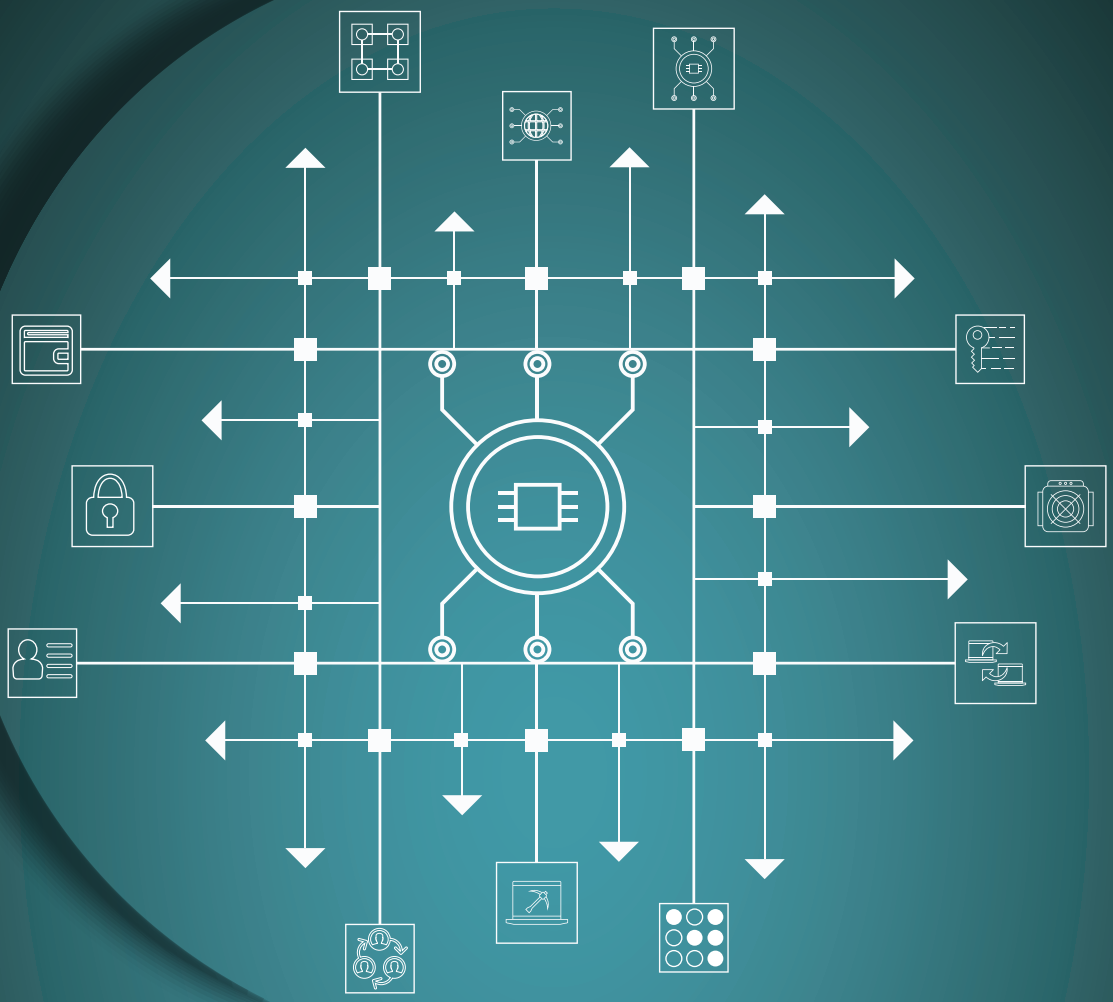
T2 Software, Inc.

B.B.N.

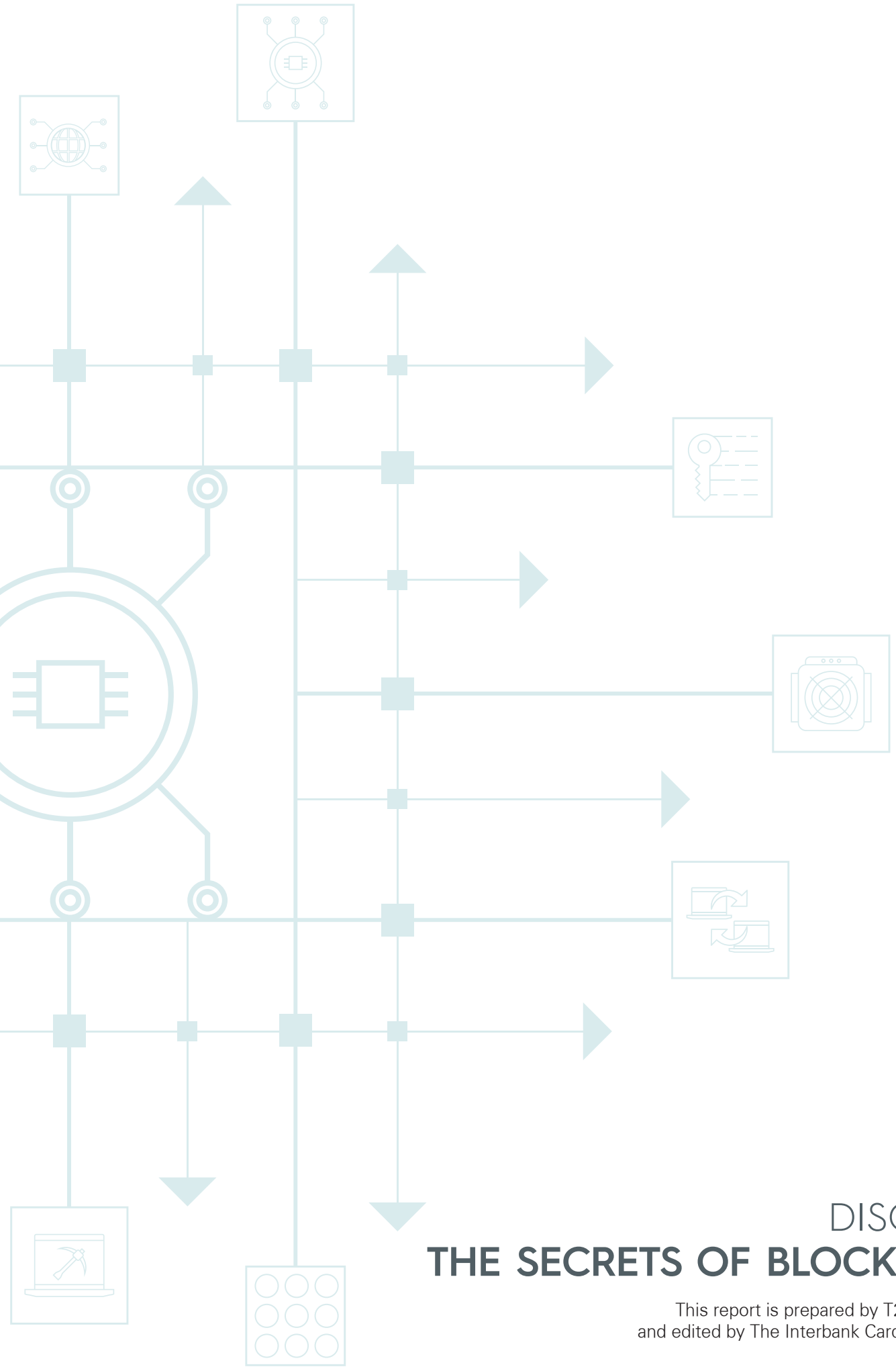
BKM
BANKALARARASI
KART MERKEZİ



DISCOVER:
THE SECRETS OF BLOCKCHAIN

BBN Phase 1

June 2018



DISCOVER:
THE SECRETS OF BLOCKCHAIN

This report is prepared by T2 Software, Inc.
and edited by The Interbank Card Center (BKM).

"In the age of digitalization,
those who are inquisitive, curious and
courageous will always be one step ahead."

Soner Canko, PhD

Foreword

Celal CÜNDOĞLU
The Interbank Card Center
Executive Vice President, IT

Blockchain technology is expected to change the way business is done in many industries, including finance, over the coming years. Following financial technologies closely and working for Turkey to be among the leading countries in this field, the Interbank Card Center is pleased to share with you the first outputs of our BBN application, implemented to see the potential and the shortcomings of blockchain, which is still very much developing. We see our BBN app, created in collaboration with T2 Software, as a valuable tool for illustrating this technology to our stakeholders and envisioning the problems it can be used to solve.

In this report, we share our observations on this technology and our significant findings for the next steps to be taken, now that this first phase of BBN is completed. We hope that our efforts will be beneficial for the people and institutions working on blockchain. We are planning to diversify our work regarding blockchain in the coming period. We will continue to explore whether it is possible to use blockchain technology in our products and services when it reaches adequate maturity.

Mustafa SAKALSIZ
T2 Software, Inc.
Founding Partner, CTO

When we talked about our projects and ideas about blockchain with the Interbank Card Center (BKM), they said that they saw blockchain enough in presentations and they wanted to turn this technology into a reality. They believed that it was time to pursue a blockchain project themselves to experiment with their own usage scenarios and see actual results.

At T2 Software, Inc., we believed that we should definitely be involved in a project planned with this point of view and told the BKM how eager we were to carry out such a project. As one of Turkey's most startup-friendly institutions, the BKM also believed in us and gave us this project.

In four months, we found solutions for many special circumstances, made a series of improvements on an emerging technology, and successfully went live. I would like to thank the T2 Software, Inc. engineers involved in this process for their dedicated work, as well as the BKM Business Development team who developed, tested and defined the project.

In this report, we try to explain the problems we have encountered, our approaches to their solutions, the lessons we have learned and our achievements. I hope that it will be useful for anyone who reads it.

Table of Contents

Executive Summary

The Interbank Card Center (BKM) is one of the institutions that has been closely following blockchain technology, which entered our lives with the article titled "Bitcoin: A Peer-to-Peer Electronic Cash System" by someone with the alias, Satoshi Nakamoto. Since its inception, technology companies and ventures have been building platforms and consortiums for blockchain technology as its potential has been recognized in time. Deciding to undertake a proof-of-concept project in order to see the adequacy of this technology and to ensurea better understanding of it in our country, BKM initiated a digital identity based project.

The main objectives of the project **were to ensure that the technology was understood correctly, to measure the maturity level of the tools involved, to answer the questions in mind and to share within the ecosystem the technology's beneficial ability to solve various business problems.**

We conducted an evaluation based on the information accumulation criteria for developing enterprise blockchain platforms, and we decided that the project should be developed in collaboration with T2 Software, Inc. The application developed in the project, **BBN**, was named after the communication slogan of BKM which translates as **"Bye Bye, Cash."** Through the BBN app, BKM makes it possible for their employees to create digital identities through applications that they can install and use on their mobile devices, save them on the blockchain, earn points for completing tasks, transfer these points to other users, and buy the products in the application's store redeeming their points. **With this set of operations, the concepts of distributed ledger and smart contracts, as well as digital identity have been incorporated.** The loyalty points in the project were set up using cryptocurrency.

This report aims to summarize the results of the first phase of the project, which was carried out in January 2017 using blockchain infrastructure, to share the lessons learned and to give technical information about the project. **The report discusses the advantages provided by the technologies used throughout the project and the difficulties encountered, and it provides information on how those difficulties were overcome.** In the content of the report, there are also inferences on the problems solved by the technology and evaluations of how the blockchain technology needs to evolve in relation to the situations that could not be solved.

In the first phase of Turkey's first blockchain app, BBN, we fulfilled our objective of getting to know the technology better, while reaching **the conclusion that blockchain is not mature enough to be used in large-scale systems.** It is believed that blockchain technology can be successful in a variety of industries, including finance and logistics, if the platforms improve in terms of functionality, consensus diversity, processing speed and capacity, and if ecosystems are created by different institutions in the industry.

In order to closely monitor the maturity of the technology, BKM will continue to run proof-of-concept projects on different blockchain platforms and share the outcomes.

1. The Technical Infrastructure of BBN App

1.1. BBN

BBN, initiated by the Interbank Card Center (BKM), is a company loyalty platform that enables the acquisition and consumption of gifts to engage company employees. Named "Bye Bye, Cash" after the slogan for BKM's communications projects with the vision of cashless payments, BBN intends to test concepts such as digital identity, distributed ledger, smart contracts and consen sus. To increase the number of peers involved in the network, BKM was represented as three separate applications instead of a single app, and the solution partner T2 Software, Inc. was one of the peers that joined the network. In the BBN blockchain network, a special permissioned blockchain infrastructure was preferred. The BBN application in which users can earn loyalty points called "partridge," and spend it in the application's store, was launched at the beginning of 2017. The BKM network completed the first phase at the beginning of 2018 and initiated the second phase.

1.2. The Blockchain Platform

At the beginning of the project, BKM had several options for the platform. Some of these were as follows:

- Hyperledger Fabric
- Ethereum closed-loop testing environment
- NXT
- Blockstack
- R3 Corda
- Hyperledger Sawtooth
- Customized Bitcoin
- A completely customized and new platform to be developed

BBN was launched on version 0.6 of the Hyperledger Fabric platform. In the middle of 2017, with the launching of the Fabric version 1.0, BBN was upgraded to the new version as of the beginning of 2018 and the second phase of the project started.

While choosing between these platforms, they aimed to meet various expectations. Those expectations included:

- A closed-loop system and a structure that requires permission so that only the peers authorized by the BKM would be able join the blockchain network,
- Smart contract support, in order to try out its possibilities,
- A platform with technical competence and support services at the desired level in order to be able to produce quick solutions in the face of possible dilemmas.

As blockchain is an emerging technology, the most important elements needed for quick solutions were the support and the possible solutions to the problems. Therefore, they needed a flexible platform, and as a result they decided to develop BBN on the Hyperledg er Fabric platform. After developing BBN, we observed that Hyperledger Fabric had been preferred in similar projects around the world.

1.3. Top Level Architecture and Technologies

The project is entirely based on open-source technologies:

- Operating system: Linux
- Application server: Payara
- Database server: PostgreSQL
- Blockchain platform: Hyperledger Fabric
- Mobile development platform: React Native
- Container technology: Docker
- Programming languages: Java, Go, JavaScript

Five peers were used in the BBN Phase 1 blockchain network.

Five peers were used in the BBN Phase 1 blockchain network. One of these peers belong to T2 Software, Inc., three belong to BKM (each is positioned as a separate entity / application) and one is the central management layer that does not interact with the end user. Due to the structure of Fabric 0.6, one peer must be defined as the root peer. In BBN, the central management layer (CML) acted as the root peer. The top level architecture of the other four peers and their systems are shown in the Top Level Architecture diagram in Figure 1. Accordingly, each institution in the BBN (BKM2, BKM3, BKM5, T2) has its own application server, database, mobile application and related services. Each institution is represented as a peer in the BBN blockchain network.

In mobile applications, instead of building a separate wallet structure, the system was improved to accommodate digital identity. In wallet structures, users have more responsibilities. Peers constantly have to contact their wallets while transactions are written on the blocks. Therefore, it is expected that those who use a wallet structure will become more informed and advanced users (power users). However, since BBN aimed to observe mostly peer-level transactions, and because Fabric does not offer a good wallet structure, the wallet design was built at the server and peer levels. The ownership issue was solved by digital identity structure. The accounts and transactions of the mobile users are transmitted to the institutional layers via the REST services on the server and are performed by the respective peer on the blockchain.

The developments on the application server, web interface and web services were built using Java 8. The mobile applications were developed in React Native, while the smart contracts on Hyperledger Fabric were developed in Go. Although Hyperledger Fabric allows for the use of other developing languages, the decisive factors for choosing the Go language were that Fabric itself was written in the Go language, the innovations first happen in the Go API, and there was also a need for a proxy structure for other languages. In Figure 1, each color in the Top Level Architecture diagram represents a different institution, and there is no other integration between them apart from blockchain. In addition, a virtual machine with a separate Amazon EC2 for each institution was created and placed in different zones. Thus, an actual network environment has been established. Only the gRPC communication protocol used by Hyperledger Fabric was active among these virtual machines.

Since the application is a closed-loop proof-of-concept project, the cloud environment was chosen to keep the development time short. On the other hand, no personal data is stored on the blockchain network.

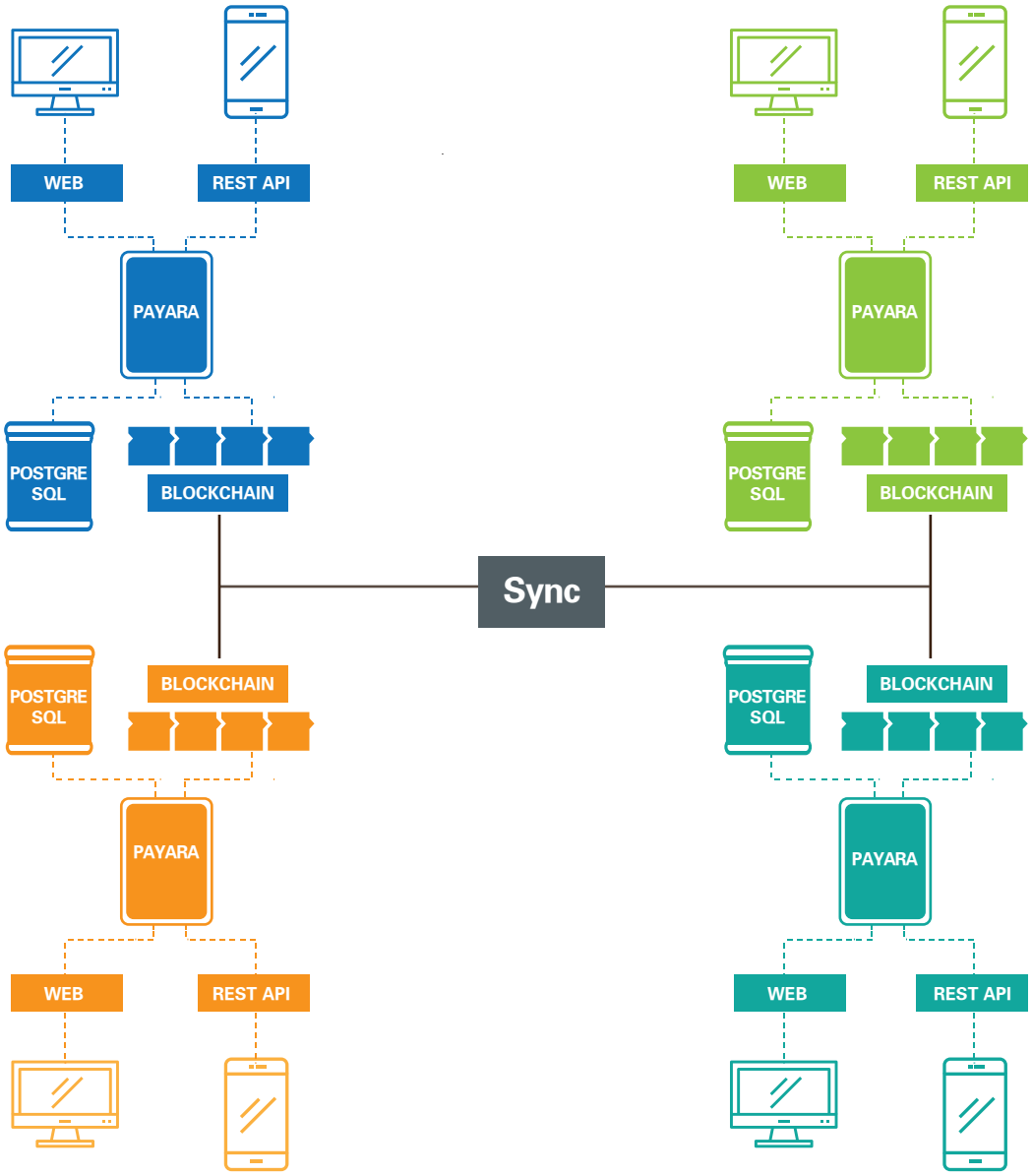


Figure 1: Top Level Architecture Diagram

1.4 Where and How to Use Blockchain

Although BBN has a great amount of information and transaction records, not all of this information is stored on the blockchain. A narrow scope of the critical data was intentionally stored on a blockchain.

Detailed information about which information is stored on which environment, according to the type of transaction and record, is shown on Table 1.

Although BBN has a lot of information and transaction records, not all of this information is stored on the blockchain.

Table 1: Distribution of the Transaction Set and Information Based on Environment

	Mobile Application	Server Database	Blockchain
User Records	Digital Identity	Shared Identity Information	Digital Identity Hash Code
Partridge (Loyalty Point) Account	Digital Identity	Identity Information and User ID Match	User ID and Partridge Account Information
Creating Partridge	-	User and Transaction Information	Partridge Created
Transferring Partridge	Transaction Initiation	User and Transaction Information Records	Transferring with a Smart Contract
Adding Products	-	Product Information (Product name, Description, Value, Photo)	Unique Code Generated For Each Product
Product Purchase	Transaction Initiation	Purchase Records	Trading Product and Partridge with a Smart Contract
User Login	Digital Identity	Verification and Authorization Transactions	-

1.5. Digital Identity and Using Digital Identity with Blockchain

One of the most important use cases of BBN applica tion was digital identity and its verification with block chain. This tested structure is intended to provide a practical use for the Know Your Customer (KYC) process. Since digital identity is private information of the user, the BBN solution is formulated in such a way that a user's identity can only be shared with the desired institution/application with their consent.

Since digital identity is private information of the user, the BBN solution is formulated in such a way that a user's digital identity can only be shared with the desired institution/application with their consent.

According to this, the digital identity is stored in an encrypted form on a site belonging to the user. In BBN, the encrypted digital identities were stored on users' personal mobile phones. When the user registers for the first time with a BBN institution, the institution also performs the verification process for this information. In BBN, this activity flow is designed as follows:

- The user enters their email address, first name, last name and phone number, and adds a selfie to create a digital identity on his/her phone.

- He/she then confirms that they were the one applying to the institution through a verification email.
- The application then shows up on the screen of the institution authority where the application was made.The user's application is verified using the information and selfie provided by the applicant.
- With the confirmation of the authority, the hash code of the digital identity is transferred to the blockchain and the user can access the application of the institution to which he/she has applied.

This structure, which is a simulation on a smaller scale of Customer Verification processes used in the real world, is similar to the way customers verify themselves with documents such as utility bills and proofs of identity when applying to a bank for opening an account. After verification, a hash code of the identity information is created using one-way cryptographic summary functions, which are transferred to the blockchain and shared with the entire network. Thus, the digital identity on the user's mobile phone becomes a confirmed identity. One-way cryptographic summary functions (e.g., SHA-1 and SHA-256) cannot be inverted or accessed again from the hash code. Therefore, this guarantees that no private information belonging to the user is stored on the blockchain and no user data is shared among the institutions. BBN has provided a structure in which a digital user does not have to go through the same verification process again when he wants to register with another organization on the same network. If the user consents to sharing their information with the institution to which they want to register, they can apply to other institutions by sharing the identity information stored on their phone.

After verification, a hash code of the identity information is created using one-way cryptographic summary functions, which are transferred to the blockchain and shared with the entire network. Thus, the user's digital identity on the phone has become a confirmed identity

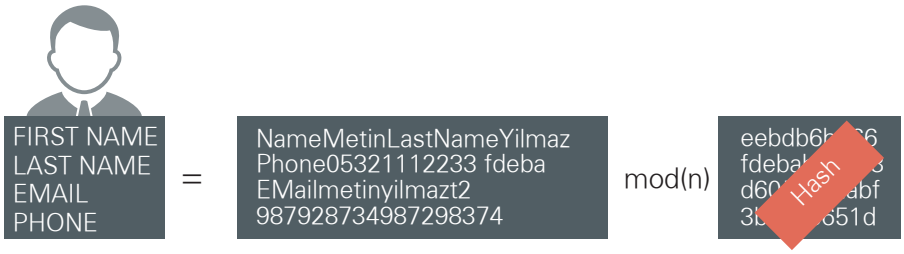


Figure 2: Digital Identity Hash Code Generation

1.6. Recovering Digital Identity

Initiative granted to users may cause situations where disaster recovery scenarios have to be implemented.For example, the options to store or share digital identities is directly up to the user in the BBN application. In this configuration, losing or changing the mobile phone, or forgetting the password for the encrypted identity might prevent the user from accessing all of their assets. Although there are organizations that provide hardware-based custody services for storing such data, BKM developed a simple and useful approach, taking into consideration that there should be a distributed solution to this issue within the system of a blockchain project. Accordingly, the problem was solved by enabling the user to share their identity and the hidden identity key on the blockchain with selected peers on the network and recover their information from these institutions when necessary. However, since it would constitute a security risk if the institutions had access to users' complete digital identities, the data sent to the institutions had to be scrambled so as to be rendered unintelligible to the peers. Therefore, a structure through which the digital identity could be recovered with fragmented codes from two separate peers was created.

2. Lessons Learned

2.1. Hyperledger Fabric 0.6

2.1.1. Unchangeable Smart Contract Structure

We can say that Fabric 0.6 is an "intermediate development version of Fabric." Some concepts in Fabric were considered for trial purposes only. For example, a simple table structure was provided in which smart contracts could be used to facilitate development. However, in the records pulled from the table, an arrangement was made so that only 100 records could be retrieved from the system's memory for the function that puts the rows in order to avoid performance problems. This value might be sufficient for test projects that do not involve too much processing, but it won't suffice for applications operating on a similar scale to BBN with about 150 people. Increasing this number would also be a temporary solution. For that reason, a different navigation structure for the records was constructed for BBN. Because a new function that allows the corresponding smart contract to receive as much data as desired was developed, the existing smart contracts were updated to use this new function.

We can say that Fabric 0.6 is an "intermediate development version of Fabric."

The smart contract structure of Fabric 0.6 is designed not to be altered. If smart contracts are modified after they are deployed in the system, the system perceives them as a completely new structure and cannot access the existing data. Error correction upgrades that do not change the overall structure of the system act in the same way, which is disadvantageous. As a matter of fact, when updating the GetRows function in Fabric 0.6 API in order to solve the problem of bringing more than 100 lines into BBN, we had to upgrade the API. Along with the change in API, the smart contracts also changed, and all of the history was lost in the newly created system. To solve this issue, Fabric 0.6 code had to be modified.

Given all the above, we can emphasize that in Fabric, we need to design and test the smart contracts very carefully before uploading them.

2.1.2. Synchronization Problem

In Fabric 0.6, when a peer collapsed, it was not possible to synchronize the blocks or transactions that occurred from another peer when it was reconnected to the corresponding peer chain network after there was a temporary break in one of the peers. This led to different results being created in different peers. This problem prevented the operation of a healthy consensus structure. This is because when the peers have differentiated data in the consensus structure to be designed, the record to be added would not be able to provide the same integrity in every peer. **For this reason, instead of a consensus structure that preserves the integrity of the data in BBN,a simpler structure was designed.** As the number of records are higher in peers that interact more with the user, the risk of encountering a problem and losing synchronization becomes higher as these interactions increase. For this reason, it is helpful to include some peers that do not interact with users in the system in order to keep the longest chain alive. **In this sense, the central management layer, which does not interact with the users in BBN, has played an important role in ensuring synchronization after breaks occur.** In Fabric 0.6, a manual intervention was required for the re-synchronization of the collapsed peers from the longest chain, and Fabric does not offer a ready tool to solve this problem. Moving data from one peer to the others does not help to solve this problem either. The solution involved developing an application that reconfigures the settings in the peer's database.

2.1.3. Performance

In the first phase, there were no performance problems in the system because a very simple consensus algorithm was used and the number of peers was small. The performance was comprised of four transactions per second. The blocks were added at a very high rate due to the fact that Fabric 0.6 does not take synchronicity between peers much into account. If the peer number increases and the consensus algorithm becomes complicated (if the need for synchronization increases), a decrease in the rate at which the blocks are added may be expected. **In this case, the block will have to be kept in a pool before being added, as in bitcoin. It will be necessary to create a verification system afterwards. This structure is present in Fabric version 1.0.**

2.2. The Need for External Consensus

When we look at the blockchain use cases, we see that there are some assumptions that are not very realistic at this point. The most common assumption is that all assets traded on blockchain are digital and represented on the blockchain in reality. For example, the idea that swapping can be done seamlessly in deed or vehicle title transactions is based on the assumption that title deeds, vehicle licenses and money are assets that exist on a blockchain completely. If this were the case, the money that is stored on the same block would be simultaneously transferred from the other party's account to our own through a smart contract when the title deed was transferred.

Beyond the digital representation of assets, there are a lot of scenarios for which large-scale data must be stored on a blockchain. For example, it is expected that certain compromises in the areas of the Internet of Things (IoT) and insurance can be completed swiftly, as soon as the preconditions defined in a smart contract are fulfilled. If we elaborate on this example, with IoT, devices can now generate data and complete certain operations. Some of these transactions will require various payment and settlement steps. Imagine that you produce electricity at home and feed it back into the electrical grid. In this scenario, smart contracts in blockchain can be used. For insurance businesses, agricultural insurance is a good example. Assume that your crops are damaged due to adverse weather conditions. The damage will be verified through the system according to the region and weather conditions and after the confirmation is completed via satellite images, smart contracts will compensate the insurance holder for the losses. Large-scale data can be analyzed this way and smart contracts that can make complex decisions can be designed. However, in blockchain systems with smart contracts, a test is performed on new registers in order to see if the register can be attached or not, due to the possibility that it might be vetoed by the smart contract. This process is performed by all members in the blockchain network who participate in the consensus process. Therefore, the smarter the contracts are and the larger the set of data they are based on, the slower the performance of attaching new registers becomes.

The smarter our contracts are and the larger the set of data they are based on is, the slower the performance of attaching new registers becomes.

Recently, blockchain applications and tokens that are backed by physical commodities have become very popular. Creating tokens on blockchain systems is a simple process that is completely digital. However, the claim that this token or the digital assethas a physical counterpart involves some external control mechanisms outside of blockchain. Consequently, the supervision of the physical asset during the registration of a new asset to the system cannot be done by smart contracts.

Moreover, in some cases, there are many consensus steps that require human experience and decision-making. For example, the production of partridge in the BBN application takes place through the initiative of BKM, as the solution is a closed-loop proof-of-concept project. The smart contract structure in the partridge production allows an partridge production at will as long as it is produced by means of a special peer owned by the BKM.

In BBN's second phase running onFabric 1.0, an external consensus feature was added to the partridge production phase and self-regulation of the system was improved by searching for the consensus of more than half of the peers in partridge production.

Here, unlike the consensus during block-building, a totally asynchronous and external reconciliation structure was designed. As these two consensus structures can work together, it is easier to realize these scenarios in real life. Instances such as commodity provision checks and special conditions in reconciliation can prevent the establishment of an automatic reconciliation structure in blockchain. This even prevents many popular scenarios from being realized in blockchain. Thus, the need for a secondary consensus step structure, which is not done automatically but does not require the entire system to be blocked, has arisen. In other words, **if consensus steps can be added to the system that can be fed either manually or externally, the number and scope of scenarios that we can achieve with blockchain will increase.**

3. What's New with Hyperledger Fabric 1.0

Endorser Peer

In order to check whether the operations which are generated are appropriate, we first have to submit the transactions to endorser peers. If endorser peers return a positive response, the transactions can be registered. Thus, there is no need for every peer in the system to test the transactions. This structure is designed in this way due to the need for high performance and a modular structure. In Fabric 1.0, there is no obligation and no limit on endorser peers. If they wish, peers can identify themselves as endorser peers and participate in the testing process.

Orderer Service

The orderer service was added to operate the consensus. The orderer service can order a certain number of transactions collectively and register them in a block. In particular, it can attempt to complete transactions that require being added to the system simultaneously by different peers or sequentially in a very short timeframe. These processes ultimately need to be put in order and this sequence should not distort the integrity of the system. In some cases, transactions must be processed together. Fabric 1.0 also introduces the Kafka structure, which enables subject-based operations to be combined and run together. The service for these combinations is also the orderer service. The orderer service does not have to be given by a single peer. It can also be given by more than one peer. This enhances the accessibility of the system.

Database Subset and Query Properties

Although blockchain is a kind of database, it is not practical to browse through all the blocks in every query and process. For this reason, the distributed ledger is cached in the databases. Each peer has its own cache database. Thus, it can respond to queries more quickly and can perform integrity tests more easily when adding blocks. If CouchDB is used instead of the default LevelDB, and JSON is selected as the data structure, rich queries are allowed on the chain.
Since CouchDB is used as a service, the plug-in database feature can be used with CouchDB. Thus, those who want to use the different query features of different databases can make different queries and enrichments to the data by adding other databases on the service.

Key-Value Store
There were table structures in version 0.6. Although they provided ease of use in some cases, table structures might limit the Fabric, in particular. With Key-Value, it gained a more extensible and customizable structure.

Membership Service (COP)
With the new Membership Service, MSP structure (Membership Service Provider) is now offered.This service can be given by multiple peers instead of a single peer. Thus, SPOF (Single Point of Failure) risk has been removed.

Organization Structure
Organization structure has been added. An organization can have multiple peers. The multiple users managing these organizations can be defined. With this structure, organization-based rules can be set more easily.

Channel Structure
A channel structure has been added. Thus, multiple ledgers can be used on the same chain. Inter-organizational specific channels can be defined. Thus, only those who have access to that channel can see it or write the relevant information onto it. Flexible usage scenarios can be creat ed by defining specific endorser peers and consensus rules for the channel structure. While creating these channels, it is specified which peers can join. The peer can be added or removed later on.

Upgradeable Smart Contract Structure
Problems that arise when upgrading version 0.6 have been ironed out and version 1.0 enables the chaincode to be updated.

Synchronization
In Fabric 0.6, a peer would lose synchronization whenever it lost its connection with other peers. When the connection was reestablished, it couldn't complete the missing blocks. This led to some peers having different chains. With Fabric 1.0, every peer is able to contain the same chain and synchronize the missing blocks. Thus, the synchronization problem has been solved.

4. Basic Blockchain Concepts

4.1. Distributed Ledger Technology (DLT)

Today, systems that are open for use by more than one party in the business world need a reliable stakeholder located in the center and operating the system. Blockchain promises to create the necessary environment of trust without the need for an intermediary institution by ensuring that copies of the information are held equally by the actors in the system. As there is a demand for transactions and information sharing to be performed without an intermediary, DLT has emerged as a technology that fills this need.

With DLT, data are disseminated to all stakeholders, and when information is generated, the information's accuracy, consistency with existing data, and consensus processes can be queried and verified with smart contracts inside DLT.

With DLT, data are disseminated to all stakeholders, and when information is generated, the information's accuracy, consistency with existing data, and consensus processes can be queried and verified with smart contracts inside DLT. Only the data that is approved by the stakeholders is processed properly in the system and every stakeholder keeps a full copy of the data. In addition, each record is cryptographically linked to all previous records. It is possible to monitor the integrity of the chain to ensure that all records have been generated in this manner and whether they have been changed or not.

4.2. Smart Contracts

In the Bitcoin White Paper, a structure was introduced that enabled the transfer of funds between people, essentially without intermediaries. For this reason, only one record was kept with DLT under bitcoin. In time, it was determined that this technology, which removed intermediaries, could produce solutions for different scenarios. The distributed ledger structure can offer productive business models, but the generation of pieces of software that can process transactions using this ledger could lead to smarter transactions. The pieces of software in question could also be developed outside of the DLT. But in this case, each shareholder in the system could make different codes and each stakeholder could interpret the data in a different way. As a result, this could give rise to an undesirable situation involving a lack of standardization in the established structure. The software components that work in the DLT, which could be developed with restricted access by a virtual machine, would enable all stakeholders in the network to run the same program and achieve a more secure form of consensus when adding registers. Ethereum was designed with this in mind as an independent platform from bitcoin and it introduced the smart contract structure to us.

The advantages of smart contracts are not just limited to the verification of data. If there is an action to be taken after receiving the resulting data, smart contracts can initiate these actions and allow certain actions to happen automatically within the defined rules. This allows some of the tasks that are undertaken by the intermediary institutions to now be undertaken with DLT.

4.3. Consensus

A couple of years after the blockchain concept entered our lives with bitcoin, many organizations from different business lines began to show interest in blockchain technology and explore its uses. In the first studies, the aim was to become familiar with the technology by conducting experiments and reconstructing current processes with blockchain. The greatest factor that allowed these designs to be realized was the smart contract presented to the world of blockchain by Ethereum, which is discussed in detail in section 4.2. Smart contracts have transformed blockchain from a one-dimensional ledger into a structure of infinite dimensions.

We can define blockchain as a combination of three basic concepts. These are:

1. Signing of entries in the form of a chain providing data integrity,
2. Storage of data in a distributed manner,
3. Storage of entries by consensus only.

In fact, the most important of these concepts is that of consensus. This is because the first two concepts become meaningful after accurate data is provided by consensus, when the integrity of the data is ensured. It would not be useful for anyone to keep entries that were fraudulently or erroneously created.

The consensus structure is quite simple in some blockchains, for instance in bitcoin. If the transfers signed by users are consistent with the pre-established transfers and transfer in the last block and the previous blocks (for example, if the user has a sufficient balance for the amount he/she wants to transfer), it is written on a block and a proper summary of the block is generated. Bitcoin also does not have a smart contract structure. If there is a smart contract in a blockchain, the transactions that are added to these blocks must also be confirmed by smart contracts.

In blockchain networks, consensus is usually based on confirmation by the majority. This majority can also be regarded as one more than half (supermajority). If we consider a network with n blocks, there are different approaches in different blockchain implementations for the (n+1)th block. For example, in bitcoin, more than one (n+1) blocks occur and they divide the blockchain into several branches. Once the (n+2)th block has begun to be created, the miners continue verifying any (n+1) they wish. This is the same for (n+2) and later blocks. So, after a certain period of time, one branch of the chain starts to become longer than the other, and the other branches disappear as the majority chooses the longest branch. If we call each block creation phase a round, we should wait more than one round to pass for real consensus to be achieved in open blockchain networks such as bitcoin. Even if the correct summary is found, if there are erroneous transactions in the block, the block linked to the next rounds will not be accepted and the chain will continue from other branches. Thus, the system grows by confirming itself. The larger and more diverse the network, the more secure it becomes.

The consensus process is different in blockchain networks such as Ripple and Fabric. By their nature and organization, these networks involve actors who trust each other. For this reason, the focus is on performance rather than security. Unlike in bitcoin, there is an expectation that consensus will be ensured in every round; branching is not allowed. The whole system is not expected to participate in establishing consensus. Certain peers selected within the system take on this task.

Generally, the majority rule is applied, but the team which sets up the system can change these criteria within the framework of business rules. Consensus is realized through the peers performing different duties rather than through gradual confirmation. For example, the actions to be performed are first sent to a group of peers and they are asked to test these actions. If these peers do not reject the transaction, they sign the operation and return it with the data changes to the site where the transaction was carried out. These changes are then sent to the peers who perform the ordering operation. There, these transactions are ordered and combined according to certain criteria. Afterwards, transaction is sent to all peers for processing it to the distributed ledger. Fabric 1.0 and Ripple are very similar, though there are a few details that are different in the structure of Ripple. Therefore, consensus in Fabric and Ripple applies to the entirety of the transaction and can be rejected or confirmed at different stages.

4.4. Permissioned Structures and Permissionless Structures

Blockchain networks are divided into different categories according to the right to read and write data.These categories are often called private and public, but it would be more accurate to call them permissioned and permissionless. Public and private classifications can be made under these categories as follows:

Table 2: Blockchain Structures

Permissioned		Permissionless	
Private	Public	Private	Public

In permissioned blockchains only the designated peers with specific rights can contribute to block formation and consensus. On the other hand, in permissionless blockchains all peers can contribute to block formation and consensus. Private blockchain structures determine who information is to be shared with. In private blockchains, the network is not open to everyone, but those who enter the network have permission to access the blockchain data. In public blockchains, the network is open to all peers.
Developed by BKM, BBN is a blockchain solution that falls within the permissioned and private blockchain category. With its added value to data security and confidentiality, this structure is often preferred in the practices carried out by financial industry players. Bitcoin is an example of a permissionless/public blockchain.

In permissioned blockchains only the designated peers with specific rights can contribute to block formation and consensus.

5. Conclusion

When we launched BBN as The Interbank Card Center, Turkey's first blockchain project, at the beginning of 2017, we started this journey with the belief that one has to experiment in order to learn as in all new technologies. When we were testing the technology at the beginning of the road, we aimed to convey to our stakeholders what we had learned, as well as recognize the weaknesses and opportunities. In the first phase we completed for our BBN app, we reached the conclusion that the blockchain technology is not yet mature enough to replace a large-scale system. We believe, however, that if standards are set and players in the ecosystem can meet on a common ground, blockchain-based applications that make use of distributed ledgers, smart contracts and consensus structures will be adopted in various areas of use by different industries in the medium term.
In Phase II, we will upgrade our BBN application to Hyperledger Fabric version 1.0 and we will create areas of use where we can test new structures, such as consensus and channels.
In addition to these works in Hyperledger, developing an Ethereum-based app is also among our 2018 objectives.As a result of all these efforts, when the right time comes, using blockchain in areas where technology will add value will be an important item on our roadmap. As The Interbank Card Center, we will continue to experiment with and learn and tell about new technologies.

Blockchain Glossary

Bitcoin: The first known cryptocurrency. It has a completely distributed infrastructure and works without intermediaries.

Blockchain: A continuously growing distributed database that was first introduced by bitcoin, in which records are linked using cryptography.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 hashing a transaction by a blockchain network. This operation is done through mining on some blockchain networks.

Consensus Protocol: The steps that a group of distributed peers take to establish the consensus about the content in distributed ledger.

Cryptocurrency: A digital currency whose production is limited by various mathematical functions and secured with cryptographic techniques and protocols.

Cryptography: A set of mathematical methods that work to provide information security concepts such as confidentiality, authentication and integrity.

Ethereum: Ethereum is a public blockchain-based distributed computing platform, featuring smart contract functionality.

Ether: It is the value token on the Ethereum blockchain. Like other cryptocurrencies, Ether can be traded on crypto currency exchanges.

EVM: With Ethereum Virtual Machine (EVM), P2P contracts called "smart contracts" can be completed using cryptocurrency.

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

Digital Identity: An identity that allows a person, organization, or electronic device to be identified in a network. Digital identity is one of the uses of blockchain that is being explored as a solution to the complexity of password management processes, as a result of the interactions of individuals with many institutions and platforms.

Distributed Ledger Technology: A type of database that has copies stored on different servers. Records grow continuously by adding one after the other.

Mining: The process of creating cryptocurrency in blockchain networks. Mining is the general name of the process of performing mathematical operations using computing power and authorization.

Peer (Node): A computer connected to the blockchain network.

Ripple: A blockchain network developed for international money transfers. The system has been developed by Ripple Labs, and it has its own currency called XRP.

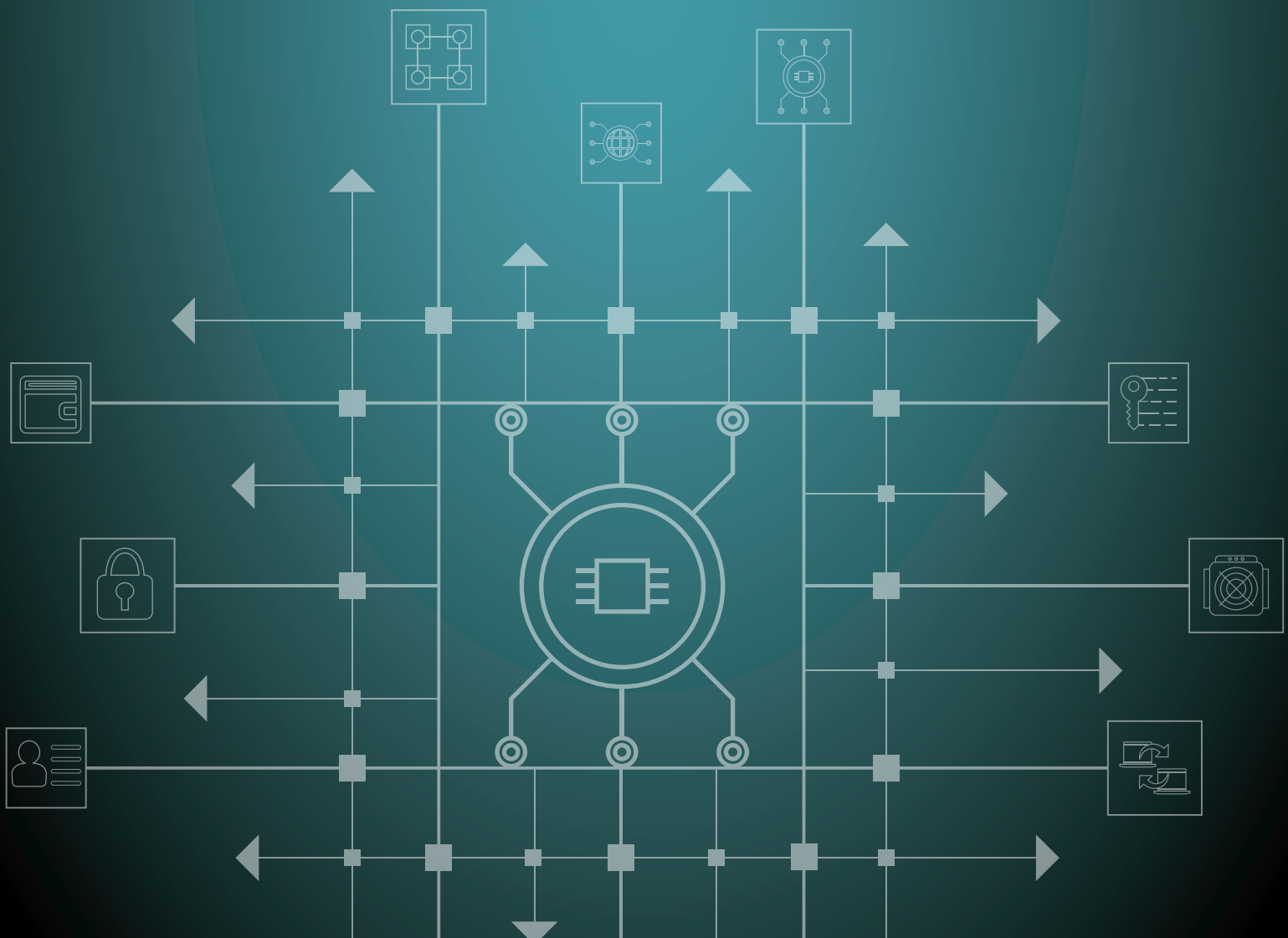
Smart Contracts: Contracts written in a programming language. Smart contracts can be executed automatically and perform transactions on distributed ledger structures.

Token: Digital assets that can be owned.

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

Wallet: The structure that stores the owner's private key.

BBN APP DEVELOPMENT TEAMS



The Interbank Card Center BBN Development Team

Soner Canko, PhD
CEO

Celal Cündoğlu
Executive Vice President, IT

Özge Çelik
Senior Vice President, Business Development

Okan Yıldız
Vice President, Business Development

Kadir Güzel
Senior Mobile Application Developer

T2 Software, Inc. BBN Development Team

Mustafa Sakalsız
Project Manager - CTO

Dr. Tan Apaydın
Mobile & Blockchain Developer

Mert Çalışkan
Web Developer

Ömer Metehan Danacı
Web & Blockchain Developer

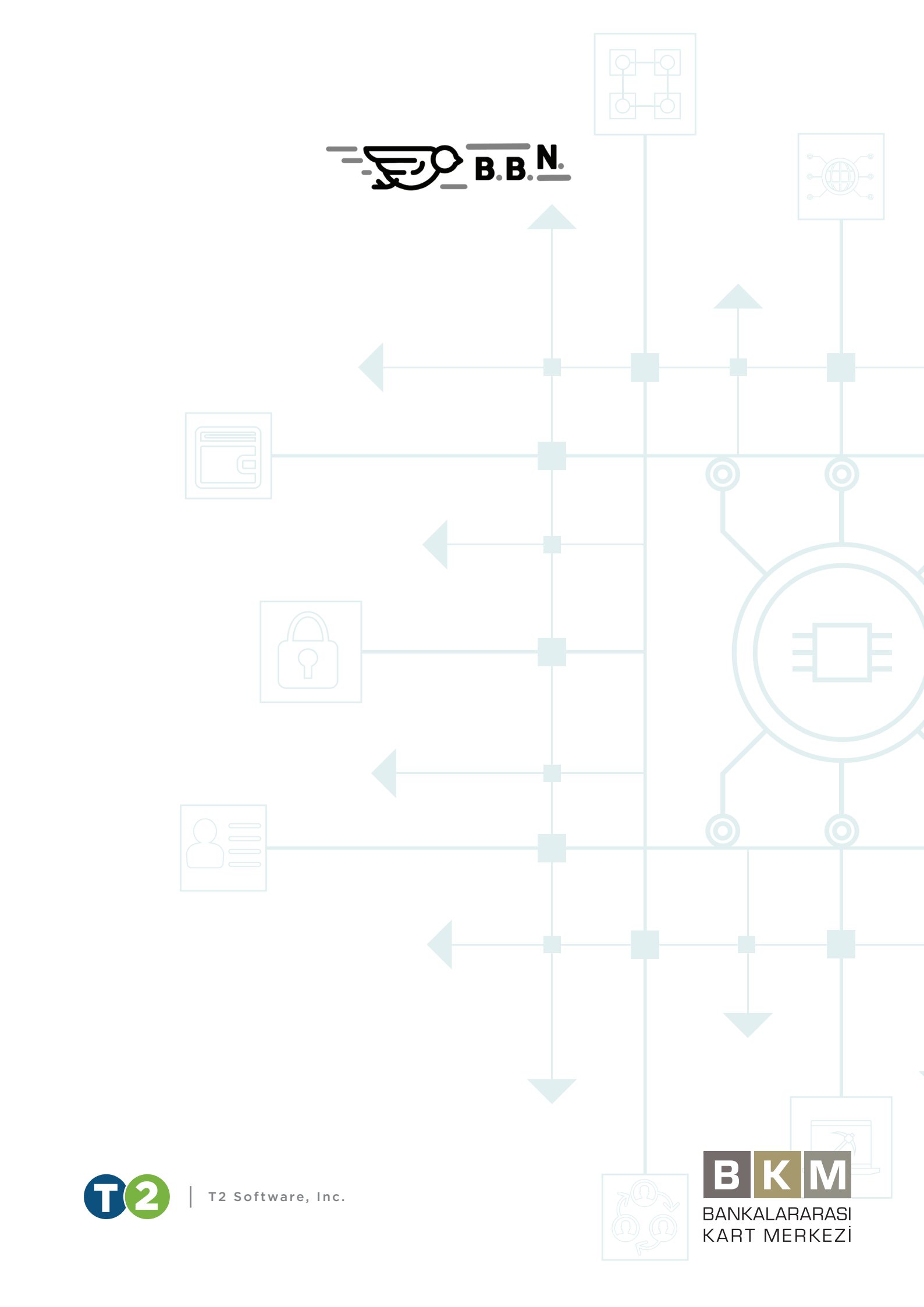
Mustafa İlker Saraç
Mobile Developer

Burak Doma
Scrum Master

Burak Başcı
UI Designer

Dr. Kamer Kaya
Consultant
Sabancı University

Dr. Ata Türk
Consultant,
Boston University



T2 Software, Inc.

BKM
BANKALARARASI
KART MERKEZİ