BKM BANKALARARASI KART MERKEZİ | Microsoft | VERİPARK

belgem.io

BLOCKCHAIN FOR EVERYONE

FEBRUARY 2019

INTRODUCTION

Soner Canko, Ph.D.
CEO of BKM
(Interbank Card Center)

Trying new technologies is inherent in BKM's culture. We pilot solutions built on AI, IOT, AR & blockchain, to assess their potential. Since we believe that value of knowledge is appreciated once it is shared, we document our findings and share it with our ecosystem. Blockchain is a technology we intently focus on learning since it is an ecosystem solution at its core.

We are proud to launch belgem.io, our second blockchain-based product (after introducing BBN on the Hyperledger Fabric platform). You can now safely store your certificates of education on our Ethereum-based cloud platform, belgem.io. This report explains the purpose of belgem.io, the architectural structure of the platform and other technical details.

We were among the pioneering companies that established Blockchain Türkiye in 2018,

and we recognize that creating the right ecosystem is the key to success when using blockchain-based solutions. belgem.io, another outcome of this vision, is the fruit of our consortium's efforts with VeriPark and Microsoft. Blockchain will continue to make headlines in the coming period and we will keep sharing our findings from our trial projects with you.

Aslı Derbent Özkan
General Manager
of VeriPark

The "business" between the "buyer" and "seller" is conducted through "intermediary institutions" and "notary services."
B2B Business model doesn't rely on a workflow between businesses; it requires the intermediation and surety of many organizations, authorities and companies.

Blockchain technology offers a game-changing shift to businesses by removing the need for an intermediary or a validation authority.

As in the belgem.io project, blockchain will make life easier for people in many fields, including finance, energy, healthcare, telecommunication, education and logistics.

It does this by eliminating trust issues between individuals.

At VeriPark, we consider blockchain a breakthrough technology that will change the future, and prepare our infrastructure for tomorrow through R&D and concept validation.

Murat Kansu
General Manager
of Microsoft Turkey

Various players, including major banks, will explore the use of the blockchain technology, allowing for the safe implementation of many activities such as e-commerce, file sharing and communication. We expect many organizations will soon cooperate to develop a common blockchain infrastructure and take advantage of the opportunities offered by the technology.

We foresee over 25 percent of the world's largest 2,000 companies investing in blockchain technologies in the next year. In 2019, 25 percent of the prosthetic 3D printers will operate on blockchain, providing a secure data-sharing and developing patient-specific solutions. By 2020, 25 percent of the world's top trading banks, nearly 30 percent of manufacturers and retailers, and 20 percent of healthcare institutions will utilize the blockchain network when providing their services. By 2021, 20 percent of the data acquired from open-source networks will be recorded to a public blockchain network and many applications will be developed to verify them. By 2022, the data of more than a billion people will be stored on a blockchain network.

Striving to help everyone and each organization achieve more, Microsoft considers the belgem.io project a major achievement for Turkey,

one that will unify education and a new technological milestone: the blockchain. The platform is one of the world's first applications developed with Ethereum Proof-of-Authority Consortium that runs on Microsoft Azure cloud computing platform. In cooperation with BKM and VeriPark, we have taken a major step in education through the use of this technology, allowing for safe and fast transactions. We are pleased that our innovative projects are contributing to the digital transformation of Turkey.

Executive Summary

Blockchain offers decentralized and cryptography-based alternative solutions for confidential transactions such as identification and authorization. Blockchain technology:

- is considered the future backbone of digital transactions because of the way it secures and regulates digital relationships.
- Cryptography ensures data confidentiality and eliminates the need for a third-party control by securing the data transfer.

Launched by BKM (Interbank Card Center), Microsoft and VeriPark, belgem.io stores the educational certificates on its safe and irrevocable blockchain infrastructure and allows the user to share them with any organization/individual they like.

We believe that understanding blockchain is essential, since it facilitates the building of trust-based business models without intermediaries. Because of this, we conduct proof of concept projects, and throughout these projects we aim to provide a more thorough understanding of the technology, measure the maturity level of the related tools, and share the experience gathered within the ecosystem.

The use case we have implemented for this proof of concept is belgem.io. The *Ethereum* blockchain platform gave us an easy way to implement our use case. It also paved the way for the integration of smart contracts into the blockchain thanks to its fundamental innovation of *Ethereum Virtual Machine* (EVM). We tested and developed our smart contracts using the programming language of Solidity *through Truffle framework on Ethereum platform*, which features coding flexibility. Utilizing the consensus mechanism of *Proof of Authority* (PoA), belgem.io is among the world's first applications developed with *Ethereum Proof-of-Authority Consortium* on Microsoft Azure. Thanks to this product, we have created a blockchain and added the nodes in a short time. The consensus algorithm of *Proof-of-Authority*, which does not involve any mining mechanisms, fully met our needs with its governance portal and block production speed.

belgem.io verified the identity of organizations with the Ethereum wallet of MetaMask and employed "BKM Express" to validate the user data. We used asymmetric cryptography to verify digital certificates. We worked with Azure's Key Vault for sensitive data management and built a mechanism on blockchain that does not store any sensitive data.

In this report, you can find the details of our experience developing belgem.io. The platform will be open to institutions and individuals other than the BKM. We are excited by the way belgem.io can be utilized to make observations in a live environment.

We will update this report with post-launch lessons learned.

1. The Technical Infrastructure of belgem.io

1.1 What is belgem.io?

belgem.io is a digital platform designed to store, view and share educational certificates on a private Ethereum blockchain. Developed in cooperation with BKM (Interbank Card Center), Microsoft and VeriPark, this platform aims to test concepts such as Ethereum, smart contracts, Proof-of-Authority consensus algorithms and governance between organizations. Thanks to its governance panel, each decision is submitted for voting with a majority requirement of 51 percent. belgem.io uses a private and a permissioned blockchain network. The platform is positioned on Ethereum Proof-of-Authority Consortium on Azure's cloud platform.

1.2 The Blockchain Platform

belgem.io runs on the Ethereum blockchain platform.

It is one of the world's first applications developed with Ethereum Proof-of-Authority Consortium on Microsoft's Azure cloud computing platform in July 2018. The platform uses the Proof-of-Authority consensus algorithm to make joint decisions between the nodes.

At the beginning of the project, the following alternatives were evaluated:

- Ethereum Proof-of-Authority Consortium (Azure)
- Ethereum Proof-of-Work Consortium (Azure)
- Parity Ethereum PoA (Azure)
- R3 Corda
- Hyperledger Sawtooth
- Customized Bitcoin

When choosing between these platforms, the team aimed to meet various expectations, such as:

- A closed-circuit system and a governance structure that can only grow or shrink by the joint decision of the system peers,
- A blockchain structure that allows for MetaMask or similar digital wallet applications,
- Use of a new programming language during the development process of smart contracts,
- A technically competent platform whose support services are able to produce quick solutions to problems.

We have chosen Ethereum, a blockchain-based distributed computing platform that is preferred by many distributed applications. Our decision was also influenced by Ethereum's support of multiple consensus algorithms. When developing the application, we tested both the Proof-of-Work and the Parity-based Proof-of-Authority on Azure. We also experienced the Truffle Framework, which provides great convenience through Ethereum transactions and smart contract tests. Our final choice was the Ethereum Proof-of-Authority Consortium, which, thanks to its structure, does not require mining, has an efficient governance portal and a block production rate of two or four seconds. Thanks to our partnership with Microsoft, we created belgem.io through the mutually nurturing combination of Ethereum and Proof-of-Authority Consortium.

1.3 Top Level Architecture and Technologies

We primarily used some open-source technologies during the implementation stage of the project.

- Operating System: Windows
- Application server: Windows Server
- Database server: MS SQL
- Blockchain platform: Ethereum
- Blockchain product: Azure Ethereal Proof-of-Authority Consortium
- Web development platform: ASP.NET MVC
- Programming languages: C#, Go, Solidity, JavaScript

The first four organizations to issue certificates on belgem.io are Microsoft Cloud Society, FinTech Istanbul, BayBayNakit Akademi and the Blockchain Turkey Platform (BCTR). We assigned the admin role to an account from BKM and authorized them to become a peer on the blockchain network. This means that the governance practice involves a voting right. When new organizations are proposed to the system, the decisions will be made in line with the votes of internal institutions and the manager. Each peer on the blockchain has equal voting right for the decisions on the governance portal. This structure, formed with smart contacts, imposes a majority requirement of 51 percent.

Participating organizations should choose one of the following options to issue a certificate on belgem.io:

I. Become a blockchain node

1. Each partner that chooses this option is entitled to participate in the private network in line with the voting. They are each required to open an account on Azure and set up the Ethereum Proof-of-Authority Consortium. The installation is completed with the public key created using MetaMask and the information about belgem.io blockchain.

1. The BKM admin provides the organizations in the blockchain network with the necessary information to login to the belgem.io web application. They are granted the authorization to send transactions to the blockchain using the web application. Through the permissioned transactions, they can create and issue certificates.

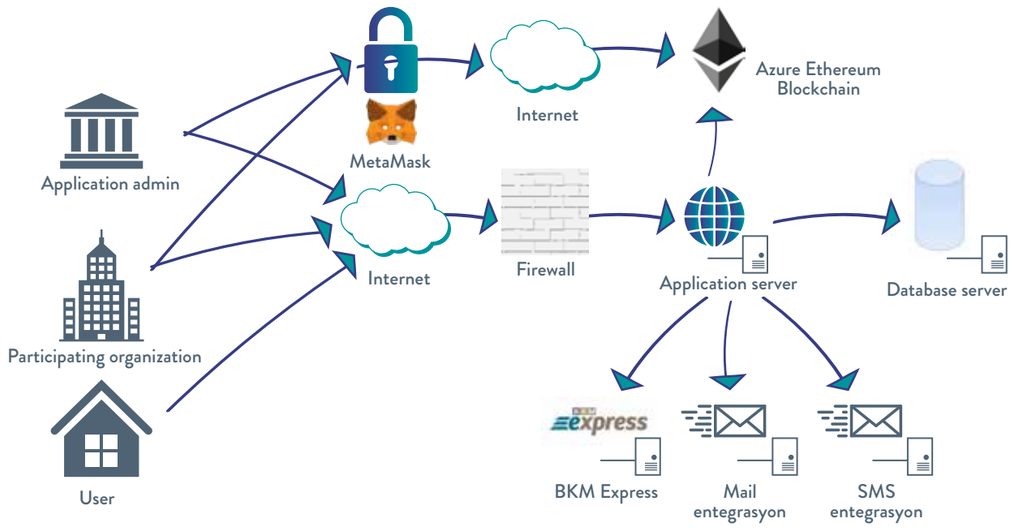
II. Only execute permissioned transactions

>> Organizations chosing this option are permitted to create and issue certificates. These institutions are not entitled to a voting right for new participants and are not included in the governance platform since they are not blockchain nodes.

Even though belgem.io is a private blockchain network, its structure allows access to the contracts through the cloud client information. People with malicious intent may send false transactions to smart contracts.

This can cause the application to lose functionality by collapsing the network or cause problems on the governance. To prevent this, we developed a Transaction Permissioning smart contract for the governance portal and certificate contracts. This contract aims to ensure that only the addresses authorized by the belgem.io peers can access the belgem.io contracts and send transactions.

Figure 1: **Top Level Architecture Diagram**



1.4 Why do we use Blockchain on Azure?

Blockchain applications on Microsoft Azure support simple setup templates for anyone with an entry-level Azure and blockchain infrastructure. The blockchain network topology is created within minutes thanks to the simple installation screens of the products provided by the Azure portal. We focused on developing our application and scenarios, rather than spending hours building and configuring the infrastructure. The Proof-of-Authority Consortium was the perfect match for belgem.io app. It met our requirements with its private and permissioned blockchain network, distributed governance feature and its management portal for enterprise blockchain projects. It took only 16 minutes to restore functionality to the entire network after keying in the platform features of belgem.io on Azure's portal. The consensus algorithm, Proof-of-Authority, creates a new block every four seconds, without the need for mining.

1.5 Verification on belgem.io

One of the main scenarios of the belgem.io app is that users can easily access the certificates issued in their name and share them in a digital environment. belgem.io contains two main roles: "educational institution" and "user." Educational institutions may vote by joining the distributed governance application, and produce and send certificates to user accounts, through their MetaMask account. Users, however, are not associated with any MetaMask wallet. Users can access their profiles created with their verified credentials through the BKM Express application, and view and share their certificates.

For a non-MetaMask user, validated credentials were transferred to the belgem.io's database in exchange for a donation transaction via BKM Express. In respect to GDPR, credentials are considered as sensitive data, they may be shared with the application/institution/blockchain only if approved by the user. BKM already utilizes the BKM Express application for user authentication. E-Government authentication, mobile applications of banks and authentication solutions for operators can serve as an alternative to this function for future user scenarios.

When the user first registers for belgem.io, the institution simultaneously performs the verification process using this information.

1.5.1 User Verification through BKM Express on belgem.io

While registering, a (1TL) charity donation transaction is performed by scanning the QR code generated on screen through the BKM Express application. This transaction identifies the authenticated information, including user's name, surname and TRIN.

Users complete the registration by filling in their e-mail address and mobile phone number.

1.5.2 Organization Verification through MetaMask on belgem.io

An institution must be invited by another institution to register the platform. The new institution's public key and authorized person information are filled out on the Organization Screen. The authorized person then receives the request and submits the new institution's proposal to the consortium through the governance application. Once the new institution is found to be eligible to participate, belgem.io manager will notify the authorized person to complete the registration process.

1.5.3 1.5.3 Digital Document Verification on belgem.io

Each certificate produced by belgem.io has a unique link. The app creates this link by using the ViewToken in the MetaMask transaction. Users can use the verification link on the belgem.io certifiate to authenticate the certificate they received from the platform and add it to their CV.

The scenario behind the design of the verification link is:

- The belgem.io produces certificates from the member organizations in the name of the user. These documents are included in the user's CV.
- The user applies for a job.
- The HR department of the relevant organization may request authentication of the digital documents in the CV.
- The encrypted ViewToken information in the certificate link is decrypted with the public key of the institution.
- The relevant users are notified of the result and deemed "verified" or "not verified."

2. Lessons Learned

2.1 Ethereum

2.1.1 Ethereum Blockchain

Simply put, Ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications.

Like Bitcoin, Ethereum is a public blockchain. Although there are some significant technical differences between the two, the most important distinction to note is that Bitcoin and Ethereum differ substantially in purpose and functionality. Bitcoin offers one particular application of blockchain technology: a peer-to-peer electronic cash system that enables online Bitcoin payments. While the Bitcoin blockchain is used to track ownership of digital currency (bitcoins), the Ethereum blockchain focuses on running the programming code of any decentralized application.

Instead of mining for bitcoin, miners in the Ethereum blockchain work to earn Ether, a type of crypto token that fuels the network. Beyond being a useful

cryptocurrency, Ether is also used to pay for transaction fees and services by application developers on the Ethereum network. There is also a second type of token called GAS. The performance of each transaction or smart contract execution is measured and paid for by GAS. However, belgem.io uses a PoA consensus algorithm, eliminating the need for these types of fees. This way, PoA spares users and educational institutions that join belgem.io the cost of dealing with crypto-management.

2.1.2 Smart Contracts

Smart contract is just a phrase used to describe a computer code that can facilitate the exchange of money, content, property, shares, or anything of value. When running on the blockchain, a smart contract becomes like a self-operating computer program that automatically executes when specific conditions are met.

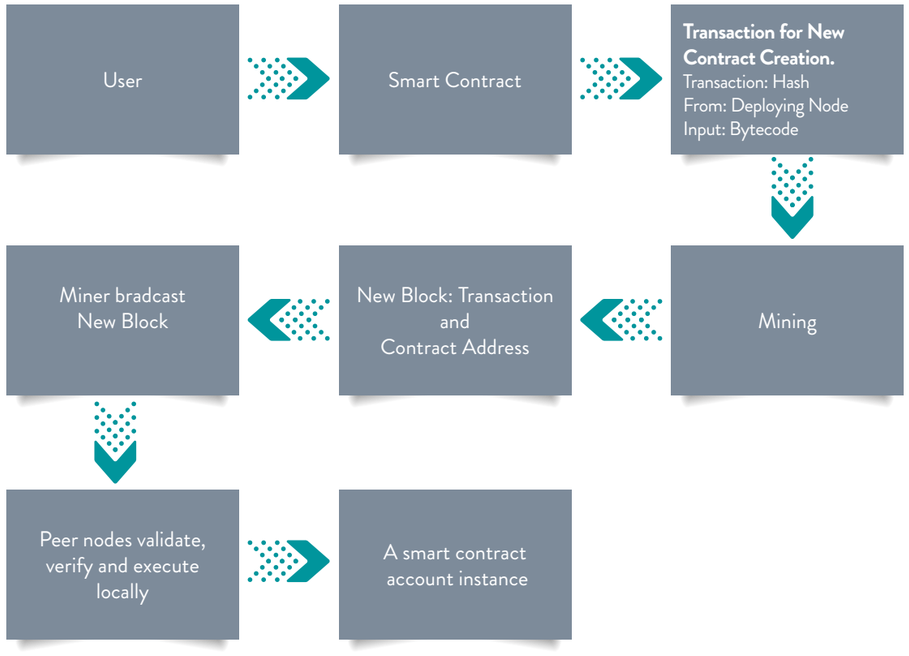
While all blockchain platforms have the ability to process code, most are severely limited. Ethereum allows developers to create whatever operations they want thanks to its coding flexibility.

Smart contracts contain the following components:

- State variables
- Functions
- Events

Smart Contract Creation

Smart Contracts are compiled and converted into bytecodes. These bytecodes are deployed to the Ethereum Virtual Machine (EVM). Below is the visual representation of how smart contracts are created:



>> The process of deploying the smart contract is triggered by a transaction.

>> The transaction must take effect.

>> Peer nodes perform the mining "competitively."

>> The new block generated after a successful mining operation includes a transaction and contract address.

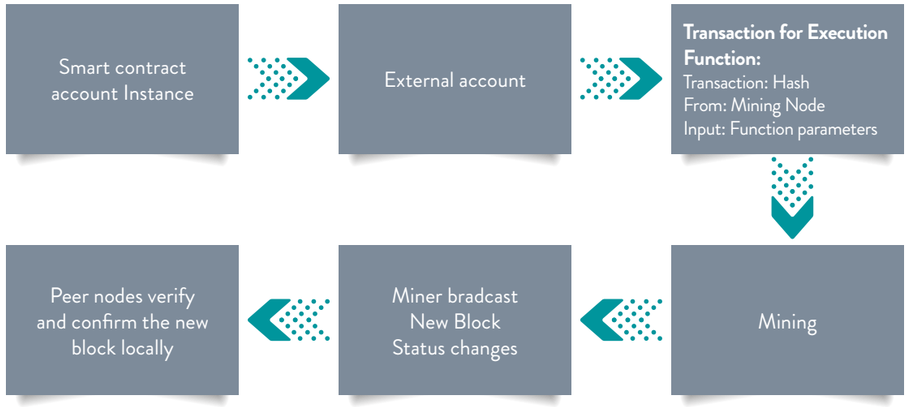
>> The new block created by the miner will be broadcasted to the peer nodes.

>> The new block will be validated by the peer nodes to become an official block in the local blockchain.

>> The new instance of the Smart Contract contains a unique address. This address must be recorded for the next contract deployment.

Smart Contract Execution

Functions included in smart contracts can be run by an external account or a distributed application (dApp).uygulama tarafından çalıştırılabilirler.



>> To execute a function defined in the smart contract, the address of the smart contract is taken.

>> Each function that changes the state calls a transaction.

>> The transaction must be mined to be approved.

>> The new block generated after a successful mining operation includes a transaction.

>> The new block created by the miner will be broadcasted to the peer nodes.

>> The new block will be validated by the peer nodes to become an official block in the local blockchain.

2.1.3 Ethereum Virtual Machine (EVM)

Ethereum's core innovation, the Ethereum Virtual Machine (EVM), is a "Turing complete software" that runs on the Ethereum network. It enables anyone to run any program regardless of the programming language, time and memory.

The Ethereum Virtual Machine makes the process of creating blockchain applications significantly easier and more efficient. Instead of having to build an entirely original blockchain for each new application,

2.1.4 In Which Fields Can We Utilize the Ethereum Network?

Ethereum enables developers to build and deploy decentralized applications. A decentralized application, or dApp, serves a particular purpose to its users. Bitcoin, for example, is a dApp that provides users with a peer-to-peer electronic cash system and facilitates online Bitcoin payments. Because decentralized applications are made up of code that runs on a blockchain network, they are not controlled by any individual or central entity.

Ethereum can also be used to build Decentralized Autonomous Organizations (DAO). A DAO is a fully autonomous, decentralized organization with no single leader. DAOs are run by programming code on a collection of smart contracts written on the Ethereum blockchain. The code is designed to replace the rules and structure of a traditional organization, eliminating the need for people and centralized control. Anyone who purchases a token will be considered the owner of a DAO. However, these tokens do not equate to equity shares and ownership; rather they serve as contributions to grant voting rights. Inspired by DAO, belgem.io's governance structure is autonomized by smart contracts.

2.1.5 What are the drawbacks of Ethereum implementation?

Despite their numerous benefits, decentralized applications are not perfect. As smart contract code is written by humans, smart contracts are only as good as the people who write them. Code bugs or oversights can create unintended issues.

Mistakes or errors in the smart contract code can leave it vulnerable to attacks. This can cause security breaches, such as the unauthorized access of the network consensus, and a rewriting of the underlying code. This goes against the essence of the blockchain, which is meant to be immutable. To fortify belgem.io, we have developed and rigorously tested highly advanced protective smart contracts.

2.1.6 Private and Permissioned Ethereum Blockchain Structure

Blockchain networks are divided into different categories according to the right to read and write data. These categories are often called "private" and "public," though 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 designated peers with specific rights can contribute to block formations and consensus. However, in permissionless blockchains all peers can contribute to block formation and consensus. Private blockchain structures determine who information is shared with. In private blockchains, the network and blockchain data is restricted to those who have specific permission. In public blockchains, the network is open to all peers.

belgem.io usecase aims to house the governance structure on a private chain and offer free transactions. belgem.io is a blockchain solution that falls within the permissioned and private blockchain category. With its improved data security and confidentiality, this structure is typically preferred in enterprise blockchain solutions..

What advantages does a private chain offer over a public chain?

Below are the top advantages that a private chain can offer institutions and organizations.

- Transactions are cheaper or free of charge.
- You are less likely to experience delays.
- You have more authority and control over the chain.

2.1.7 Azure Ethereum Proof-of-Authority Consortium

The Ethereum Proof-of-Work Consortium is a governance platform designed to make it easier and quicker to authorize, configure and manage a multi-member consortium Ethereum network with minimal Azure and Ethereum knowledge. With a single-click deployment through the Azure portal, each member can update the organization name, and add new organizations or remove existing organizations from the consortium.

Although belgem.io is a private blockchain network, users could potentially connect to the network through the belgem.io client (RPC) information. This means they could send transactions to the governance app and certificate authentication contracts.

To prevent fraudulent transactions, we wrote an additional contract, which includes Transaction Permissioning. This ensures that only authorized accounts can perform transactions. The “admin” organization, which is the first participant on the private network, adds a new participant in the governance application by authorizing accounts that join the system through this contract.

2.1.8 Performance

The block creation statistics of the belgem.io application is displayed on Azure Monitor.

You can perform the following actions through Azure Monitor:

- Detection of infrastructure and network interruptions
- Monitoring network statistics of each node
- Customized transaction tracking
- Creating performance output

2.2 Our Software Development Tools

2.2.1 Truffle

Truffle is a development framework that allows developers to easily develop applications on Ethereum. Here are the top features of Truffle that we utilize throughout the project:

- Smart contract compilation, linking and testing
- Automated testing for quick development
- Easy switch and transfer between structures
- Private and public network management
- Package management with EthPM and NPM
- Interactive console for direct contract interaction

2.2.2 Ganache

Ganache, formerly called TestRPC, offers a personalized blockchain structure where you can test your distributed applications. Ganache is available for Windows, Mac and Linux, allowing you to easily test your application on your own computer‘s blockchain.

2.2.3 Parity

Miners, service providers and exchanges need fast synchronization and maximum up-time. Parity Ethereum provides the core infrastructure required for fast and reliable services. Developed using the programming language Rust, Parity aims to be the fastest and the most secure Ethereum client.

Highlights of Parity:

- Modular codebase for easy customization
- Advanced CLI-based client
- Minimum memory and storage requirements
- Synchronize in hours Warp Sync
- Modular for integration into your service or product

2.2.4 Azure CLI 2.0

Azure CLI 2.0 is a cross-platform command-line tool for managing Azure resources. It makes it easier to manage your resources with scripts. We have taken advantage of the forums and documentations of Azure CLI. This has enabled us to save time when installing the blockchain with the desired features. You can use it in your browser with Azure Cloud Shell, or install it on macOS, Linux or Windows and run it on the command line.

2.2.5 Solidity

Solidity is a contract-oriented programming language for writing smart contracts. It is used for implementing smart contracts on Ethereum and various blockchain platforms. It was influenced by C++, Python and JavaScript and is designed to run on Ethereum Virtual Machine (EVM). It was developed

by former Ethereum core contributors, such as Gavin Wood, Christian Reitwiessner, Alex Beregszaszi, Liana Husikyan, and Yoichi Hirai.

2.2.6 Contract ABI (Application Binary Interface)

Smart contracts are compiled to bytecodes under a specific contract address and stored in the blockchain. An ABI is necessary to access the contract bytecode, specify which function in the contract to invoke, and guarantee that the function will return data in the expected format.

2.2.7 Web3.js

The web3.js library is a collection of modules that allows you to interact with a local or remote Ethereum node using an HTTP or IPC connection.

This official javascript API enables interaction with smart contracts.

2.2.8 Nethereum

Nethereum is the .Net integration library for Ethereum. It simplifies the access to and interaction with smart contracts both for public and permissioned Ethereum nodes like Geth, Parity or Quorum.

2.2.9 List of Ethereum Clients

We prefer to use Parity for belgem.io, as it is one of the Ethereum protocol's seven clients. It uses the Azure Ethereum Proof-of-Authority's consortium product, and Parity's Aura consensus engine.

The other Ethereum clients include:

Client	Language	Developer
go-ethereum	Go	Ethereum Foundation
cpp-ethereum	C++	Ethereum Foundation
Pyethapp	Python	Ethereum Foundation
Ethereum(J)	Java	<ether.camp>
Ruby-ethereum	Ruby	Jan Xie
Parity	Rust	Ethcore
ethereumH	Haskell	BlockApps

2.3 Sensitive Data Management

2.3.1 Azure KeyVault

We see many blockchain implementations that end up storing its data, in an encrypted format, on its network.

However, advancements in quantum computing put blockchain security as well as encrypted data stored on the network at risk. Each encryption algorithm has a

lifespan. Because of this, we send the transactions performed within the belgem.io to the public keys generated by Microsoft Azure Key Vault (Cloud HSM) and did not write any critical data to the blockchain. We created a public key for each user who registered to belgem.io on Key Vault with a FIPS 140-2 Level 2 HSM and sent the certificates to these public keys.

You can see the transaction set and the distribution of the data in the table below.

	Web Application	Server Database	Blockchain
User Login	User Email and Password	Verification and Authorization Transactions	-
User Registration	Authentication with BKM Express	User Information (TRIN number, name, surname, email and mobile number)	Public key created on behalf of the user
Organization Registration	Starting the Process	Information about the institution and the authorized person	Organization's public key
Certificate Request	Information about the requested certificate	Certificate requesting institution, requester and certificate information	-
Certificate Registration	Information about the requested certificate	Certificate issuer, certificate holder, name and date on the certificate	Certificate issuer, certificate holder, name and date on the certificate

3. Conclusion

3.1 Summary

The top features of the current platforms include privacy, performance (number of transactions per second) and durability. In blockchain projects choosing the most suitable structure to your usecase is more important than focusing on the superior capabilities of each platform.

belgem.io application

- >> utilizes the open-source Ethereum platform, as it creates smart contracts for certificate authentication and inter-institutional governance structure.
- >> utilizes Proof-of-Authority consensus algorithm to create a democratic structure between the nodes.
- >> provided an average of four seconds of block production speed, although high performance is dispensable for this specific usecase.
- >> utilizes cloud HSMs on Azure Key Vault for securing users' data.

3.2 Glossary

>> Address: Cryptocurrency addresses are used to send or receive transactions on the network. An address is a string of alphanumeric characters that can also be represented as a scannable QR code.

>> Asymmetric Cryptography: Asymmetric cryptography is also known as public key cryptography. It uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). A public key may be shared with everyone, while the private key in the Parity is kept secret. Protocols such as SSH, S/MIME rely on asymmetric cryptography for encryption and digital signature functions.

>> BBN: 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 consensus.

>> BKM Express: A payment system that makes online shopping fast, easy and joyful, developed with BKM, banks and leading companies of e-commerce area. Card owners can shop without sharing any card information online by saving their cards on BKM Express. The places of business that accept card on e-commerce websites can approach more customers as a Member Place of Business of BKM Express.

>> Blockchain: A digital distributed ledger, comprised of unchangeable, digitally recorded data in packages called blocks. Each block is then "chained" to the next block using a cryptographic signature. This allows blockchains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions.

>> Confirmation: This means the blockchain operation has been verified by the network. This occurs through a process called mining, in a proof-of-work system (e.g. Bitcoin). Once a transaction is confirmed, it cannot be reversed or double spent.

>> Consensus Algorithm: A consensus algorithm ensures that the next block in a blockchain is the one and only version of the truth. It also keeps powerful adversaries from derailing the system and successfully forking the chain. The most common consensus algorithms are Proof-of-Work, Proof-of-Stake and Proof-of-Authority.

>> Cryptography: Cryptography is the encryption and decryption of data. There are two main cryptographic concepts used in blockchain: hashing and digital signatures. In general, there are three widely used forms of encryption: symmetric cryptography, asymmetric cryptography, and hashing.

>> dApp (Distributed Application): A decentralized application (dApp) is an application that is open source and operates autonomously with no entity controlling the majority of its tokens.

>> Digital Signature: A digital signature proves that a message originated from a specific person and no one else. When you visit a website, you are using SSL. This uses a digital signature to establish trust between you and the service.

>> Distributed Ledger: A type of database that is spread across multiple sites, countries or institutions. Distributed ledger data can be either "permissioned" or "permissionless" to control who can view it.

>> Elliptic Curve Digital Signature Algorithm (ECDSA): ECDSA is a cryptographic algorithm used by Bitcoin to ensure that funds can only be spent by their rightful owners.

>> Encryption: Encryption is the process of turning a clear-text message (plaintext) into a data stream (cipher-text), which resembles a meaningless and random sequence of bits.

>> Ether: Ether is the native token of the Ethereum blockchain and is used to pay for transaction fees, miner rewards and other services on the network.

>> Ethereum: Ethereum is an open software platform based on blockchain technology. It enables developers to build and deploy smart contracts and decentralized applications.

>> Ethereum Test Network: To mitigate the risk of bugs in your smart contract on the main net, it is important to test it before deploying to the Main Network. Ethereum has multiple test networks that can be configured as an acceptance environment. Ethereum provides several test networks, such as Rinkeby, Ropsten, and Kovan.

>> EVM – Ethereum Virtual Machine: EVM is the Ethereum smart contracts bytecode execution environment. Each node in the network runs EVM. All the nodes execute all the transactions that point to smart contracts using EVM. This means that every node performs the same calculations and stores the same values.

>> EVM Bytecode: This is the programming language in which accounts on the Ethereum blockchain can contain code. The EVM code associated with an account is executed every time a message is sent to that account, and has the ability to read/write storage and send messages.

>> GAS: The usage of blockchain costs money. This money is used to reward miners who validate your transactions and append them to the blockchain. All transactions on the blockchain have an associated fee called GAS. GAS is a unit of complexity that is used to set the price of code execution. GAS complexity does not depend on the current value of ether.

>> Geth Console (Go Ethereum): Geth is the command line interface for running a full Ethereum node implemented in Go. Installing and running Geth allows you to take part in the Ethereum frontier live network, mine real ether, and transfer funds between addresses. It also allows you to create contracts and send transactions, explore block history, and much more.

>> Hash Functions: The hash function transforms the digital signature before sending it and the hash value to the receiver. The receiver uses the same hash function to generate the hash value and then compares it to what they received with the message. If the hash values are the same, it is likely that the message was transmitted without errors.

>> Immutability: Immutability means a block cannot be modified after it is created. In blockchain, blocks are chained together so that you can't go back and change their contents without having to change every subsequent block. Depending on the consensus protocol, you can't change blocks without the express agreement of everyone involved. This is sometimes referred to as "mutable by consensus."

Keccak-256: A type of cryptographic hashing function. Ethereum uses Keccak-256.

>> **Ledger:** A ledger is only a record store, where records are immutable and may hold more general information than financial records.

>> **Master Node:** A master node is a cryptocurrency full node or wallet that stores a full copy of the blockchain in real time. It is always running. Master nodes differ to normal nodes because they increase the privacy of transactions, provide instant transactions, participate in governance and voting, and enable budgeting and treasury systems in cryptos.

>> **MetaMask:** A MetaMask is a bridge that allows you to visit the distributed web in your browser. It allows you to run Ethereum dApps right in your browser without running a full Ethereum node. MetaMask includes a secure identity vault, providing a user interface to manage your identities on different sites and sign blockchain transactions.

>> **Mining:** The process by which transactions are verified and added to a blockchain. This process of solving cryptographic problems using computing hardware also triggers the release of cryptocurrencies.

>> **Node:** A node is essentially a computer connected to blockchain network.

>> **Open source:** Software for which the original source code is made freely available and may be improved and modified by anyone.

>> **Solidity:** Solidity is a contract-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms.

>> **TestRPC:** TestRPC is a Node.js-based Ethereum client used for testing and development. It uses ethereumjs to simulate full client behavior and improves the efficiency of Ethereum application development. It also includes all popular RPC functions and features (like events) and can be run deterministically to make development a breeze.

>> **Token:** A digital identity for something that can be owned.

>> **Transaction Block:** A transaction block is a collection of transactions on the bitcoin network. It is gathered into a block, which can then be hashed and added to the blockchain.

>> **Truffle:** Truffle is a development environment, testing framework and asset pipeline for Ethereum that aims to make life as an Ethereum developer easier.

>> **Turing complete:** A computer is Turing complete if it can solve any problem that a Turing machine can when given an appropriate algorithm and the necessary time and memory. When applied to a programming language, it means that a Turing complete computer can fully exploit its capabilities.

>> **Wallet:** Wallets are used to store private keys.

>> **Web3.js:** Web3.js is a collection of libraries that allow you to interact with a local or remote Ethereum node using a HTTP or IPC connection. It communicates under the hood to a local node through RPC calls. Web3.js works with any Ethereum node that exposes an RPC layer.

DEVELOPER TEAM OF belgem.io

THE INTERBANK CARD CENTER

Celal Cündoğlu
Executive Vice President

Özge Çelik
Senior Vice President Business Development

Okan Yıldız
Business Development Vice President

Enes Türk
Engineer

MICROSOFT

Cavit Yantaç
Software Engineering Manager
DPE
Lead

Behice Funda
Business Program Manager
at
Microsoft EMEA

Emre Kenci
Senior Software Engineer

Seda Akdemir
Technology Strategist

VERIPARK

Tahir Özmen
Project Manager

Gencay Sazak
Senior Software Developer

Volkan Kavadarlı
Software Developer

Görkem Gökçe
Senior Customer Manager

CONTENTS

BKM BANKALARARASI KART MERKEZİ

Microsoft

VERİPARK