**Milton Friedman Egyetem**

**A képen szimbólum, embléma, Védjegy, Betűtípus látható

Automatikusan generált leírás**

**Blockchain as a secure and efficient identification system**

BID-Walled

Györki Attila, Dobi Szabolcs, Meződi Patrik

Table of contents

[1 Project description 3](#_Toc165964993)

[1.1 Topic 3](#_Toc165964994)

[1.2 The goal 3](#_Toc165964995)

[1.3 Requirements 4](#_Toc165964996)

[2 The system 5](#_Toc165964997)

[2.1 Definition of state-controlled provider/agency types 5](#_Toc165964998)

[2.2 Functionality of BID-Walled 7](#_Toc165964999)

[3 Requirements of the system 10](#_Toc165965000)

[3.1 The Blockchain 10](#_Toc165965001)

[3.1.1 Block structure 10](#_Toc165965002)

[3.2 Functionality of transactions 13](#_Toc165965003)

[3.2.1 Types of transactions 13](#_Toc165965004)

[3.2.2 Transaction process 14](#_Toc165965005)

[3.2.3 Attributes 15](#_Toc165965006)

[3.2.4 Validation 16](#_Toc165965007)

[3.3 Actors 17](#_Toc165965008)

[3.4 Structure of the network 18](#_Toc165965009)

[3.5 Smart contracts 21](#_Toc165965010)

[4 Human resource needs 22](#_Toc165965011)

[4.1 Development Team 22](#_Toc165965012)

[4.2 Networking Team 22](#_Toc165965013)

[5 Roadmap: Developing and implementing 24](#_Toc165965014)

[5.1 Phase I: Primary identification cards 24](#_Toc165965015)

[5.2 Phase II: Secondary Documents 24](#_Toc165965016)

[5.3 Phase III: Other public administration 25](#_Toc165965017)

[5.4 Phase IV: ISPs and TSPs 25](#_Toc165965018)

[5.5 Phase V: Bank sector 25](#_Toc165965019)

[6 Summary 25](#_Toc165965020)

# Project description

## Topic

The goal of the project is to create a blockchain-based identification and digital signature facility linked to a single plastic card. The disadvantage of the current system is that an adult citizen needs at least four forms of identification (ID card, social security card, tax card, address card), and optionally a driving licence, bank card, credit card. Administrations are inflexible, even though our data is already stored in one place, it must be re-entered, scanned, and stored at the next service provider/office. Stored in a blockchain-based BID-Walled (*BID: BlockChain ID; walled: enclosed within walls, especially for protection or privacy)*, it would be enough to authenticate our identity with an NFC-compatible plastic card, while it could also be used to sign contracts, as it would be protected by a multi-factor authentication method. (The card would have to be physically with us, authenticated with a PIN in the first instance, and then finalised with another authentication method such as SMS, email, or a dedicated app).

The project would, among other things, speed up the administration, reduce the state's expenditure on issuing documents, increase data security and reduce the administrative burden on offices and service providers.

A képen szöveg, képernyőkép, Betűtípus, dokumentum látható

Automatikusan generált leírás

## The goal

Our Team wants to reach the following goals with this project:

**- Blockchain-based identification and digital signature:** the project aims to create a blockchain-based system that allows identification and digital signature using a single plastic card.

**- The need for a single card:** the aim is to allow people to have a single card with all the necessary identification and verification data.

**- Flexible administration:** instead of the current inflexibility of administrations, we should have a single point of entry in the system, making data easily and quickly accessible to different service providers and agencies.

**- Use of NFC compatible cards:** NFC compatible plastic cards allow fast and secure identification and digital signatures.

**- Multi-factor authentication:** use multi-factor authentication methods to protect data and signatures, such as PIN, SMS, or app-based authentication.

**- Speed up administration:** the new system would allow faster administration by simplifying data access and verification.

**- Reduction of public costs:** The project is expected to reduce public costs as fewer documents would need to be issued.

**- Increase data security:** The use of block-chain technology and multi-factor authentication methods would increase data security by making it more difficult to gain unauthorised access to data

## Requirements

Requirements for the project:

* presentation of the system, disadvantages of current systems, advantages of new system
* defining data protection aspects
* formulating technological challenges
* opportunity for development
* plan of implementation
* defining necessary HR-resources

# The system

The system would be run by a central main system, supervised, and insured by the state. Economic and legal operators would be able to register with the system in a certified and secured way, which would categorise their activities.

Each category would have state-regulated access and write rights. The "Education Office", for example, would not have access to bank account statements or land registry title deeds, while the bank would not have access to graduation results. Each category, subject to data protection rules and following the principle of "as little as necessary", can only see what it needs to do its job and can only create the blockchain that its category justifies.

## Definition of state-controlled provider/agency types

One of the basic objectives of the system, data protection, should be laid down in law at the state level. The basic categories of people to be included in the system and the 'read' and 'write' rights of these categories must be defined. It is a basic requirement for a bank to be able to store data related to banking services in a blockchain (such as bank account number, bank statement, credit debt, etc..), and for this, it may need access to data such as ID card number, address or residence, last 3 or 6 months bank statement stored at another bank, or in the case of a mortgage, the title deed of a property, documents proving its encumbrance-free status.

These circles should be managed in the main system and managed in smart contracts tailored to the specific service sector. The following service sectors are identified for the system:

* public
  + document office (registration and drafting of identity documents)
  + education office (registration and editing of study data)
  + land registry (keeping and editing records relating to real estate ownership)
  + Labour office (registering and editing labour data - registration, duration of working time, etc.)
  + tax office (registration and editing of tax files)
  + health office (recording and editing health data)
  + pension fund (monitoring pension contributions and data)
  + Vehicle Register (Vehicle Service Platform) (vehicle ownership data management)
* privacy:
  + bank
  + ISPSs and TSPs (internet- and telephone service providers)

Given the diversity of employers and educational institutions, there individual access would not be provided by the system, but employers would be able to access data by communicating with the employment office, while educational institutions would be able to access data by communicating with the education office, and the obligation to notify would be part of the communication with them. Once a new employment contract is signed, the employer would send its data to the office, which would store it (declared salary, start date, type of employment, etc..) on the blockchain.

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírásA képen szöveg, képernyőkép, diagram, kör látható

Automatikusan generált leírás

*Blockchain structure and write permissions*

*A képen szöveg, képernyőkép, diagram, tervezés látható

Automatikusan generált leírás*

*Reading permission*

## Functionality of BID-Walled

After the various privileges have been established, the card itself can be created and its functionality and definition clarified.

The first block of the card would be made up of personal data (essentially integrating all our current ID card numbers), would be equipped with an NFC-enabled chip when created and would be equipped with a 6-digit PIN code chosen by the citizen. In addition, an additional authentication (2-factor authentication) method would be added to the card to ensure that it could not be misused if it fell into the wrong hands, even if the PIN was known. The second factor could be email, phone number (or even biometric) identification.  
 The protection of the card is particularly important when considering its functionality.

With a freshly produced and state activated "Personal Blockchain" (hereinafter "Chain Card"), you can do everything quickly. When opening a bank account or making a telephone payment, it is not necessary to hand over a separate identity and address card, it is sufficient for the bank to scan the Chain Card, which the citizen confirms with a password and a second authentication method, and the bank will have access to the legally regulated data parts that it needs to open the bank account. The bank performs the data capture in its own system, the contracts are presented to the customer, and the customer can then digitally sign the contracts by scanning his card and re-authenticating, essentially giving the bank "permission" to create a new blockchain (which in this case is the bank account data, the bank account contracts, privacy notices, etc.).

A képen szöveg, diagram, képernyőkép, sor látható

Automatikusan generált leírás

*Verification*

When changing data, for example to switch to a larger package with your phone provider, you accept the contract by scanning the Chain Card and digitally sign it with two-factor authentication, giving you permission to add another block to your chain.

The Chain Card is a three-factor authentication system for digital signatures (you need the physical card, the password and a third method at the same time), which allows you to sign contracts and give your consent to the service provider to access a certain part of your blockchain (personal data). To increase system security, authentication by email or SMS also provides an opportunity to include in the message not only an authentication request, but also precise information about exactly what data the other party wants to see or record (like the way it is currently done, when an application is launched, the application informs you what data it wants to access.)

A képen szöveg, diagram, képernyőkép, sor látható

Automatikusan generált leírás

*Signing contracts*

# Requirements of the system

## The Blockchain

### Block structure

The blocks must be able to store all the data generated during transactions, including personal data and documents. The amount and quality of data will vary, so it can be simple data (ID number, date of birth, etc.) and even documentary data (bank statement, employer's certificate...), but it must also include "transactions", which currently means data updates, queries, and contracts.

As an example, imagine that the structure of a block could be as follows for the project described above:

* **Block header:** Contains the block ID, the ID of the previous block, the time the block was created and other metadata.
* **Transaction data:** includes all transactions within a block, such as data updates, data queries or contracting.
* **Data**: contains all data stored in the block, including personal data and documents.
* **Hash:** thehash value of the block content, which ensures data integrity and block chaining.
* **Digital signature**: a digital signature of the content of the receipt that ensures the authenticity and security of the data.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírás

#### Header

* **Block** Identifier: this is a unique identifier that uniquely identifies a block among other blocks in the block chain. Usually, to speed up access to the block, the block identifier can be the hash value of the block.
* **Previous Block Identifier**: this is the identifier of the previous block to which the current block is linked. It ensures the continuity and chaining of the blockchain.
* **Timestamp:** the time or timestamp when the block was created, indicating when the block was created. This helps to keep track of the chronological order of data in the blockchain.
* **Metadata**: This can be optional data that contains additional information about the block. For example, metadata could be the number of transactions stored in the block, the block creator ID, or any other relevant information.

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

#### Transactions

Transaction data is the information stored within the block that documents its transmission and changes in the blockchain. For the above-mentioned project, which aims at a blockchain-based personal identification and digital signature system, transaction data contains information that identifies individuals and their digital signatures and related activities.

The structure of transaction data can be:

* **Transaction** Identifier: a unique identifier that uniquely identifies a transaction in the blockchain. This is usually the hash value of the transaction.
* **Sender and Receiver** Identifier: the identifiers of the entities involved in the transaction. These can be individuals, companies or other entities that use a digital signature for identification.
* **Digital Signature**: a digital signature generated by the sender to certify that the transaction has been authenticated by the appropriate user. This ensures the authenticity and integrity of the data in the blockchain.
* **Transaction Amount**: in our case, this is personal identification data or documents, certificates, contracts.
* **Transaction Status**: the status of a transaction, such as successful or unsuccessful. This can help you track transactions and identify potential problems.

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

#### Data

In the "Data" section, the following information can be found in the block:

* **Personal data and documents**: this includes the identification data of individual users and the documents they generate, such as ID cards, tax cards, bank account statements, etc.
* **Transaction hashes**: these are the hashes of the transactions in the block that are recorded in the block, but not the transactions themselves.
* **Metadata**: information related to the block, such as block creation time, block size, difficulty level, etc.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírás

#### Hash

A "checksum" or "hash" is a summation of the data in a block, which results in a unique identifier and helps to maintain the integrity and security of the block. It creates a hash from the block's timestamp, transactions, data, header, and the hash of the previous block, so integrity is assured, as even a single character change will break the integrity of the blockchain (the hashes will not match).

A képen szöveg, Betűtípus, képernyőkép, Acélkék látható

Automatikusan generált leírás

#### Digital Signature

While the checksum ensures data integrity and block chaining, the digital signature guarantees data authenticity and security. It contains the signature associated with the block, a key important element of cryptographic security and identification. The digital signature concatenates the contents of the block, including the block header and all transactions, into a single string and hashes this string. The resulting hash value is ultimately the digital signature. The digital signature is therefore the special cryptographic signature associated with the data, while the checksum (hash) is just a unique identifier for the block contents.A képen szöveg, képernyőkép, Betűtípus, diagram látható

Automatikusan generált leírás

## Functionality of transactions

### Types of transactions

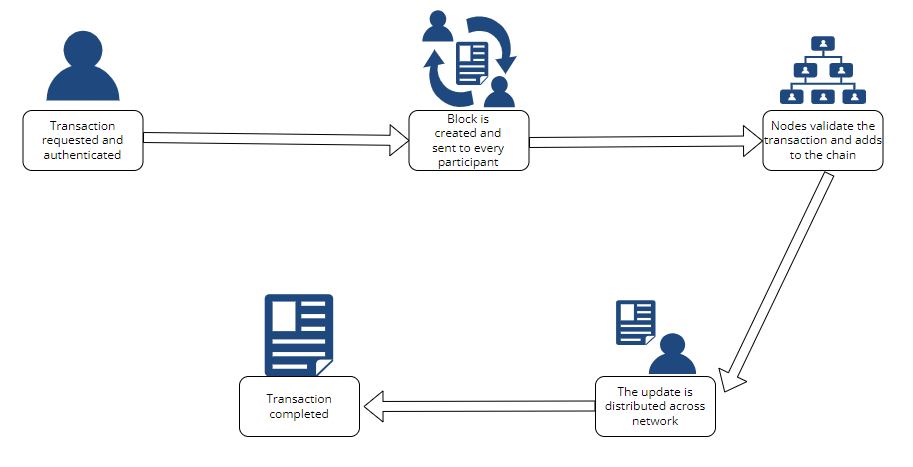
In the light of the specificities of the project, transactions here do not mean real transactions, money flows, but data operations, so several types need to be defined, considering the nature of the data and the application areas of the blockchain.

* **Data updates (*writes)***: these are "transactions" when a user updates or modifies data already stored in the blockchain. For example, if a user changes his/her address or updates a contract, a data update transaction is recorded on the blockchain network. Since it requires a lot of calculation to overwrite an existing block (they are linked to each other, and all the hashes are built on each other, and changing an existing block means that the whole ledger must be recalculated), when there is no “overwriting” in the system. Instead of that, a new block is created, what contains information about the “expired block”. To maintain the amount of data is stored, it can be made a maintenance cycle when the unused blocks are removed, and the whole ledger is recalculated, considered the load on the network. (For example, this maintenance should be taken night time or Sundays, planned and widely separated to keep the business running).
* **Data queries (*read)***: the purpose of data queries is to retrieve one or more data from the blockchain. These transactions do not modify the data, they only read it. For example, in a banking application, a customer would initiate a data query transaction to retrieve the balance of his/her bank account, or a bank administrator would request a data query to identify the customer.
* **Record new data (*create new block)***: this transaction type is created when new data needs to be added to the block chain, creating a new block. For example, the registration of a new user into the system would result in a new data capture transaction containing the new user's personal data.
* **Contracting (*digital signing, writing)***: contracting transactions are events where two or more parties enter into an agreement in a contract and this information is recorded in the blockchain. For example, two business partners would enter into a new business agreement and this contract would be recorded on the blockchain in a contracting transaction, or a customer might order a new telephone service.

Each transaction type can have different and distinct effects on the blockchain network and blocks. It is important to properly define these transaction types to ensure data integrity, security, and application efficiency in the project.

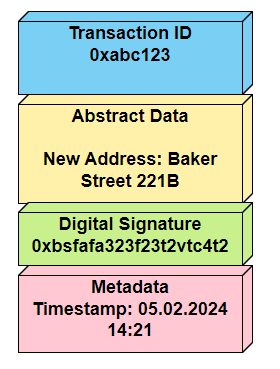
### Transaction process

* **Transaction creation**: during transaction creation, users or systems prepare and compile the necessary data to execute the transaction (in a GUI, graphical user interface, for example by filling in a form). This step involves the collection and formatting of data for the transaction, for example, if a user changes their personal information, this new data is collected and prepared during the transaction.
* **Transaction signature**: once the transaction has been created, it must be digitally signed by the user. This digital signature ensures the authenticity and accessibility of the data. The digital signature is a cryptographic method that identifies and verifies the origin of the transaction. In practice, this can be done using a plastic card, via NFC, by entering a code.
* **Transaction forwarding to the network**: transactions are forwarded as a network packet to all participants in the blockchain network. This process is usually done through peer-to-peer network communication, and transactions are received and checked by all network nodes.
* **Add transaction to block**: transactions are recorded in the blocks of the blockchain. Before being included in the blocks, transactions must be validated to ensure that they are valid and comply with the rules of the blockchain protocol. If the transactions are successfully validated, they are added to the blockchain network in which the transaction is included.



### Attributes

* **Transaction ID**: A unique identifier assigned to each transaction. This can be a hexadecimal or text identifier that uniquely identifies the transaction on the network.
* **Abstract data**: this data is the subject of the transaction itself, for example, a new address in the case of a data update. This data can be in text or binary format, depending on the type of data.
* **Signature**: a digital signature that ensures the authenticity of and access to data. This cryptographic method identifies and verifies the origin of the transaction to ensure the security of the data.
* **Metadata**: this is additional information that can help identify and manage the transaction. For example, the time the transaction was created, the addresses of the sender and recipient, or other transaction-related information.



### Validation

* **Signature verification**: the validation nodes of the blockchain verify that the digital signatures attached to transactions are genuine and valid. Various cryptographic algorithms, such as ECDSA (Elliptic Curve Digital Signature Algorithm), can be used for this purpose.
* **Transaction rule checking**: the blockchain must check that transactions comply with the network's defined rules and protocols. This includes, for example, checking the format, size, and other technical parameters of the transaction. If the transaction does not comply with these rules, it can be rejected.
* **Integrity and authenticity checking: the** network checks the integrity and authenticity of the data related to the transaction. This may include, for example, authenticating transaction-related data and checking its consistency with information from other systems or data sources.

A képen szöveg, képernyőkép, diagram, tervezés látható

Automatikusan generált leírás

## Actors

In defining the participants and roles in the project, we first need to have a comprehensive understanding of the actors involved in the system and their roles and responsibilities in storing and managing the data. It is important that the definition of roles reflects privacy and security considerations as well as business objectives and requirements.

* **Users**: these can be the average users who register with the system and store or manage data on it. For example, John Doe, who wants to store his personal data and documents in the blockchain, to make a transaction, to conclude a contract. But so is a bank, a telephone company, or an education authority.
* **System administrators**: these are the people responsible for the operation, maintenance, and supervision of the system. They ensure that the system is kept up and running and control access and privileges. For example, an IT department responsible for maintaining and monitoring the blockchain network.
* **Data controllers**: these actors are responsible for the management and secure storage of data within the system. They manage access to data and rights for users and other participants. For example, a data protection specialist who monitors and manages data access and security in the blockchain.
* **Authenticators**: these actors are responsible for the authentication and verification of data in the system. For example, a central authentication service that verifies and confirms the authenticity and validity of data in the blockchain.

These roles may overlap and complement each other, depending on the functions and responsibilities they must perform in the system. It is important that all actors have appropriate access and privileges to access and manage data, and that these roles reflect the privacy and security principles of the blockchain network.

## Structure of the network

One of the main strengths of blockchain technology is the tamper-proof nature of the data, because instead of a piece of data being centrally stored in a database, everyone has a "copy" of that blockchain. In centralised databases, if data is tampered with at the centre, from then on, it is difficult to trace back what is valid data and what is not. For blockchains, on the other hand, it is a different story. As described above, all changes go through validations, and it is useless to rewrite a point in one block, because all other points still contain the real data. However, the point of our project is precisely to avoid unnecessary data storage and to avoid data being managed by someone who only needs it twice a year or less. All data should be stored in as few places as possible and where it is generated, where it is used. Following the principle of 'need-minimum', only store what the bank needs for its day-to-day work but maintain the means for it to always have access to the data.

A képen szöveg, képernyőkép, Betűtípus, tervezés látható

Automatikusan generált leírás

In terms of offloading validations from sectors and maximising privacy, a block would be placed in two places: once with the State as a complete block, since the State has the largest resources and the greatest responsibility towards citizens, and in pieces with the other participants in the network. (The Land Registry and Educational Authority in the example are also part of the State, so it is important to note that by "Government" we mean the State as the central authority, the "operator" so to speak).

A képen szöveg, képernyőkép, diagram, Színesség látható

Automatikusan generált leírás

The speed and resource allocation of validation can thus be distributed among the actors in the network: the central state participant can validate any block, while the other actors can only validate the associated one. Following the current three-factor authentication (physical card, PIN, SMS/app/email), two additional actors will join for security: one public and one semi-public. Of course, the depth of validation can be further increased here, as we can expect up to multiple nodes/nodes to be confirmed per sector. This scheme could be further developed and extended in the direction that the state would operate all "archival full nodes", on which the complete blockchain is stored, and the sectors would only operate "pruned nodes", where only the end of the blockchain of a given length is included and used.

Instead of a duplicate chain in the shape of an L, another solution could be to have a copy of each chain for each actor in the network, following the classical example. In this case, each actor would have its own validation nodes and the transaction, i.e. data modification or data entry, would be accepted after a certain number of confirmations.

A képen szöveg, képernyőkép, rajzfilm, tervezés látható

Automatikusan generált leírás

Data security and integrity can be further enhanced by not only validating a transaction by checking nodes in its own sphere, but also requiring confirmation from more spheres, which spreads the load across different providers and increases security by talking about multiple, separate sectors. To distribute the system architecture and the network load, each sphere would have a small number of "archival full nodes" where the entire blockchain is stored, while a larger number of "pruned nodes" would assist the daily validation processes, where only the last X number of elements of the blockchain would be stored and validated.

## Smart contracts

A smart contract is a computing protocol that is automatically executed when certain conditions are met on the blockchain network. It is a programmed contract that executes business agreements between two or more parties without the need for intermediaries or third parties.

A smart contract usually consists of the following parts:

1. **Code**: the smart contract program code that defines the tasks to be performed and the behaviour.
2. **Conditions**: the conditions under which the smart contract is executed. These are usually pre-defined conditions or events, such as time limits or the execution of other transactions.
3. **Execution environment**: the environment or platform required to run the smart contract, enabling it to run and execute on the blockchain network.

In our project, smart contracts would provide access management and read/write permissions. Upon connection to the system, each actor (state, government, agency, bank, phone provider, etc..) would be assigned to a category, and each block would have a "character identifier" (e.g. personal data, bank data, land registry data, etc..), and then these categories would be managed through the smart contract.

Smart contracts would be responsible for managing and controlling access rights in the project:

1. **Storage of access rights**: access rights associated with each block type and actor type would be stored in smart contracts.
2. **Access rights management**: smart contracts would allow adding new access rights, modifying, or deleting existing rights.
3. **Checking Access on Transaction Queues**: before each transaction, smart contracts would check that the originator of the transaction has the appropriate access rights to the block.
4. **Smart contracts for blocks**: each block type would have a separate smart contract to manage access rights for that block.

This structure would allow each actor to access only the blocks it is allowed to access, and to read or write only to blocks of the type it is allowed to. Smart contracts would ensure strict access control and guarantee the security and integrity of block content on the network.

The smart contract code would define access rights for each block type and actor.

**For example**: the smart contract of the government window would contain the codes and conditions for which actors are authorized to read and write to the block containing tax information. If a citizen wants to modify his/her tax information, the government branch smart contract would check if the citizen had access rights to this block and only authorize the transaction if the citizen has the appropriate access rights. For this project, each block type would have a separate smart contract that manages the access rights for that block:

* The smart contract for the **Personal data** block can only be written and read by the steering wheel.
* The smart contract for the **Bank Data** block can only be read and written by the bank.
* The smart contract for the **Property Data** block can only be written and read by the land registry.
* The smart contract for the **Education Data** block can only be written and read by the education office.

# Human resource needs

Given the complexity of the system, it requires a diverse and highly experienced team to implement it, ranging from network specialists to senior developers, and even so raises several feasibility issues such as network congestion, data flow manageability, and data protection guarantees.

## Development Team

The system needs to use several languages in combination, so it is essential to have a team that can develop in Solidity, JavaScript/TypeScript languages at a high level, and a strong front-end team, as all end-users (citizens, service providers, government administrators) need to work on a single visual interface. But we cannot forget about smart contracts or the various APIs:

* **Blockchain developer**: a professional with in-depth knowledge of blockchain technology and platforms. Ability to develop and integrate applications into blockchain networks, as well as create various smart contracts and decentralized applications.
* **Backend developers**: responsible for the development of the backend part, which includes the business logic and data management of blockchain-based applications. They are familiar with databases, APIs, and server-side programming.
* **Frontend developer**: a professional responsible for the design and development of user interfaces (UI/UX). They are familiar with web technologies such as HTML, CSS, JavaScript, and frameworks such as React or Angular.
* **Smart contract developers**: specialised developers who develop and test smart contracts in blockchain networks. They are familiar with Solidity or other smart contract languages and best practices for designing and developing decentralized applications.
* **Tester/QA specialist:** responsible for testing and quality control of developed applications and smart contracts. Ability to perform automated and manual tests to ensure stability and functionality of applications.
* **Product Manager**: the team leader responsible for coordinating and managing the project. Communicates between the team and the customer, prioritises tasks and ensures that applications meet business objectives and customer needs.

## Networking Team

In the project, we only used a few actors for the examples, but building the full system is a huge network challenge, so it is essential to build a team of network developers with complex knowledge, so the next generation of team members is definitely needed:

* **Network systems engineer**: design, deploy and configure blockchain networks. Knowledge of network architectures and protocols and ability to optimise network performance and scalability.
* **Security specialist**: responsible for the security and vulnerability monitoring of blockchain networks: can identify and manage security risks and develop and monitor security strategies and tools.
* **DevOps specialist**: knowledge essential for the continuous integration and continuous delivery (CI/CD) of blockchain applications. They help automate development processes and ensure fast and reliable release of applications.
* **Network administrator:** responsible for the day-to-day operation and maintenance of blockchain networks, monitoring network performance, managing network devices and infrastructure, and ensuring network availability and stability.
* **Blockchain expert**: A professional with in-depth knowledge of blockchain technologies and platforms. They help you design and implement projects and optimise the scalability and performance of your applications.

In addition, of course, it also requires a lot of human resources outside the IT world, such as strategic management, a financial team to manage the project budget, legal, data protection, or marketing and communication specialists.

# Roadmap: Developing and implementing

Given the complexity of the system, it should be considered that it is not possible to develop the whole system in a "lab" and then replace the current system overnight, so it should be broken down into development phases, as a public system migration of this scale can take up to 5-8 years. The phases need to be defined, with a carefully planned pilot period for each phase, so that any errors or shortcomings that may occur during use can be addressed in time. The development phases and draft implementation plan described below are only indicative, and it is clearly worth a separate study to work out the steps to be taken to introduce it into a country's public administration. It is important to note that even just completing the first phase would be a major administrative success.

A képen szöveg, képernyőkép, sor, Diagram látható

Automatikusan generált leírás

## Phase I: Primary identification cards

Considering the nature of what the system is being built on, the first phase would be to replace the basic four ID cards. Every adult citizen in Hungary has an identity card, a residence card, a social security card and a tax card. Of these, the primary ID cards are the ID card and the address card, which gives a good starting point for the implementation of the system. In the first phase, the system would be more restricted and the blockchain would consist of only two blocks: the digitised data of the ID card in the first block and the digitised version of the address card in the second block. At this stage, it could be interpreted as a pilot phase that the old documents are not yet replaced by the new blockchain technology BID-Wallet, but only the newly issued ID cards are entered in this way. After a certain number of issued documents and a certain pilot period, the old documents will be withdrawn and replaced in several phases, with a final date set for the phase when the last document belonging to the old system will be withdrawn. (This could be up to 10 years, as the expiry date of the document issued on the day before the first day of implementation will be exactly 10 years from now). During the pilot period, the operation should be continuously monitored to ensure that it is working as expected and to address any errors or shortcomings that may arise, be it a data protection issue or the handling of situations not considered during development.

## Phase II: Secondary Documents

The replacement of the remaining two ID cards (social security card and tax card) can be started in time from the launch of the first phase of the phase. The digitisation of the two cards can be done in parallel or separately. As in the previous phase, the pilot phase would mean that newly issued documents would be issued digitally using only blockchain technology. If a citizen is included in the pilot phase of "Secondary IDs" who was not included in the pilot phase of "Primary IDs" and therefore does not yet have a blockchain-based ID document, the citizen would automatically be included in the previous pilot phase and all four documents would be block-chained at the same time.

## Phase III: Other public administration

If the first two phases have been successfully launched and the pilot phase can be declared a success and its shortcomings and issues addressed, we can move on to the third phase, while remaining in the public sector. This is where all the other documents and offices related to public administration would be added to the system - of course, broken down into several phases - the blockchain: land registry documents, education office, employment office, etc. The definition of the phases requires careful planning, as there may be parts that can run in parallel, but care must also be taken to consider the system's load-bearing capacity to ensure stable operation.

## Phase IV: ISPs and TSPs

The fourth phase is the first major leap: so far, blockchain has grown in the public sector, and this is the first point where the system needs to be further developed in the private sector, with the involvement of various service providers. It is very important to put in place the legal and regulatory framework for this, to give service providers sustainable dates and to continue to break down the phase into sub-phases. For example, even by launching a public tender to find just one telephone operator to launch the system in pilot version, and once the public/operator blockchain relationship is stabilised and initial bugs are addressed, the tried and tested system can be rolled out to the rest of the market.

## Phase V: Bank sector

The fifth (and final phase of our project at this stage), which should be less technically challenging, based on years of experience, but perhaps one of the most sensitive steps in terms of the sensitivity of the sector (mixing financial and personal data). It is precisely for these reasons that we believe that the final stage of implementation should be the involvement of banking service providers, as it would be dangerous to enter this sector without experience of operating the system. Although the most famous use of blockchains is in the financial area (cryptocurrencies), in our case, the blockchain would mix personal data with financial data, and therefore requires extreme caution.

As mentioned at the beginning of this paragraph, this roadmap is only a guideline example, clearly its elaboration deserves a full project document and the joint work of legal, economic and IT experts. Legislation, societal resilience (resistance, if any?) to change, financial constraints, network load and a host of other factors will have a profound impact on the development of the roadmap.

# Summary

Our project is exploring a completely new and bold use of blockchain and wants to find a way to implement it. As it turns out, when building such a system, even a 25–30-page document is enough to just reveal the outline, present the idea and scratch the surface. Clearly, building this is a huge project, with the help of a lot of highly skilled and experienced professionals. Our goal - that the vast number of documents, certificates, certificates, and contracts could be collected on a blockchain - is achievable, the direction is forward-looking, and although it will take a lot of time and money to build and implement, the payback is priceless.

 How much time do we spend in offices in a year? How much time and effort do we spend requesting documents in one place and transferring them to another? How many ID cards and cards do we currently have in our wallets? How many plastic cards are currently in circulation?

The best example of trust in blockchain is cryptocurrency. But if the system is so secure, why should we only keep our money there? Why not keep our entire wallet?