Test Scenarios: 126
- Number of Test Scenarios Executed: 126

The summary of transactions executed during such testing is provided in the table below.



TRANSACTION SUMMARIES

- Total Number of Transactions: 109
- Number of Blocks Generated: 137
- Number of Accounts Defined: 17
- Transferred BiGAs Units / Amount: 69 / 94.229 BiGAs
- Issued BiGAs Units / Amount: 9 / 136.410 BiGAs
- Redeemed BiGAs Units / Amount: 6 / 10.282 BiGAs

BiGA Functions Test Results

The functions reviewed under BiGA Project tests are specified in the table below. The testing of functions is successfully completed by all participants

BiGA Functions Tests Evaluation	Albaraka Türk Participation Bank	Garanti BBVA	Kuveyt Türk Participation Bank	VakıfBank	Ziraat Bankası
Node installations and participation to the blockchain network	✓	✓	✓	✓	✓
Installation of web application	✓	✓	✓	✓	✓
Definition of BiGA Platform Portfolio Account over the GTS	✓	✓	✓	✓	✓
BiGA Platform New User Definition	✓	✓	✓	✓	✓
BiGA Platform New Account Creation	✓	✓	✓	✓	✓
Dematerialized Gold – BiGA Conversion	✓	✓	✓	✓	✓
BiGA Issuance	✓	✓	✓	✓	✓
Intra-Member BiGA Transfer (Portfolio-Client, Client-Client)	✓	✓	✓	✓	✓
Inter-Member BiGA Transfer (Portfolio-Client, Client-Client)	✓	✓	✓	✓	✓
BiGA Redeem	✓	✓	✓	✓	✓
BiGA – Dematerialized Gold Conversion	✓	✓	✓	✓	✓

BiGA has a parametric infrastructure that allows for the transfer of any digital asset.

This asset transfer infrastructure also allows for digitalization and transfer of any assets in addition to gold.

BiGA
İSTANBUL TAKAS VE SAKLAMA BANKASI A.Ş.
1GRAM ALTIN KARŞILIĞI ŞİFRELİ DİJİTAL VARLIK
ENCRYPTED DIGITAL ASSET EQUIVALENT TO 1GRAM GOLD
ISTANBUL CLEARING, SETTLEMENT AND CUSTODY BANK INC.

İSTANBUL TAKAS VE SAKLAMA BANKASI A.Ş. • BiG
İSTANBUL SETTLEMENT AND CUSTODY BANK INC.
İSTANBUL CLEARING SETTLEMENT AND CUSTODY BANK INC.

TECHNICAL OUTPUTS

The purpose of this document is to guide the new studies to be conducted by sharing the experiences in BiGA project. It is also aimed to provide a perspective to the entrepreneurs and R&D centers familiar with the issue and evaluating project alternatives. In addition, it is intended to present the concrete outputs and benefits to the public authorities following up the studies conducted in this field, and to reach out to the concerned parties for potential collaboration. The technical and process-related experiences throughout the project are shared in this section.

BiGA Project, proof-of-feasibility studies are conducted on the basis of the fundamental principles of blockchain approach that differs from conventional data processing, storage, reconciliation methods and technologies. In this context, the technical know-how on blockchain and cryptography in the project is presented below.

Operating principles of distributed systems:

In conventional approaches, data are stored in a centralized location and it is shared with the other related stakeholders to the extent required through integration

A • 1 GRAM ALTIN KARŞILIĞI ŞİFRELİ DİJİTAL VARLIK •
ENCRYPTED DIGITAL ASSET EQUIVALENT TO 1 GRAM GOLD

methods. As for blockchain approaches, data and transactions are simultaneously stored at all stakeholders with exactly the same format and content. This assures the integrity, accessibility, privacy and accuracy of the data no matter who is the stakeholder.

Different blockchain infrastructures: The usage of permissioned blockchain networks is considered as an important criterion at the initial stage in order to find a corporate solution. In this context, trials are conducted with Hyperledger and Quorum infrastructures.

After careful studies, Hyperledger Fabric 1.0 infrastructure is preferred not to be used in the project since it does not meet the satisfactory maturity criteria for a solution to be commissioned in the production environment. Quorum is used by changing its structure through forking method due to its similar restrictions. Moreover, a similar forking can be made for Hyperledger infrastructure. The project is continued with Quorum because it has more accessible resources and the blockchain network can be enabled and activated faster with Quorum Maker.

Consensus algorithms:

BFT (Byzantine Fault Tolerance) and RAFT algorithms are tried in order to guarantee the integrity, accessibility, privacy and accuracy of data to be stored at stakeholders since the structure has a distributed architecture. RAFT algorithm is a default with Quorum. With current capabilities, it is inadequate for our blockchain approach.

Cryptographic algorithms

The cryptology and proof algorithms used to simultaneously ensure the privacy of transactions and data transfers among nodes and their traceability by the authorities are considered as the most important contribution of this project to blockchain ecosystem. As a matter of fact, not only the aforementioned algorithms assure the privacy of transactions, but also the accuracy of encrypted data across nodes can be validated by the parties. The basic algorithms used in the project, which are highly valid and applicable in the literature, are as follows.

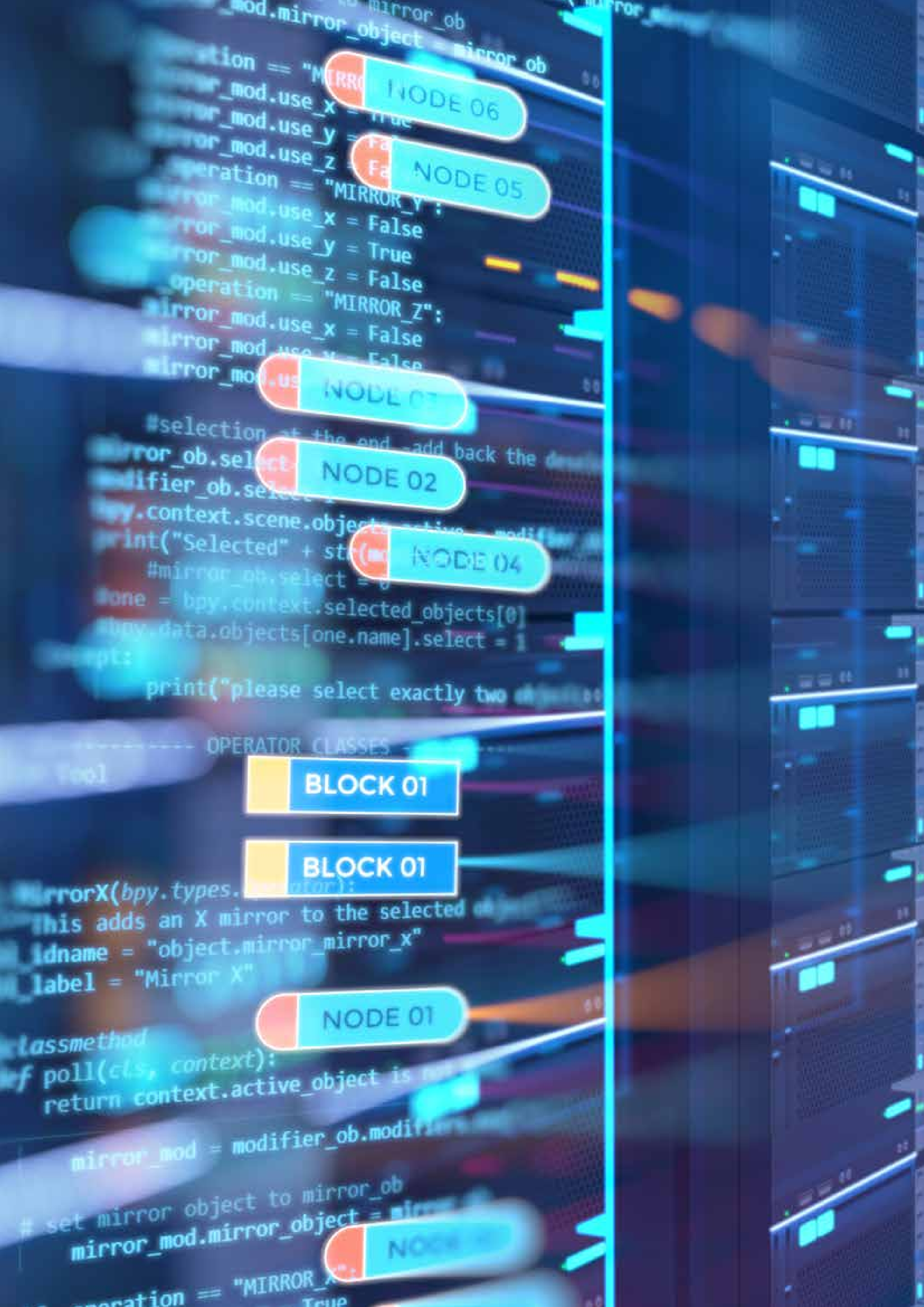
- Homomorphic encryption
- Range proof
- Equality proof
- Diffie Hellman proof
- ECDSA (Elliptic Curve Digital Signature Algorithm)

Blockchain account structures:

Blockchain designs present the structures allowing users to conduct a transaction and to monitor the result and if a transaction is conducted over an asset, the resulting balance of such transaction. They are created with Public and Private key pairs. While public keys allow for conduct of transactions over the network, private keys define the account itself.

Pre-Compiled contracts:

The development of zero-knowledge proof algorithms with intensive mathematical operations on Quorum using Solidity language is not deemed satisfactory in its current state in terms of performance. There are pre-compiled contract structures in Ethereum and Quorum which are used for solving performance-requiring problems and businesses with intensive transaction requirement. In this project, the zero-knowledge proof algorithms are built using pre-compiled contracts. Thus, performance loss is minimized and Quorum platform is forked. These are expected to contribute to the literature with their contents and methodologies.


NODE 06
NODE 05
NODE 02
NODE 04
BLOCK 01
BLOCK 01
NODE 01

BUSINESS OUTPUTS

Businessoutputsaregivenunderthreemain categories as provided below. These are described as transfer of an asset, ensuring business continuity and establishment of a payment system infrastructure.

Asset Transfer

- The end-to-end lifecycle of a digital asset is through digitalization of gold and its addition to the system established on the blockchain network and execution of its transfer in a secure channel.
- Every transaction conducted on existing blockchain networks can either be viewed by anyone or cannot be viewed at all. An encrypted transaction network is established using the zero-knowledge algorithms studied in BiGA Project. This structure is designed in a manner ensuring that nobody could view the transactions except for the sender and receiver of such transactions, that the nodes could approve or reject all transactions without viewing their contents, and that the nodes identified as authority in the system could view the contents of all transactions at

any time desired. This feature positively differentiates BiGA from all known blockchain solutions. Thus, the feasibility for establishment of infrastructures necessary for widespread deployment of blockchain-based financial solutions is demonstrated.

- BiGA has a parametric design that allows for the transfer of any digital asset. Therefore, this asset transfer infrastructure established also allows for digitalization and transfer of any assets other than gold. From this aspect, BiGA has proved that alternative financial structures could be extensively deployed through a single blockchain infrastructure.

Business Continuity

- One of the most important properties brought by the blockchain technology is that the database is simultaneously the same in all nodes. Therefore, due to instantaneous reconciliation made on the system established as such, the system can run on a 7-day/24-hour basis without interruption.

- The system can continue to run over the other nodes of the blockchain network even if any node on the blockchain network becomes inaccessible. When the inaccessible node is included in the network again, it automatically retrieves and reaches the same level of knowledge with the other stakeholders on the network.

- The fact that the database is simultaneously the same in all nodes eliminates the state of a single point of failure. Companies may conduct their activities without considering the scenarios such as operation of the system with backup/redundancy or disaster recovery, etc. This offers serious benefits in terms of both business continuity and costs.

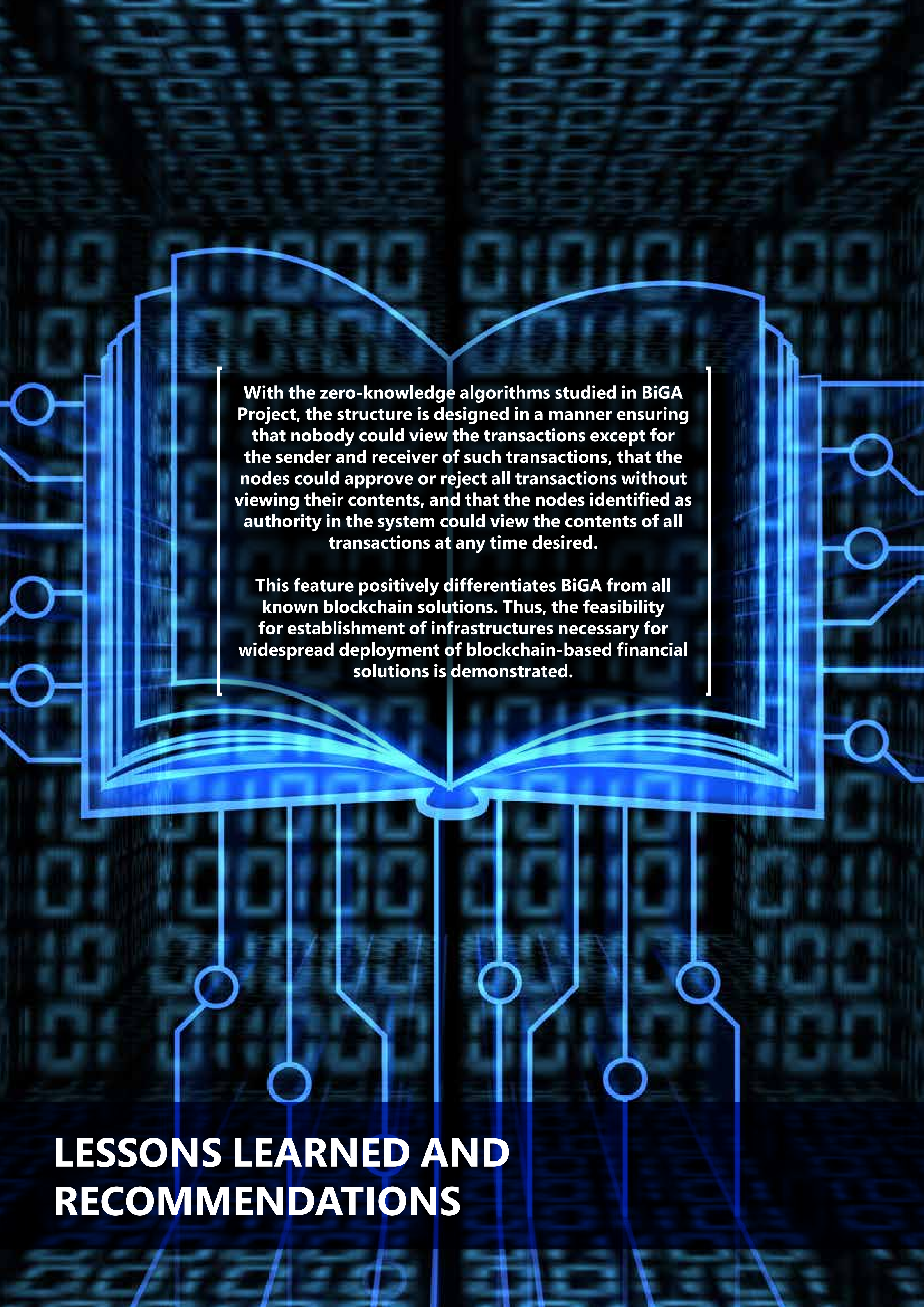
Payment System Infrastructure

- Gold Transfer System has person-to-person transfer feature are expected to mobilize gold. It is targeted to further increase the mobilization of gold with BiGA.

- Thanks to the blockchain approach and digital asset transfer system infrastructure, it allows for transformation of gold into a digital payment instrument.

- The nodes to be added to the system are each planned to be financial institution. The integration of such institutions with and their exit from the system can be realized very quickly through installation automations developed.

- It is ensured that the customized reports can be arranged independently of any institution since all data are given to the user. Thus, the dependencies suffered by the institutions in relation to such reporting are minimized.



With the zero-knowledge algorithms studied in BiGA Project, the structure is designed in a manner ensuring that nobody could view the transactions except for the sender and receiver of such transactions, that the nodes could approve or reject all transactions without viewing their contents, and that the nodes identified as authority in the system could view the contents of all transactions at any time desired.

This feature positively differentiates BiGA from all known blockchain solutions. Thus, the feasibility for establishment of infrastructures necessary for widespread deployment of blockchain-based financial solutions is demonstrated.

LESSONS LEARNED AND RECOMMENDATIONS

Blockchain is an approach closely followed up with a limited number of concrete examples and the impacts of which are unknown in the fullest sense. Many researchers and institutions are willing to conduct studies on this matter that need many different technical data, knowledge and skills in addition to the blockchain approach. This enables the review of the subject through establishment of project groups by creating interdisciplinary synergy rather than merely conducting personal studies. In fact, it is also difficult to research, learn, and develop different issues such as advanced mathematics, developing, new-generation software languages, application virtualization, etc. in the same project. Considering this situation together with the fact that the blockchain approach is yet on the bottom rung of the latter; the findings that especially stand out include the insufficiency of the documents that can be read as references; the lack of stable versions for the frameworks and platforms developed; the lack of desired level of maturity for the additional technologies facilitating the usage of platforms; and the inadequacy of the number of projects and project documents that can be taken as reference; etc.

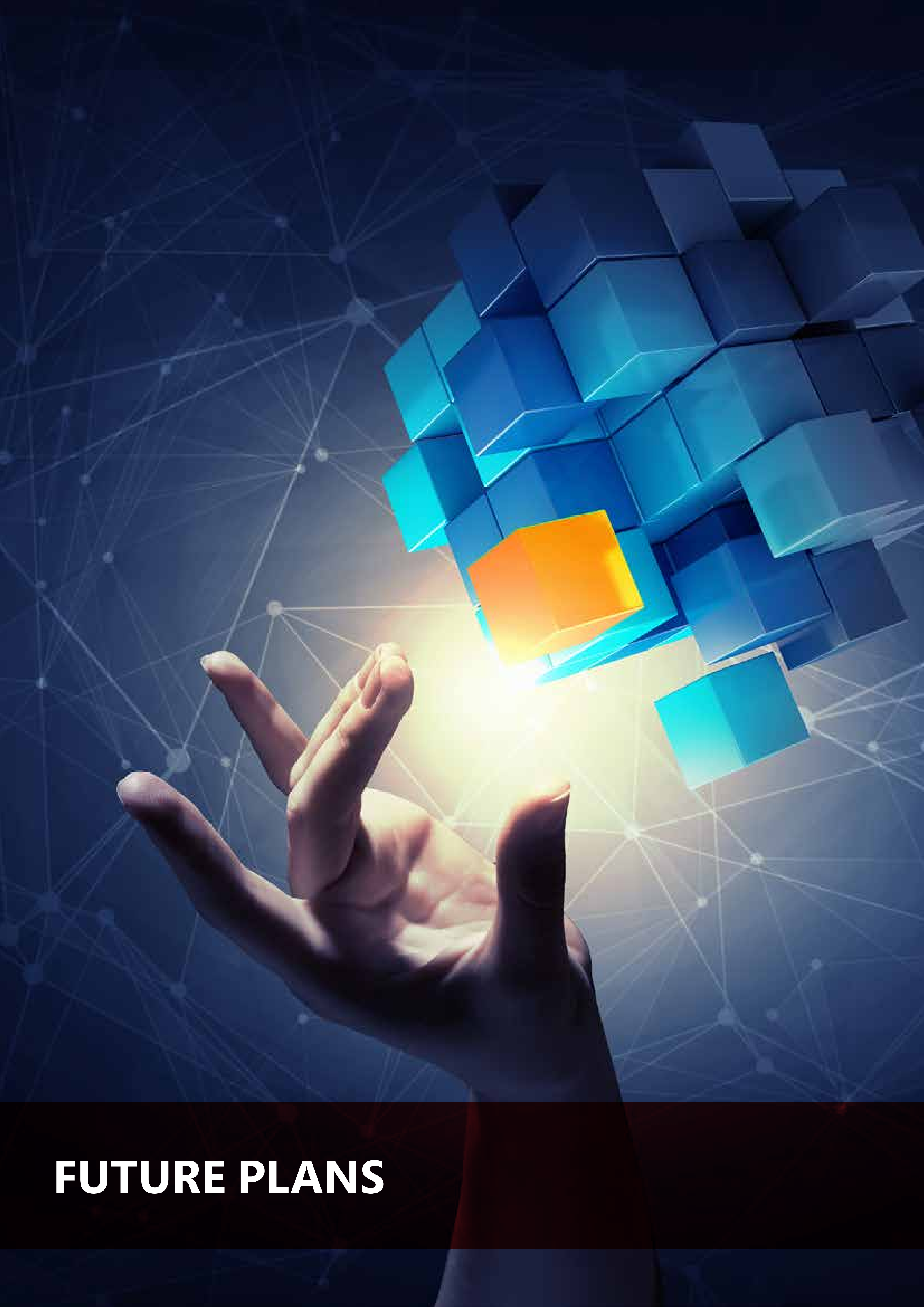
Since software development environments and tools currently used are developed considering requirements in the conventional architectures; the performance or the intention to perform developments and debugging and tests using the same tools and methods further complicate studies. Exhaustive efforts are needed for installation of an environment even for a simple debugging process.

In this context, for entrepreneurs willing to deal with this issue from another point of view, we recommend that such type of third-party studies and activities related with development, packing, testing, debugging, deployment tools and technologies should be performed.

It stands out as an important detail that a project of R&D nature with many uncertainties and restraints should not be designed and configured in standard corporate information technologies infrastructures under any circumstances. In fact, it is required to show utmost efforts in order to stabilize the development and testing environments in the information technologies structures like banking, where information security policies are implemented at the highest level. Instead, the provision of the entire development environment including developer computers in a completely isolated environment is crucial for the project schedule and success. Cloud environments can be considered as a good alternative for such studies.

Apart from its technical restrictions, it takes time to properly understand the alternatives brought by the blockchain approach to the conventional perspectives and its somehow destructive effect. In fact, all stakeholders and participants may ask each other the question of why we are not doing it with traditional methods.

In addition, similar questions may be frequently encountered while the project is explained to third parties. As an institution, we define blockchain as an approach, a philosophy, rather than considering it as a technology.



FUTURE PLANS

Phase-1 of the project is completed with lessons learned and recommendations for the future studies. In Phase-2 of the Project, it is aimed to allow the end users to conduct the transactions over BiGA platform via the banks. In this context, it is planned to continue studies on the headings specified below.

Changing the Zero-Knowledge Proof Algorithm

The cryptologic algorithms that are currently used have some restrictions. These restrictions should be eliminated especially when we want to use this infrastructure for other assets even though it meets adequate requirements for transfer of gold. The transaction is conducted within a period of nearly 3 seconds in a space of 2^{32}. The transaction time increases logarithmically when the space is increased. The goal here is to ensure that the transactions can be conducted in 1 second in a space of 2^{64}

.

The size of a transactions covers nearly 30 kB in the current transaction structure. The transaction size is aimed to be 1 kB as a result of improvement of cryptologic algorithms to be used.

In addition, the maximum amount that can be transferred may be 2^{32} in size depending on the space under the current conditions. The maximum amount that can be transferred will be increased when the space is 2^{64}.

Removal of the Quorum Maker dependency

It is aimed to eliminate the dependency on the Quorum Maker tool used as a supporting solution in order to rapidly activate the blockchain network to be established in the Project.

Changing the consensus algorithm

It is planned to change the RAFT algorithm currently used in the Project as IBFT (Istanbul Byzantine Fault Tolerance) in order to correct the deficiencies identified.

Secret key recovery scenarios

A business model will be developed for the recovery of secret keys in case of loss of such keys to be used by the related parties due to high security requirements of the blockchain solution. The fact that Takasbank is authorized for custody banking and has adequate business knowledge in this field provides an important advantage for the development of the required business model.

Concealment of the parties involved in transfer

In the transactions currently conducted, the contents of transactions are concealed with cryptologic algorithms. The public keys representing the identities of the parties to transactions are currently visible. The public keys will also be hidden with an additional development to be made.

Updateable smart contract

As required by the fundamental operating principles of the blockchain, it is essential that the content of a block generated should not be changed. However, it is required that especially smart contracts should be updated in time considering the potential business requirements. In this context, studies will be conducted on updating of smart contracts without any distortion in the consistency of data between the blocks.

Development with Hyperledger Fabric Platform

It is planned to make developments with alternative blockchain platforms in order to have a higher performance in BiGA platform. In this context, the current transaction structure and the modified zero-knowledge transaction structure will also be developed with Hyperledger Fabric platform.

Know Your Customer studies

The accounts to be used on the blockchain are created by the institutions under the current structure. The reason to this is the requirement to know the actual identity of the account holders on the blockchain platform. Since identity details are received from the institutions after they are approved, this obligation is on the account of institutions. It is planned that in the upcoming periods, a digital

identity platform through which identity details can be approved independently from the institutions will be developed and thus, dependency on institutions will be minimized and that personal users can manage their own accounts.

Wallet application for personal use

In the following phases, after ensuring that personal users can conduct their transactions on their own, it is planned to develop a mobile wallet that will allow individuals to use the system more comfortably.

Evaluation of some extreme scenarios

- Studies to be conducted for the business model and technical solution regarding the actions to be taken in case of loss of secret/private keys
- Working on preventive solutions against the possible scenario of hijack of specially authorized accounts by malicious parties;
- Working on the actions to be taken in case n nodes maliciously act against the consensus on a network with n nodes;

The headings listed above are considered as the issues to be dealt within the new projects in the upcoming period.

CONCLUSION

The blockchain that made its debut for the first time in 2008 has become popular after overvaluations in cryptocurrencies that have occurred in 2017. The studies for usage of blockchain in corporate life have also started in the same period. The fact that this research process that we, as Takasbank, actively started in 2016 has reached to this point with a concrete project is considered as an important milestone. It is expected to put forward the idea of developing a project after individuals and entities conduct some literature researches and follow up the breaking news in this field. However, it is of great importance to determine the correct business scenario and to ensure that the project team focuses on this activity and the senior executives assume a pioneering role in this field on a concurrent basis.

Setting off with the vision of becoming the one that is followed instead of the one that follows the developments on blockchain, Takasbank has completed an R&D project with a high added-value with both its business model and its technical solution.

As with every technology and innovation, understanding the blockchain without conducting R&D projects seem impossible in the short run. At this point, we would like to emphasize the importance for the institutions and entrepreneurs evaluating blockchain to proceed with pilot projects as soon as possible. The importance of teamwork extending from top level to the specialized personnel working on the project, the business unit employees and the external stakeholders stands out as an important factor for the conclusion of the project.

As Takasbank, we are proud that we have led the persons and entities conducting studies on blockchain with our studies that focuses on full privacy and compliance with regulations, which seemed to be the biggest obstacles preventing the usage of this technology in the financial areas.

PROJECT TEAM

Gökhan ELİBOL
Project Sponsor

İlker KUŞCU
IT Director

Nesrin ÖZKURT
Business Unit Director

Mustafa ATAHAN
Project Manager

Faruk Selman LEKESİZ
Project Manager

Mustafa ŞENTÜRK
Software Specialist

Muhammet EVİRGEN
Software Specialist

Ramazan BARDA
Software Specialist

Mustafa KELEŞ
Software Specialist

Elvan SAKANCI
Analyst

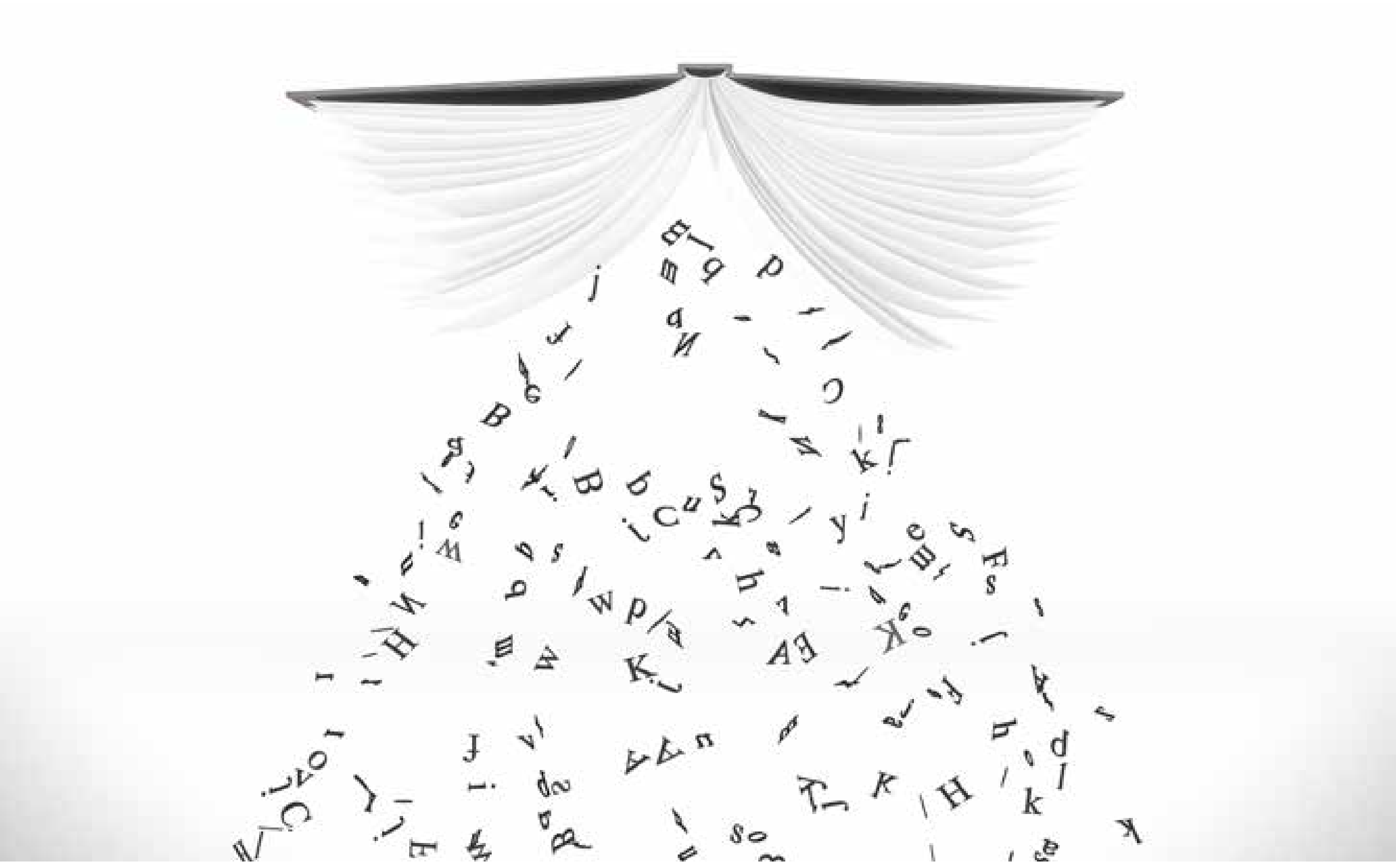
M. Fatih BAYINDIR
Information Security Specialist

Kadir SARI
Infrastructure Specialist

For their valuable contributions in our BiGA Project, we would like to extend our gratitude individually to the **Chairman of the Board of Directors of our Bank** and **Borsa Istanbul General Manager Mr. Mehmet Hakan Atilla** and **the members of our Board of Directors;** to our **Deputy General Manager Mr. Gökhan Elibol;**

to our former senior managers **Mr. Murat Çetinkaya, Mr. Mahmut Kayacık** and **Mr. Ekrem Arıkan** who provided full support from the beginning of the Project; to **BiGA Project Team** and to all our **Takasbank colleagues,** to **Assoc. Prof. Dr. Mehmet Sabır Kiraz** and to **TÜBİTAK BİLGEM Blockchain Laboratory;** to **Assoc. Prof. Dr. Kamer Kaya** from **Sabancı University**; to the distinguished managers and employees of **Albaraka Türk Participation Bank, Garanti BBVA, Kuveyt Türk Participation Bank, Vakıfbank** and **Ziraat Bankası;** and to the **fintech ecosystem** that shared their opinions and technical support with us during the different stages of the project.

Istanbul Takas ve Saklama Bankası A.Ş.



ABBREVIATIONS / TERMS OF GLOSSARY

BFT (Byzantine Fault Tolerance): BFT is a state of distributed information technologies systems in which a system, particularly components of the system may fail and there may be missing information about whether a component is faulty or not. The term is named by a metaphor called as the "Byzantine Generals' Problem". This metaphor means that actors must reach a consensus on the common strategy in order to prevent the failure of the system that may cause a disaster; however, some actors are not trustworthy. In BFT, a component like a server may display different symptoms to different observers, thus appear to be inconsistent by being both faulty and appearing to be operational in the troubleshooting systems. It is difficult for the other components to declare that the component that appears to be inconsistent has failed and to remove it from the network; because they must first reach a consensus on the component that has failed. The BFT is the reliability of a fault-tolerant computer systems against such conditions.

BiGA: The value of 1-gram 995/1000 pure LBMA-compliant gold on the Blockchain platform. 1-BiGA equivalent to 1-gram gold.

BiGA Project: Means all studies and activities conducted for the development of BiGA Blockchain platform.

BiST: Borsa İstanbul (Istanbul Stock Exchange)

Blockchain: A continuously growing distributed database that was firstly introduced by Bitcoin, in which records are linked to each other using cryptographic elements. The records in this database are packaged as blocks and linked with the summary values of the blocks that precede them in order to be protected against alteration.

Confirmation: The act of approval of a transaction by a Blockchain network. This operation is done through mining on some Blockchain networks.

Consensus Algorithm: Consensus algorithm means the protocols proposed for resolution of a problem of reaching a consensus in computer science.

Consensus Process: The steps that a group of peers take to reach a consensus about the content on a distributed ledger.

Dematerialization: Conversion of a physical asset into a digital asset.

Digital Commodity: A non-physical commodity with a market value that can be transferred electronically and is limited in quantity.

Digital Identity: An identity that allows a person, organization or an electronic device to be recognized in a network.

Docker: A computer program realizing virtualization at operating system level that is also known as 'containerization'. It was firstly released in 2013 and developed by Docker, Inc.

EFT: Electronic Fund Transfer

Fork/Forking: Modifications made in the blockchain protocols in order to protect the blockchain history, to prevent inconsistencies or to add new features.

Distributed Ledger: A type of database with its copies stored and spread across different servers, different countries or different institutions. Records constantly grow as they are added and stored one after another.

Fungible Custody: The type of custody service in which an asset stored is stored jointly with the assets of the same properties and any asset from the shared area is returned in case of a refund.

GTS: Gold Transfer System

Issue / Issuance: The conversion of dematerialized gold in the GTS system to BiGAs.

LBMA: London Bullion Market Association

Node, Peer: A computer connected to the blockchain network.

Permissioned Blockchain: The Permissioned Blockchain uses an access control layer to manage those that have access to the network. Unlike public blockchain networks, the endorsers on the blockchain networks are reviewed by the network owner. They do not trust anonymous nodes for verification of transactions or they do not benefit from the network effect.

Quorum Maker: Quorum Maker is a tool allowing users to establish and manage a Quorum network. Manual arrangement of configuration files and generation of nodes is a slow operation and open to errors. Quorum Maker can create any number of different configuration nodes dynamically with reduced user logins. It provides a wizard-like interface with a series of questions that will direct the user while creating nodes with this tool.

RAFT: RAFT is a consensus algorithm designed as an alternative to Paxos. It was aimed to be more comprehensible than Paxos through development of a different logic; but it was proved that it was secure and it offered some additional features. RAFT offers a general path for distribution of a state machine in a group of computer systems and ensures that each node in the group reach a consensus on the same state transition series. There are many open-source reference applications in addition to the applications completely developed with Go, C ++, Java and Scala.

Redeem: The conversion of BiGA balance on the blockchain system into dematerialized gold balance in the GTS system.

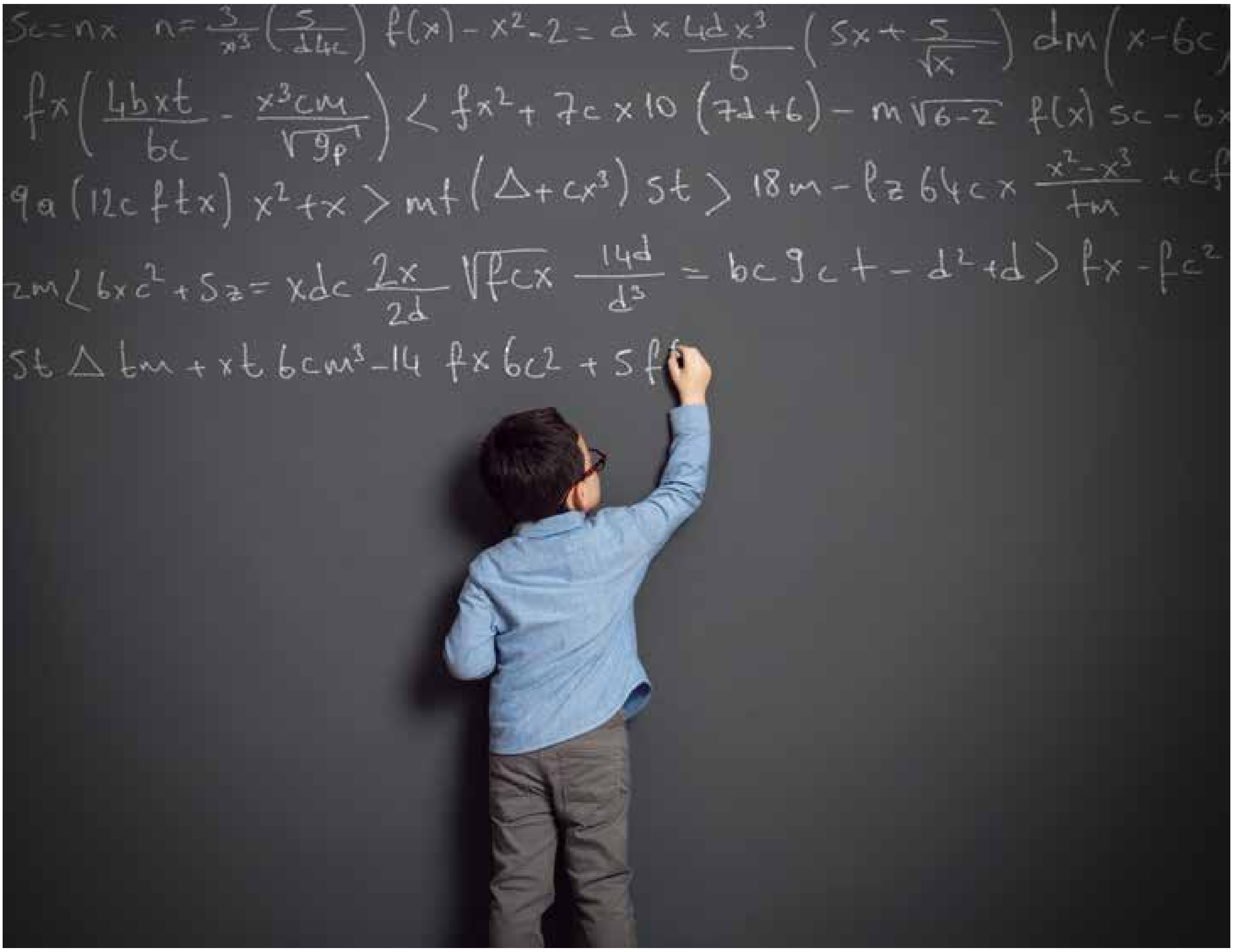
Smart Contracts: The contracts written in a programming language. Smart contracts can be executed automatically and perform transactions on distributed ledger structures.

Stable Coin: Digital currencies indexed against an asset with a fixed value.

Token: Digital assets that can be owned.

Transaction Block: A set of sequential transactions that aggregate a certain number of transactions and that are added to the Blockchain as a summary.

Wallet: The structure that stores the private key of the owner.



APPENDICES

Appendix A

Zero-Knowledge Proofs

Let $\mathbf{\Sigma} = \{0,1\}$. Let L be a language. Recall $\mathbf{L} \in \mathbf{NP}$ means that there exist a deterministic algorithm $\mathbf{V} : \mathbf{\Sigma^* \; x \; \Sigma^*} \rightarrow \{0,1\}$ and that $\mathbf{x} \in \mathbf{L}$ means that there exist $\mathbf{P} \in \mathbf{\Sigma^*}$ such that $\mathbf{V(x,P)} = 1$ with **/P/ < poly(/x/)**. We say that **P** is a short proof that $\mathbf{x} \in \mathbf{L}$.

If **V** is randomized, then we have the MA complexity class. If **V** can interact with **P**, then we get **IP** (interactive proofs). It turns out that **IP = PSPACE**.

Zero-Knowledge Proof Systems

The goal is to prove a statement without revealing extra information for some **N** and **x**, prove **x** is a quadratic residue in $\mathbf{Z}^*_{\mathbf{N}}$.

Let $\mathbf{L} \subseteq \Sigma^*$. For **L**, the zero-knowledge proof system L(P,V)is a pair:

1. (**Completeness**) is verifier for all $\mathbf{x} \in \mathbf{L}$ and says **"yes"** after interacting with the prover.
2. (**Soundness**) is a verifier for all $\mathbf{x} \notin \mathbf{L}$ and all **P*** providers and says **"no"** after interacting with a probability of **1/2**.
3. (**Zero Knowledge**) For all **V*** verifiers, there is the simulator **S*** that is a random polynomial time algorithm as with all $\mathbf{x} \in \mathbf{L}$.

$$\{\mathbf{transcript}((\mathbf{P},\mathbf{V}^*)(\mathbf{x}))\} = \{\mathbf{S}^*(\mathbf{x})\} \tag{1}$$

+ (equality of distributions) is ensured.

In case of existence of a simulator (if $\mathbf{x} \in \mathbf{L}$, then), it indicates that **V*** cannot learn more than the fact $\mathbf{x} \in \mathbf{L}$.

Example: Let there be $\mathbf{N = pq, x \in Z^*_N}$. Let's say that we wish to prove that **x** is a quadratic residue in $\mathbf{Z^*_N}$. Let it be $\mathbf{x} = \alpha^2$ **(modulo N)**.

- P: $\mathbf{r} \leftarrow \mathbf{Z_N}$, sends $\alpha = r^2$.
- V: sends $\mathbf{b} \leftarrow \{0,1\}$.
- P: sends $\mathbf{z} = \mathbf{r}\alpha^{\mathbf{b}}$.
- V: tests $\mathbf{z}^2 = \alpha\mathbf{x}^{\mathbf{b}}$. If equal, it yields the output "yes", otherwise it yields the output "no".

The completeness of this design is immediate. As for soundness, if α is not a quadratic residue, then the verifier says **“no”** with a probability of at least **1/2** (i.e. if $\mathbf{b = 0}$). If α is a quadratic residue, but not x; then the verifier says **“no”** with a probability of at least **1/2** (e.g. if $\mathbf{b = 1}$).

Claim: If x is not a quadratic residue of $\mathbf{Z}^*_{\mathbf{N}}$; then **V** says **“no”** with a probability of at least 1/2 for all $\mathbf{P}^*$.

Then it remains to exhibits that the scheme is a perfect zero knowledge. Let $\mathbf{V}^*$ be a verifier and suppose $\mathbf{\{transcript(P,V^*)(N,x)\} = \{S^*(N,x)\}}$.

A black-box simulator $\mathbf{S}^*$ is created as follows:

1. Select a random $\mathbf{z}_N \leftarrow \mathbf{Z}^*_{\mathbf{N}}$ and select a random $\mathbf{b} \leftarrow \mathbf{\{0,1\}}$.
2. Set $\boldsymbol{\alpha} = \mathbf{z^2/x^b \text{ mod } N}$.
3. Calculate $\mathbf{V^*(x)}$ and give the first message from the prover.
4. V^* removes one *b* from $\{0,1\}$. If $b \neq b^1$,proceed with step 1; otherwise, the output **[a,b,z]** is given as transcript. This is achieved with two iterations on average.

Claim: $\mathbf{\{transcript(P,V^*)(N,x)\} = \{S^*(N,x)\}}$ **(equality of distributions).**

Sketch of proof: Since **x** is a quadratic residue, α is a uniform quadratic residue within $\mathbf{Z}^*_{\mathbf{N}}$. *b* has the same distribution produced by $\mathbf{V}^*$ when α is known. It ensures the equation $\mathbf{z, z^2 = \alpha x^b}$.

Soundness is improved through repetition of the protocol. This repetition is made as follows:

- P: $\mathbf{r_1,\dots,r_n} \leftarrow \mathbf{Z_N}$, sends $\boldsymbol{\alpha_1} = \mathbf{r^2_1,\dots,}\ \boldsymbol{\alpha_n} = \mathbf{r^2_n}$

- V: sends $\mathbf{b_1,\dots,b_n} \leftarrow \mathbf{\{0,1\}}$,

- P: sends $\mathbf{z_1 = r_1\alpha^b_1,\dots,\ z_n = r_n\alpha^b_n}$

- V: tests the equality of $\mathbf{z^2_i = a_i x^b_i}$ for $\mathbf{i = 1, \dots, n}$. If so, it yields the output **“yes”**, otherwise, it yields the output **“no”**.

We have shown the "completeness" and "soundness" states of this scheme; however, it is still uncertain what kind of a simulator it will create. (We can guess that all b_i are correct with a probability of $\mathbf{1/2^n}$ only.)

Theorem: If **L** has a three-round perfect zero-knowledge proof with a negligible probability of cheating, then **L ∈ BPP**.

Since quadratic residue does not exist in **BPP**, it is considered that quadratic residue state does not constitute a three-round perfect zero-knowledge protocol.

Hence, we see a weaker version of zero knowledge:

Algebraic Zero Knowledge: For a language **L**, (P,V) is a (t, ∈) – zero-knowledge proof system if the following conditions are met:

1. **Soundness**
2. **Completeness**
3. **Algebraic ZK**: Let there be a simulator like $\mathbf{S}^*$ for all **x ∈ L** states for all verifiers $\mathbf{V}^*$; the distribution $\mathbf{\{transcript((P,V^*)(x))\}}$ is indistinguishable from $\mathbf{\{S^*(x)\}}$.

Theorem: If there is a (t,∈)-bit commitment draft, all languages in NP have computable ZK proofs.

Definition: (imprecise definition) (t,∈)-bit commitment design is defined as follows:

1. The committer has the commitment b $\in\{0,1\}$ and sends *commit*(*b*) $\in \{0,1\}$ bit (the bit committing to the bit *b*).
2. The contractor may open the commitment as b^1 and the verifier can check that $b = b^1$.

This scheme must be as shown below:

- **Binding:** An infinitely strong committer cannot convince the verifier that the commitment is a commitment for $b \neq b^1$.
- **Sound: commit(b)** does not provide any information about b. In other words, in case of any bit b $\in \{0, 1\}$, $\{\mathbf{commit(b), b}\}$, and $(t, \in)$- is indistinguishable from $\{\mathbf{commit(b), r|r \leftarrow \{0, 1\}}\}$.

For example: One-way permutations mean commitment schemes:
Let $\mathbf{f : \{0, 1\}^n \rightarrow \{0, 1\}^n}$ be a one-way permutation. Select $\mathbf{r} \leftarrow \mathbf{\{0, 1\}^n}$ and let $\mathbf{commit(b) = [f(r), B(r) \oplus b]}$; here, **B** is a central bit of **f**.

Appendix B

Homomorphic Encryption

In abstract algebra, homomorphism is a map protecting the structure between two algebraic structures like groups.

Group G can be defined as a set through a transaction ◦ combining the members **a** and **b** in order to create another element and can be expressed as $\mathbf{a \circ b}$. In order to characterize it as a group, the set and transaction $(\mathbf{G}, \circ)$ must meet four requirements known as group axioms:

- **Closure**: The result and inputs of the transaction are included in G; in other words, **a, b** and $\mathbf{a \circ b}$ are located in **G**.

- **Associativity**: For all **a, b**, and **c** located in **G**, $\mathbf{(a \circ b) \circ c = a \circ (b \circ c)}$.

- **Identity Element**: There is an element **e** in **G**; therefore, for each element in G, the equality is equalled to $\mathbf{e \circ a = a \circ e = a}$. Each group has only one identity element.

- **Inverse Element**: For each **a** in **G**, there is an element **b** in **G** yielding $\mathbf{a \circ b = b \circ a = e}$; where, **e** is the identity element.

The identity element of the group G is generally written as 1. The result of a transaction may depend on the sequence of the elements processed. In other words, the result of the combining element **a** with the element **b** does not necessarily yield the same result with the combining element **b** with the element **a**; the equation $\mathbf{a} \circ \mathbf{b} = \mathbf{b} \circ \mathbf{a}$ may not necessarily be correct at all times.

This equation always holds for the addition/summation property in the whole numbers group; because for any two whole numbers, $a + b = b + a$ (the commutativity property of addition). The groups that are $a \circ b = b \circ a$, always verifying the commutativity property equation, are called as *abelian* groups.

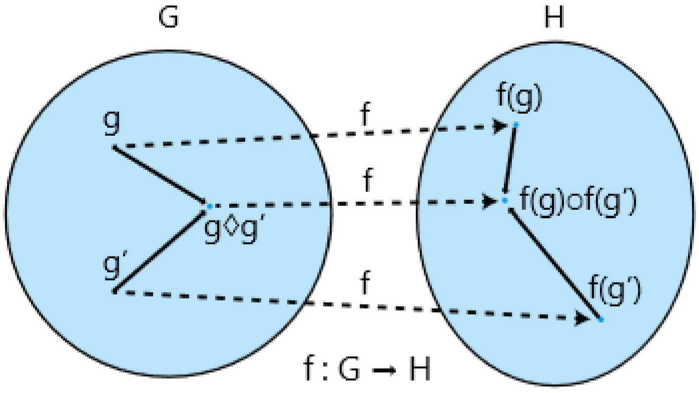


Figure 1: Group Homomorphism

Given two groups $(\mathbf{G,*})$ and $(\mathbf{H,\circ})$, a group homomorphism from the function $(\mathbf{G,*})$ to the function $(\mathbf{H,\circ})$ is $\mathbf{f} : \mathbf{G} \rightarrow \mathbf{H}$; where the following equation is verified for all $\mathbf{g'}$ and $\mathbf{g}$ within $\mathbf{G}$.

$$f(g * g^{\iota}) = f(g) \circ f(\iota^{0})$$

The group homomorphism can be illustrated as shown in Figure 1.

Let (P,C,K,E,D) be an encryption scheme; where **P; C** are the plain text and cipher text fields; **K** is the key space and **E; D** are the encryption and decryption algorithms. Assume that plain texts form a group **(P, *)** and encrypted texts form a group **(C;** ∘); and that the encryption algorithm is a map from the group **E, P** to the group **C**; in other words, $\mathbf{E_k} : \mathbf{P} \rightarrow \mathbf{C}$; where $\mathbf{k} \in \mathbf{K}$ is a secret/private key (in a private key encryption system) or a public key (in a public key encryption system).

For all **a** and **b** in **P** and $\mathbf{k} \in \mathbf{K}$; if

$$\mathbf{E_k(a) \circ E_k(b) = E_k(a*b)} \qquad (2)$$

The encryption scheme is homomorphic.

REFERENCES

[1] TAKASBANK-TÜBİTAK BİLGEM BİGA Cryptographic Architectural Design Özel çalışma (Special case study), 2018

[2] NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system, 2008.

[3] NARULA, N. VASQUEZ, W. VIRZA, M. zkLedger: Privacy-Preserving Auditing for Distributed Ledgers, 2018.

[4] Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., and Capkun, S. Evaluating User Privacy in Bitcoin

[5] RON, D. and SHAMIR, A Quantitative Analysis of the Full Bitcoin Transaction Graph, 2012.

[6] REID, F. HARRIGAN, M. An Analysis of Anonymity in the Bitcoin System, 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing.

[7] ANDROULAKI, E, KARAME, G.O., ROESCHLIN, M., SCHERER, T. and CAPKUN, S. Evaluating User Privacy in Bitcoin.

[8] SPAGNUOLO, M. Thesis: BitIodine: Extracting Intelligence from the Bitcoin Network, 2013 Politecnico di Milano

[9] MEIKLEJOHN, S., POMAROLE, M., JORDAN, G., LEVCHENKO, K., Mccoy, D., VOELKER, G.M., SAVAGE, S. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, 2013

[10] GARMAN, C., GREEN, M., Ian MIERS, I. Accountable Privacy for Decentralized Anonymous Payments, 2016.

[11] BUNZ, B., BOOTLE, J., BONEH, D., POELSTRA, A., WUILLE, P., and MAXWELL, G. Bulletproofs: Short Proofs for Confidential Transactions and More, 2017.

[12] KOENS, T., RAMAEKERS, C., and van WIJK, C. Efficient Zero-Knowledge Range Proofs in Ethereum ING, 2017

[13] Hearn, M.: Merge avoidance: Privacy enhancing techniques in the bitcoin protocol (2013), http://www.coindesk.com/merge-avoidance-privacy-bitcoin/

[14] Wilcox-O'Hearn, Z.: Zcash begins (2016), zCash Blog Post, https://z.cash/blog/zcash-begins.html. Retrieved 2016-10-31.

[15] MA, S., DENG, Y., HE D., ZHANG J., XIE X., An Efficient NIZK Scheme for Privacy-Preserving Transactions over Account-Model Blockchain, 2017

[16] Certicom Research, SEC 2: Recommended Elliptic Curve Domain, Parameters, Standards for Efficient Cryptography, 2010

[17] National Institute of Standards and Technology, FIPS PUB 186-4: Digital signature standard, 2013

[18] Schnorr Non-interactive Zero-Knowledge Proof, Newcastle University, 2017 [18] Ian Miers, Christina Garman, Matthew Green, Rubin, A.D., Zerocoin: Anonymous Distributed E-Cash from Bitcoin, 2013

[19] Koens, T., Ramaekers, C., van Wijk, C., Efficient Zero-Knowledge Range Proofs in Ethereum, ING 2018.

[20] https://crypto.stanford.edu/pbc/notes/crypto/zk.html

[21] Homomorphic Encryption https://www.springer.com/cda/content/document/cda_downloaddocument/9783319122281-c1.pdf?SGWID=0-0-46-1487904-p177033600

TAKAS İSTANBUL

FinTechHub
TAKASİSTANBUL

PHYSICALLY-BACKED GOLD, COMPLIANT WITH REGULATIONS AND OFFERING MAXIMUM PRIVACY AND SECURITY

24h SECURE TRANSFER

TAKAS
İSTANBUL

Takasbank

İstanbul Settlement and Custody Bank Inc.
Reşitpaşa Mahallesi, Borsa İstanbul Caddesi, No: 4 Sarıyer 34467 İstanbul
T +90 212 315 25 25 F +90 212 315 25 26 ats@takasbank.com.tr
www.takasbank.com.tr