Public Sector Lending Transparency

Section 1 Summary

Use Case Summary			
Use Case ID:	GOV-001	**Use Case Type:**	Vertical
Submission Date:	May 28, 2018	**Is Use Case supporting SDGs**	Yes
Use Case Title:	Public sector lending transparency	**Domain:**	Government and public sector
Status of Case	Pilot	**Sub-Domain**	Government and non-profit transparency
Contact information of person submitting/ managing the use-case	Full Name: Suzana Mesquita de Borba Maranhão Moreno (BNDES) Job Title: Software Engineer E-mail address: suzana@bndes.gov.br Telephone number: 55-21-993056325 Social media: https://www.linkedin.com/in/suzana-moreno/ Web site: https://www.bndes.gov.br		
Proposing Organization	BNDES, Brazil		
Short Description	This use case is a proposal for changing the process of lending projects in The Brazilian Development Bank using a stable coin with DLT technology. The main goal is achieve more transparency of the public money allocation. However, the new proposal achieve other benefits like operational costs reduction and the generation of data to support aggregate analysis of the benefits arising from the bank's loans.		
Long description	This use case is a proposal for changing the process of lending projects in The Brazilian Development Bank using a stable coin with DLT technology. The stable coin is used when disbursing money from BNDES to the client and from the client to contractors. Then, the contractor can redeem to get its fiat money. It is a closed ecosystem between BNDES, clients and contractors in order to avoid regulatory risks. In order to achieve the desired transparency, it is necessary to identify everyone who do transactions using the stablecoin. In future view, there is also important to identify services and products offered from contractors to clients. The main goal is achieve more transparency of the public money allocation. However, the new proposal achieve other benefits like operational costs reduction and the generation of data to support aggregate analysis of the benefits arising from the bank's loans.		
SDG in Focus (when applicable)	16 – Peace, Justice and Strong Institutions		

Value Transfer:	Tokens representing fiat money	Number of Users:	20+
Types of Users:	Development bank, Lender, Contractor, Society		
Stakeholders	Government, Development bank (or Public agency), Commercial banks, Lender, Contractor, Society, Auditor		
Data:	=> Use case shared data (ideally stored in DLT): - Entity identification (link between DLT account and real world entity identification) - Product or service type identification (Future Vision only) => Use case specific DLT data: - Account - Token balance to each account - Project identification - Instances of use case shared data identification => External data - not stored in DLT: - Entity additional information (number of employees, revenue, geographic region, industry, sector etc.) => All public information (see Security and privacy section).		
Identification:	Full identification of Lenders and Contractors required by the development bank		
Predicted Outcomes:	The predicted outcomes of the adopting the new process are to: - increase transparency of public money allocation - make clients' proofing of their spending simpler - reduce audit and compliance costs - improve public money allocation by postponing fiat money lending - minimize time to publish lending information - produce data to do aggregate analysis of the benefits arising from the development bank's loan		

Overview of the Business Problem or Opportunity
- In general, society demands more transparency in the use of public money. - The development bank uses public money to finance projects that adhere to government

development policies priorities.

- The society does not trust the development bank.

- The development bank needs to verify that the public money is being used as planned.

    - Periodically, lenders need to prove each money spending, including transfer to contractors.
    - The development bank needs to verify that lenders' proof correctly demonstrates that the public money was used as planned.
    - Auditors verify that the development bank indeed has assessed lenders' money spending.
    - Maximizing process automation would increase processes efficiency, while reducing the development bank's verification and audit costs.

- The process information of lending is fragmented.

    - The development bank owns the projects and disbursements data. Each lender or contractor has its transfer data.
    - Transfer data is protected by commercial banks - financial privacy.
    - The development bank has to collect transfer data in order to publish lending information to society.
    - The development bank does not have contractor's registry.
    - The development bank has to collect and group data to demonstrate benefits arising from the development bank's loans.
    - Integrating data would improve the process efficiency, while minimizing cost.

- In order to minimize paperwork, the development bank disburses to lenders large amounts of money.

    - Lenders take some time to spend all the money so they have to invest the funds. If the value of investment interest rate is bigger than the value of the lending interest rate, lenders may have an incentive to postpone the project schedule.
    - To make disbursement date and money spending date closer would improve the process efficiency and improve fiat money allocation.

Why Distributed Ledger Technology?

DLT would improve the current solution because it is possible to achieve public money loans transparency without trusting the development bank. Transfer data become easily accessible and can be used to make the underlying processes of lender's proof of money spending and the process of collecting and publishing loans benefits simpler and more efficient.

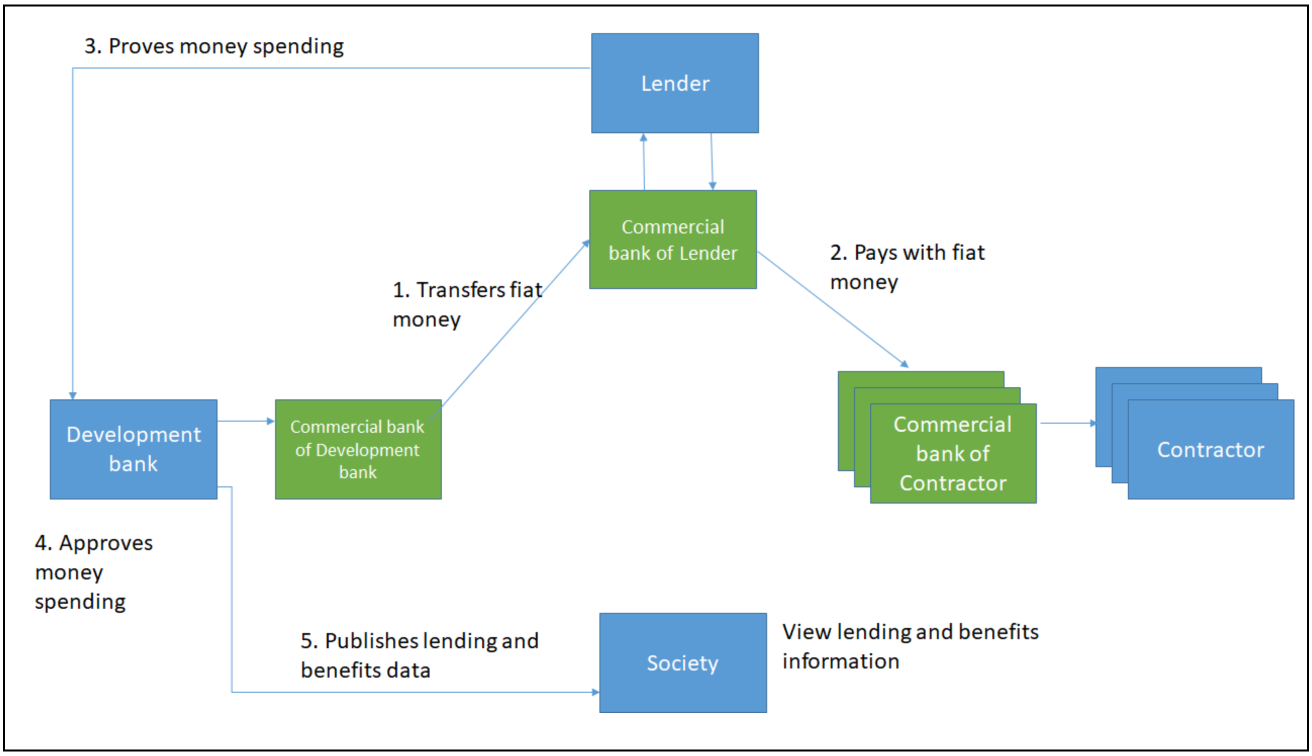
In addition, the use of DLT token enables the development bank to disburse fiat money just-in-time. Many times the money can flow to contractors directly.

Section 2 Current process

Current Solutions
Value is transferred by corresponding banks; There is a lot of manual work to prove and validate money spending; There is a lot of manual work to publish lending and benefits data; Lending and benefits data can be manipulated by the development bank; There is no data publication in real time.

Existing Flow (as-is)		
Step	**User Actions**	**System Actions**
1.	The development bank makes a transfer of fiat money to lender using the service of commercial banks.	The development bank's internal system registers the transfer Each commercial bank updates its ledger The lender's internal system registers the transfer
2.	The lender pays some contractors using a service of commercial banks. It can take a while to spend all money.	For each payment: The lender's internal system registers the payment Each commercial bank updates its ledger The contractor's internal system registers the payment
3.	The lender proves his money spending to the development bank.	The development bank system register the lender's spending proof
4.	The development bank approve lender's money spending. It can involve a lot of manual work.	The development bank system changes disbursement status
5.	The development bank publishes lending and benefits data	N/A

Process scheme (as-is)


3. Proves money spending
Lender
Commercial bank of Lender
1. Transfers fiat money
2. Pays with fiat money
Development bank
Commercial bank of Development bank
Commercial bank of Contractor
Contractor
4. Approves money spending
5. Publishes lending and benefits data
Society
View lending and benefits information

Data and information (as-is)		
Data	**Type**	**Description**
1	Fiat money transactions	The way value is transferred between: (a) the development bank and the lender and (b) the lender and contractors
2	Money spending proof	Documents, images etc used to proof the money was used as planned. It must include commercial bank statements to proof that the lender paid contractors and what products or services type were commercialized.
3	Lending data	Detailed information about each transaction, including who the lender and the contractors were, what time each transaction happened and what the value of each transaction was, what product or service type was commercialized in each transaction.
4	Benefits data	Aggregate information about transactions joined with entities additional information. Examples: How many transactions involved companies with small revenues? How much money was transferred in a geographic region or an industry?

Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	Development bank	Financial institution designed to provide medium- and long-term capital for productive investment

2	Commercial bank	Financial institution to provide transfer/payment between parts
3	Lender	Entity who takes the loan with the development bank
4	Contractor	Entity who sells a product or service to the lender
5	Society	Everyone who is interested to know how the public money was allocated and what were the benefits of that

Other Notes

Some steps must occur before the described use case but are not relevant to the description:

- The development bank must approve a development project within a contract. The contract must state the conditions of each public money disbursement;

- The lender must ask for a disbursement to the development bank;

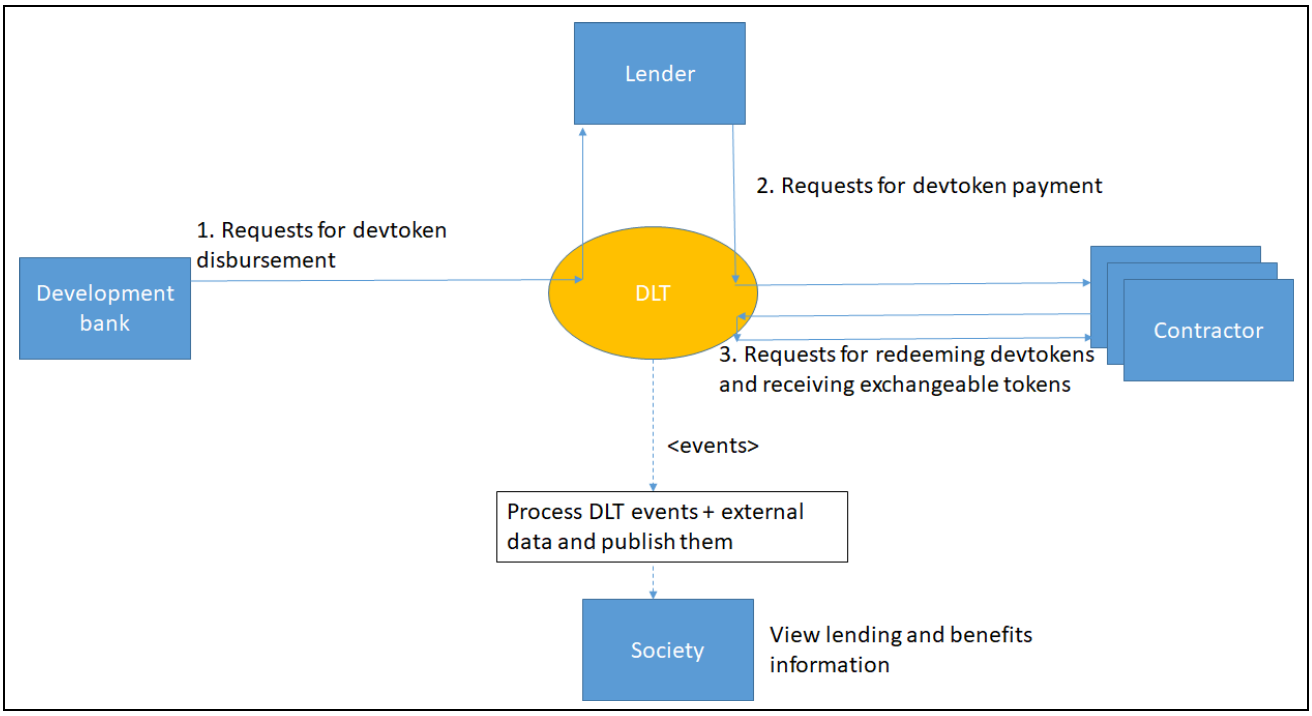
- The development bank approves disbursement to the lender.

Section 3 Expected process

Future Vision

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	The development bank requests for devtoken disbursement.	DLT checks the development bank is authorized and the lender is enabled to receive devtokens. If true, DLT mints new devtokens and transfers them to the lender's address. DLT emits <disbursement event>.
2.	The lender request for devtoken payment	DLT checks the lender is authorized and has enough balance and the contractor is enabled to receive devtokens. If true, DLT transfers devtokens to the contractor. **This transfer demonstrate what the product or service commercialized are. In addition, it has legal value to be used as lender's proof of money spending.** DLT emits <payment event>.
3.	A contractor requests for redeeming devtokens and receiving exchangeable tokens * At some point before, the development bank must input enough exchangeable token in DLT.	DLT checks the contractor is authorized and has enough balance and the smart contract has enough exchangeable tokens. If true, DLT burns the received devtokens, makes the conversion between the devtoken value and the exchangeable token value and transfers the corresponding exchangeable token value. DLT emits <redemption event>.
Trigger event	N/A	When a trigger event of DLT is observed, a system updates the lending and benefits information.

Process scheme (to-be)

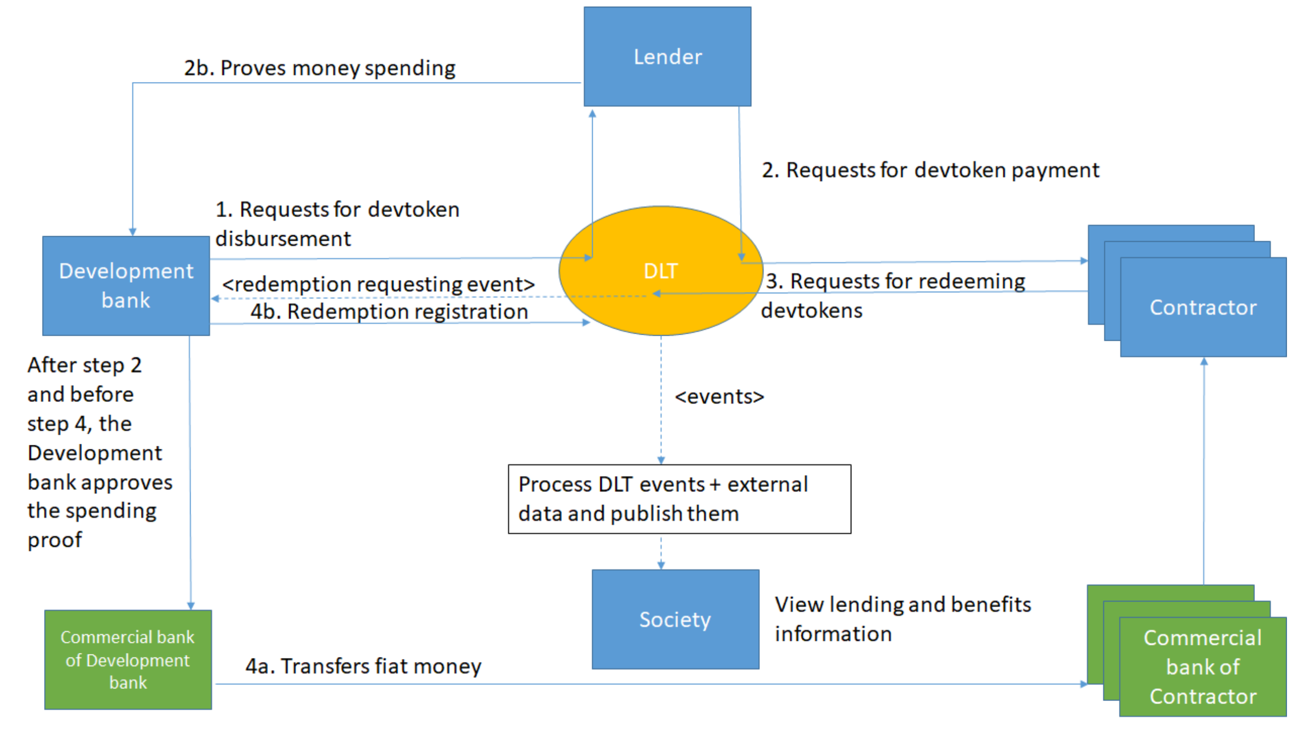

Lender
2. Requests for devtoken payment
1. Requests for devtoken disbursement
Development bank
DLT
Contractor
3. Requests for redeeming devtokens and receiving exchangeable tokens
<events>
Process DLT events + external data and publish them
Society
View lending and benefits information

Transition Vision

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	The development bank requests for devtoken disbursement.	DLT checks the development bank is authorized and the lender is enabled to receive devtokens. If true, DLT mints new devtokens and transfers them to the lender's address. DLT emits <disbursement event>.
2.	The lender request for devtoken payment. (2a) At the same time, proves his money spending to the development bank. (2b)	DLT checks the lender is authorized and has enough balance and the contractor is enabled to receive devtokens. If true, DLT transfers devtokens to the contractor. (2a) **This transfer does not demonstrate what the product or service commercialized. Then, although the transfer contains devtoken values*, it cannot be used as complete spending proof.** * Since devtoken values are available to DLT, it is possible to update published lending and benefits data when trigger event is fired. DLT emits <payment event>. The development bank system register the lender's money spending proof. (2b)
3.	A contractor requests for	DLT checks the contractor is authorized and has

	redeeming devtokens	enough balance. If true, DLT burns the received devtokens and emits <redemption request event>.
After step 2 and before step 4	The development bank approves the money spending proof.	The development bank system changes disbursement status.
4.	The development bank observe that a redemption request event has occurred. The development bank pays the contractor using a service of commercial banks. (4a)	The development bank's internal system registers the payment (4a) Each commercial bank updates its ledger (4a) The contractor's internal system registers the payment (4a) DLT emits <redemption event>. (4b)
Trigger event	N/A	When a trigger event of DLT is observed, a system updates the lending and benefits information.

Process scheme (to-be)


Lender
2b. Proves money spending
2. Requests for devtoken payment
1. Requests for devtoken disbursement
Development bank
<redemption requesting event>
4b. Redemption registration
DLT
3. Requests for redeeming devtokens
Contractor
After step 2 and before step 4, the Development bank approves the spending proof
<events>
Process DLT events + external data and publish them
Society
View lending and benefits information
Commercial bank of Development bank
4a. Transfers fiat money
Commercial bank of Contractor

Future and Transition Vision

Participants and their roles

Actor	Type/Role	Description

1	Development bank	Financial institution designed to provide medium- and long-term capital for productive investment
2	Commercial bank	Financial institution to provide transfer/payment between parts
3	Lender	Entity who takes the loan with the development bank
4	Contractor	Entity who sells a product or service to the lender
5	Society	Everyone who is interested to know how the public money was allocated and what were the benefits of that

Data and information		
Data	**Type**	**Description**
1	Devtoken	Token representing fiat money value. It is used to transfer value between: (a) the development bank and the lender and (b) the lender and contractors. It cannot be transferred to a entity who is not registered and enabled to receive devtoken. The token should only be used to execute the associated development project.
2	Fiat money transactions	The way fiat money is transferred between: (a) the development bank and contractors in the transitional vision
3	Money spending proof	Documents, images etc used to proof the money was used as planned in the transitional vision. It must include what products or services type were commercialized. It does not need to include commercial bank statements since this information is available at DLT.
4	Exchangeable token	A token that can be exchanged by fiat money or other cryptocurrency without use the devtoken smart contract.

Security and privacy
1.Since transparency is the main requirement, the ideal information visibility is public; 2. If business privacy prevent public visibility, this critical subset of data can be encrypted or protected; 3. DLT system should be able to provide mechanisms of DLT data integrity control; 4. DLT data and related services (System Actions) should be available in 24/7/365 mode; 5. The entity identity solution should prevent identity fraud. 6. The products and services type identification solution should prevent fraud. (Future Vision only)

Main Success Scenario
1. All information exchange and payments occur in Distributed Ledger in automatic mode; 2. Payments are transferred using digital currency (either devtoken or an exchangeable token);

3. Money spending proof occurs without human verification;

4. Lending and benefits data published without human intervention.

Conditions (pre- or post-)

1. The development bank must have established a financial contract with lenders;

2. Lenders and contractors who receive devtokens must be registered in the identity solution and enabled to receive devtoken;

3. Produts and servides types used in devtoken transactions must be registered in Product or service type identification (Future Vision only);

4. Devtoken smart contract must be deployed;

5. All parties are connected to DLT-network.

Performance needs

1. Transactions processing near real time;

2. 24/7/365 availability;

3. Volume of disbursements > 1000 Tx/day, volume of transactions > 10.000 Tx/day;

4. Lending and benefits data published in the moment they are available (near real time).

Legal considerations

Changing how a lender proves his money spending has legal impacts.

Risks

1. Legal risks, including regulation of cryptocurrencies, money spending proofing and taxation;

2. Security risks;

3. Contractors do not accept devtokens;

4. Lenders do not want devtokens;

5. Risks related to DLT immaturity.

Special Requirements

N/A

External References and Miscellaneous

1. Project using this use case =>

Brazilian State Bank to Tokenize Brazilian Real on Ethereum’s Public Blockchain - https://www.trustnodes.com/2018/03/06/brazilian-state-bank-tokenize-brazilian-real-ethereums-public-blockchain

Other Notes
1. For simplicity, this use case does not describe a scenario where: - Lender can request for redemption - Contractor can transfer devtoken again

Trubudget for the Amazon Fund

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-002	**Use Case Type:**	*Vertical*
Submission Date:	March 22, 2019	**Is Use Case supporting SDGs**	*Yes*
Use Case Title:	Trubudget for the Amazon Fund	**Domain:**	*4. Government and public sector*
Status of Case	*Pilot*	**Sub-Domain**	*b. Government and non-profit transparency*
Contact information of person submitting/ managing the use-case	*José Nogueira D'Almeida Jr.* *Software Engineer* *nogueiradalmeida@gmail.com* *+55 (21) 97189-2811* *https://www.linkedin.com/in/nogueiradalmeida/* ***www.bndes.gov.br***		
Proposing Organization	*BNDES – Brazilian Development Bank*		
Short Description	*Trubudget for the Amazon Fund is a blockchain system that improves the reliability of the information providing the money tracking for the investments of Amazon Fund in Brazil.*		
Long description	*The Amazon Fund is a REDD+ mechanism created to raise donations for non-reimbursable investments in efforts to prevent, monitor and combat deforestation, as well as to promote the preservation and sustainable use in the Brazilian Amazon.* *The Amazon Fund is managed by BNDES, the Brazilian Development Bank, which is responsible for raising and investing funds, monitoring the projects supported, rendering accounts and communicating results obtained.* *Germany is one of the main donors of Amazon Fund. The Germany's Development Bank KfW and BNDES are cooperating to use the blockchain technology to record how funding is spent. The Trubudget is a generic blockchain system that allows to register workflows. The Trubudget for the Amazon Fund is an use case that registers the money flow. It started in 2017, it had a Proof-of-Concept Phase in 2018 which consisted in simulations with real clients and in 2019 is in the Pilot Phase, which consists in real disbursement monitored and controlled by the blockchain. The payments process from BNDES to its Clients was the choice to be recorded on Trubudget blockchain in the Pilot Phase.*		

SDG in Focus (when applicable)	*Goal 6 – Clean Water and Sanitation* *Goal 13 – Climate Action* *Goal 15 – Life on Land* *Goal 16 – Peace, Justice and Strong Institutions* *Goal 17 – Revitalize the global partnership for sustainable development* *All these objectives are related to the Amazon Fund and the Trubudget aims to improve the management of it.*		
Value Transfer:	*There is no value transfer in the blockchain solution described. This is a declarative ledger.*	**Number of Users:**	*30+*
Types of Users:	*BNDES Business Analyst* *BNDES-Clients Business Analyst* *Auditors* *Donors* *Government agencies*		
Stakeholders	*BNDES, KfW(Germany), Petrobras, TCU (government agency), Norway*		
Data:	*Users* *Projects* *Subprojects* *Workflow items* *There is a communication between Trubudget and the ERP System, which every disbursement that occurs in the ERP, it makes a new record in the respective Trubudget Subproject.*		
Identification:	*Every user has credentials (login and password) to use the system. Some users have admin power, which means that they can create other credentials.* *Projects, Subprojects and Workflows items need permission of its owner to read/write.*		
Predicted Outcomes:	Trubudget aims to be an additional source of information in a blockchain for the stakeholders monitor the Amazon Fund projects. The system is able to provide the Client's, BNDES and Donors access to the same data at any time. This is similar to the Circularization technique commonly used by Audit companies, when the auditor sends a letter directly to a third party to confirm an information about the audited organization. In a future phase, it can replace some process/report that is currently made offchain.		

Overview of the Business Problem or Opportunity
The donors of Amazon Fund and BNDES could be concerned about the correct use of the disbursements for the projects executed by their clients, generally NGOs. This system can improve the timing of the information and the reliability of it.
Why Distributed Ledger Technology?
Every stakeholder (Donor, BNDES, Clients/NGOs) has its system and provide the information of money expenditure using the traditional ways (emails, documents, spreadsheets, receipts, etc). The Trubudget for the Amazon Fund integrates this information in one blockchain system, where

the data is immutable, secure, verifiable and transparent.

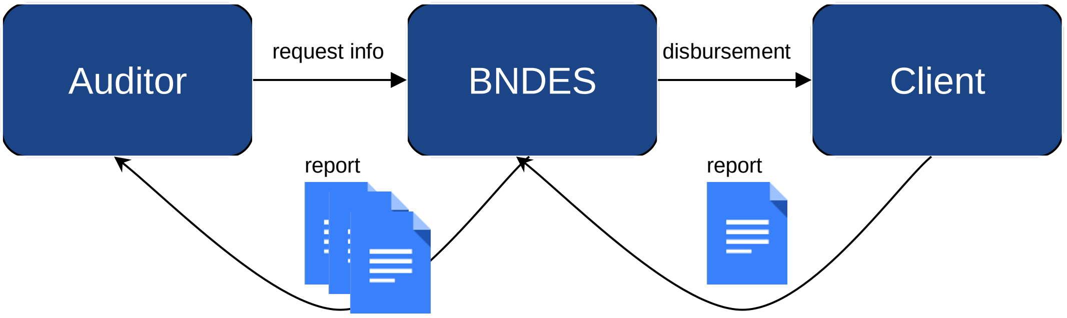
Section 2: Current process

Current Solutions
The disbursements of BNDES are made to its Clients using the traditional Brazilian Payment System (SPB). The Clients executes the project according to the Amazon Fund principles and then reports the expenditure to BNDES. BNDES aggregates all its Clients reports and make its reports to the donors periodically.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	BNDES Analyst submits a disbursement in the ERP system	The ERP system sends a disbursement through the Brazilian Payment System
2.	The Client checks the project bank account	No system action
3	BNDES periodically reports to the Auditor how and when the money was spent	No system action

Process scheme (as-is)



Data and information (as-is)

Data	Type	Description
1	*Documents*	A report of project ongoing results must be send to BNDES, who manages the Amazon Fund. BNDES collects all those results from its clients, make analysis and then produce its reports to the auditors (donors and government agencies).

2	*Payment transactions*	The Clients' expenditures receipts must be send to BNDES.

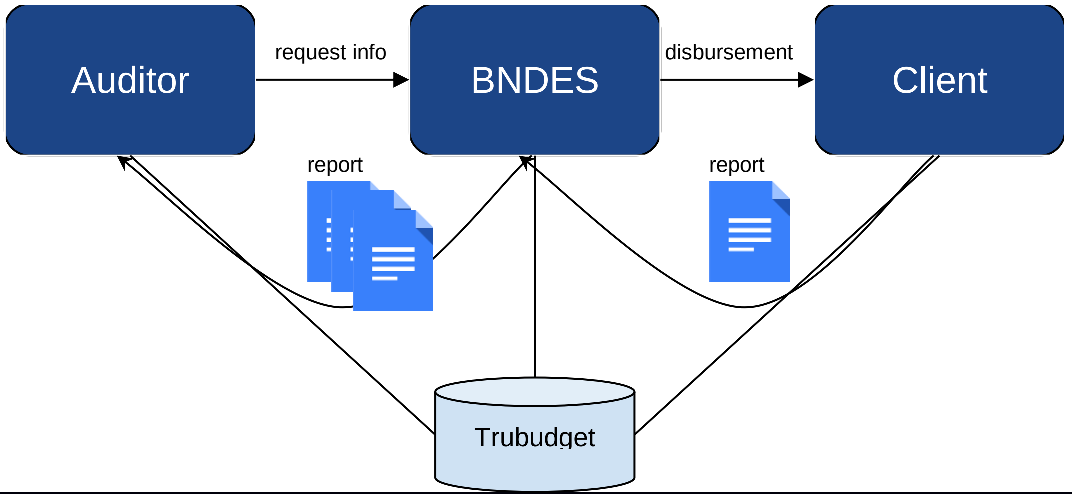
Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	*BNDES*	Manages the Amazon Fund and evaluate the results of ongoing projects and approves/rejects new projects
2	*KfW/Norway*	Monitor their donations and audit the BNDES management
3	*TCU (as example)*	Audit the BNDES Amazon Fund management
4	*BNDES Clients*	Executes the projects and report the results

Other Notes
N/A

Section 3: Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	BNDES Analyst submits a disbursement in the ERP system	The ERP system sends a disbursement through the Brazilian Payment System and this payment is loaded into Trubudget Ledger. Trubudget sends an email to the Clients
2.	The Client checks the project bank account and then approves the receipt in the Trubudget Ledger.	Trubudget sends an email to BNDES team
3	The Auditor logs on Trubudget at any time and check the money flow for every iteration described in the steps 1 and 2	Trubudget shows every money step through the ledger

Process scheme (to-be)



Participants and their roles		
Actor	**Type/Role**	**Description**
1	*BNDES*	Manages the Amazon Fund and evaluate the results of ongoing projects and approves/rejects new projects
2	*KfW/Norway*	Monitor their donations and audit the BNDES management
3	*Auditor*	Audit the BNDES Amazon Fund management
4	*BNDES Clients*	Executes the projects and report the results

Data and information

Data	Type	Description
1	*Documents*	A report of project ongoing results must be send to BNDES, who manages the Amazon Fund. BNDES collects all those results from its clients, make analysis and then produce its reports to the auditors (donors and government agencies).
2	*Payment transactions*	The Clients' expenditures receipts must be send to BNDES.
3	*Trubudget Workflow*	All the stakeholders can access Trubudget at any time to check daily the status of each project of the Amazon Fund.

Security and privacy
Application security: *The Trubudget has access control to login into the system, as well it offers specific permission for each project, subproject and workflow item.* *Network security:* *The Trubudget network is a permissioned blockchain based on Multichain. Therefore only the approved nodes have the grants to join on this. Currently there are two nodes: BNDES and KfW. Norway and Petrobras were invited to join. The Clients uses the BNDES frontend node.*

Main Success Scenario + expected time line
Description of DLT-based solution, which potentially will be created

Conditions (pre- or post-)
Not applicable

Performance needs
Trubudget is based on Multichain permissioned blockchain technology. *The confirmation time in a permissioned networked the can vary according to the consensus mechanism, number of nodes, etc. Trubudget does not require real-time update for all nodes. It is desired and viable a few minutes of confirmation time.* *Trubudget already contains a Restful API, which supports external calls from other systems.* *A few transactions per day are expected on Amazon Fund and since Trubudget is based on Multichain permissioned blockchain technology, the transaction throughput is not an issue.* *"In MultiChain you can set the block size limit much higher (up to 1 GB) and the block time much lower (down to 2 seconds), so based on this calculation it could process over 2 million tx/second. But for now the codebase itself can handle a little over 1000 tx/second on mid-range hardware, using either the multichain or bitcoin protocol. (In reality you would also have to consider the connection between block size and propagation latency which affects the minimum viable block time." [https://www.multichain.com/qa/5556/about-throughput-performance]*

Legal considerations

There is a possibility that Trubudget could not replace any of the current processes and/or reports because legal and regulatory rules. In fact, at this point, we are considering Trubudget as an additional source of information.

The General Data Protection Regulation in EU law was a concern because Trubudget stores every single data in its blockchain, including emails. Therefore, we decided to use corporate emails to keep only corporate data and avoid personal data.

Risks

Legal, business and technical risks related to use case

The information provided on Trubudget is already open and public by the Amazon Fund.

Trubudget is an opensource project under the MIT License. The software uses other opensource libraries and modules and these external modules can have vulnerabilities.

Special Requirements

The agreement between KfW and BNDES was formalized by a Memorandum of Understanding and if someone does not follow the rules, it can affect the business.

External References and Miscellaneous

KfW Trubudget site:

https://openkfw.github.io/trubudget-website/

Trubudget for the Amazon Fund Video Demo:

https://www.youtube.com/watch?v=0tysH44dzm8&feature=youtu.be

BNDES Trubudget site:

www.bndes.gov.br/trubudget

The Trubudget source code:

https://github.com/openkfw/TruBudget

The ETL SAP-Trubudget source code:

https://github.com/bndes/trubudget-bndes

Other Notes

Trubudget for Amazon Fund is workflow management system that tracks the money flow in a blockchain. Its use case is simple. It is an additional and reliable source of information for different stakeholders to follow the donations of the supported projects for the Amazon Forest.

Appendix 1:
Domains and subdomains for use cases categorization

Vertical:

1. Finance
    a. Financial management & accounting
    b. International & interbank payments
    c. Clearing and settlement
    d. Reduction of Fraud
    e. Financial messaging
    f. Asset lifecycles and history
    g. Trade finance
    h. Regulatory compliance & audit
    i. AML/KYC
    j. Insurance
    k. Peer-to-peer transactions
2. Healthcare
    a. Pharma
    b. Biotechnology
    c. Medicine
3. Industries
    a. Manufacturing
    b. Energy
    c. Chemical
    d. Retail
    e. Real estate
    f. IT and telco
    g. Supply chain management
    h. Transportation
    i. Agriculture
4. Government and public sector
    a. Taxes
    b. Government and non-profit transparency
    c. Legislation, compliance & regulatory oversight
    d. Voting
    e. Taxation and customs
    f. Intellectual property management
    g. Land Registries

Horizontal:

1. Identity management
2. Security management
    a. Public Key Infrastructure
3. Internet of Things

4. Data processing, storage and management
    a. Data Validation (includes provenance)

Mudamos - Lawmaking

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-003	**Use Case Type:**	*Vertical*
Use Case Title:	Mudamos	**Is Use Case supporting SDGs**	*No*
		Domain:	*List 1 Appendix 1 d*
Status of Case	*Implementation*	**Sub-Domain**	*If necessary*
Contact information of person submitting/ managing the use-case	*Marco Konopacki* *Project Coordinator* *marco@itsrio.org* *+55 21 999278090* *marco@itsrio.org* *@marcoamarelo* *http://itsrio.org* *http://mudamos.org*		
Proposing Organization	*Institute for Technology and Society*		
Short Description	*Mudamos is a mobile application that enables Brazil's citizens to participate in lawmaking by proposing their own bills and signing onto one another's proposals using verified electronic signatures.*		
Long description	*Mudamos is a mobile application that enables Brazil's citizens to participate in lawmaking by proposing their own bills and signing onto one another's proposals using verified electronic signatures. Any citizen with a smartphone (Android or iOS) can download the app and register with his or her electoral ID, name and address, information which Mudamos keeps secure and verifies with Brazil's Electoral Court. The app issues what is known as a cryptographic key pair, a small piece of code used for verification. One half of the key is stored on the user's phone and the other with Mudamos, which makes it possible to authenticate a person's signature. In this way, members of the public can draft and sign petitions in a way that is verifiable and secure.*		
SDG in Focus (when applicable)	*Enter one or more number (1-17) and specific corresponding indicator/s as applicable* *See https://www.un.org/sustainabledevelopment/sustainable-development-goals/* *Goal 16: Promote just, peaceful and inclusive societies*		

Value Transfer:	*If potential solution allows to transfer any value (e.g. assets, tokens, etc.)*	**Number of Users:**	*350.000*
Types of Users:	*Voters regular registered to vote.*		
Stakeholders	*Citizens (engaged citizens in support for law making), Legislative Houses (representatives and public servants).*		
Data:	*In order to make the whole process auditable, Mudamos publishes the signatures list periodically by registering the files in public blockchain networks, where they can be publicly scrutinized. This ensures that signature lists are immutable, and if an interested agent wants to audit the entire signing process, from the first signature collected, they have the capability to do it without relying on Mudamos or any other agent.*		
Identification:	***Auto geranted Private key / Electoral data***		
Predicted Outcomes:	**Signature lists in support of citizens' initiative draft bills.**		

Overview of the Business Problem or Opportunity

Brazil's Constitution provides several direct democratic mechanisms, including the referendum, plebiscite, and citizens' initiatives. The initiative mechanism allows any citizen to propose a draft bill to the lower house of municipal, state or federal legislatures. If the proposal gets the requisite number of signatures from registered voters in support then the campaign organizators present the bill before the House. Once the signatures are verified, the Speaker assigns a House committee to start bill discussion that could lead (or not) to the bill becoming a law. At the federal level, the minimum amount of signatures is 1.5 million, which is problematical to organize using paper-based petitions. Popular initiatives to collect signatures are often paper-based which, apart from being costly, also present problems of transparency and integrity. In fact, no citizen bill has ever been approved at the national level due to the verification barrier and participation costs.

Thus Institute for Technology and Society (ITS Rio) created Mudamos in 2017 to reduce the high costs of creating paper-based petitions by offering a verifiable online mechanism for the creation and signing of citizen petitions and offer a robust means of participation that, in turn, should help to raise citizens' degree of trust in political institutions and contribute to the construction of participatory rules and norms.

Why Distributed Ledger Technology?

The uniqueness of the signatures is guaranteed by the association of unique electoral ID number combined with the signature timestamp and the user's private key. The private key generates a unique hash based on the data reported for signature. Verifiability is guaranteed by publishing the user's public key along with the data given for signature and the signature hash. In order to make the whole process auditable, Mudamos publishes the signatures list periodically by registering the files in public blockchain networks.

Section 2: Current process

Current Solutions

N/A

Existing Flow (as-is)		
Step	**User Actions**	**System Actions**
1.	Create a campaign for signature gathering	N/A. Paper-based
2.	Paper-based form download from legislative house	Access legislative house website and download form template.
3.	Signature	N/A. Paper-based signature
4.	Present signatures	N/A. Paper-based process. 1.5 million paper-based signatures have an average of 2ton weight.

Process scheme (as-is)

Data and information (as-is)		
Data	**Type**	**Description**
1	*Documents*	Electoral Personal Data (Name, Electoral ID, ZIP Code) and signature written down on paper-base forms.
2	*Payment transactions*	N/A

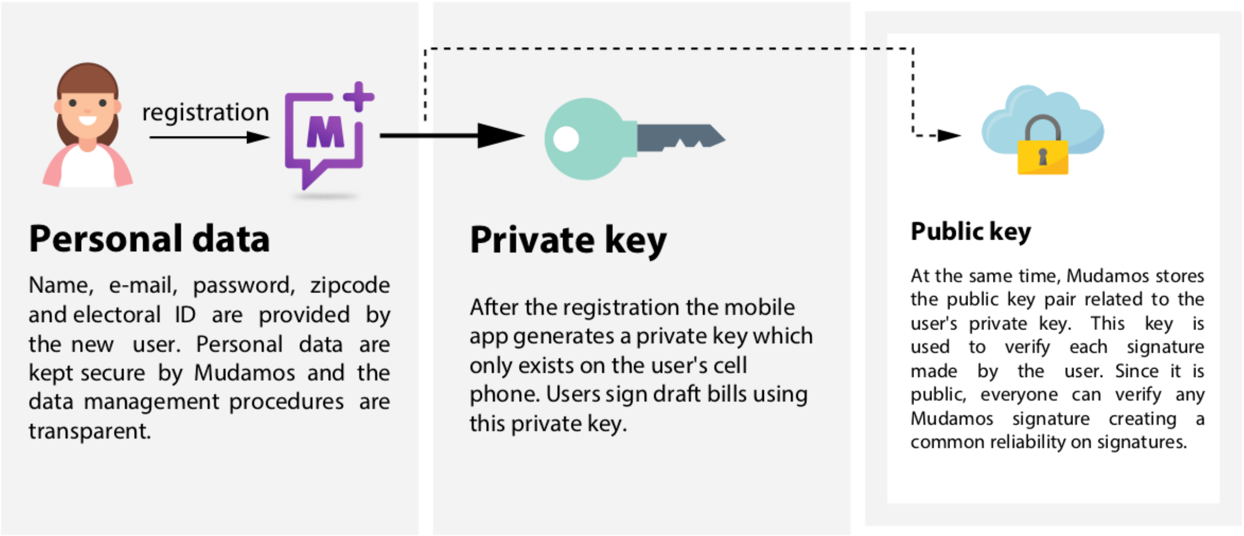
Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	*Legislative houses*	Brazilian legislative houses in any different level (city, state and national) where draft bills and signature are addressed for.
2	*Signature campaign leaders*	People who decide organize campaigns in support for a drat bills and manage all logistics for that.
3	*Signers*	People how sign in support for a draft bill.

Other Notes
Any assumptions, issues

Section 3: Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	Register on Mudamos	Generate key pair
2.	User signature	Electoral data hashing based on private key
3.	Signature verification	Checking electoral data against signature hash and user’s public key
4.	Check public signature lists	PDF signature list hashes checking on public Blockchains
5.	Reach signatures threshold	Present lists into a flash drive to legislative house speaker to start bill discussion

Process scheme (to-be)



Personal data

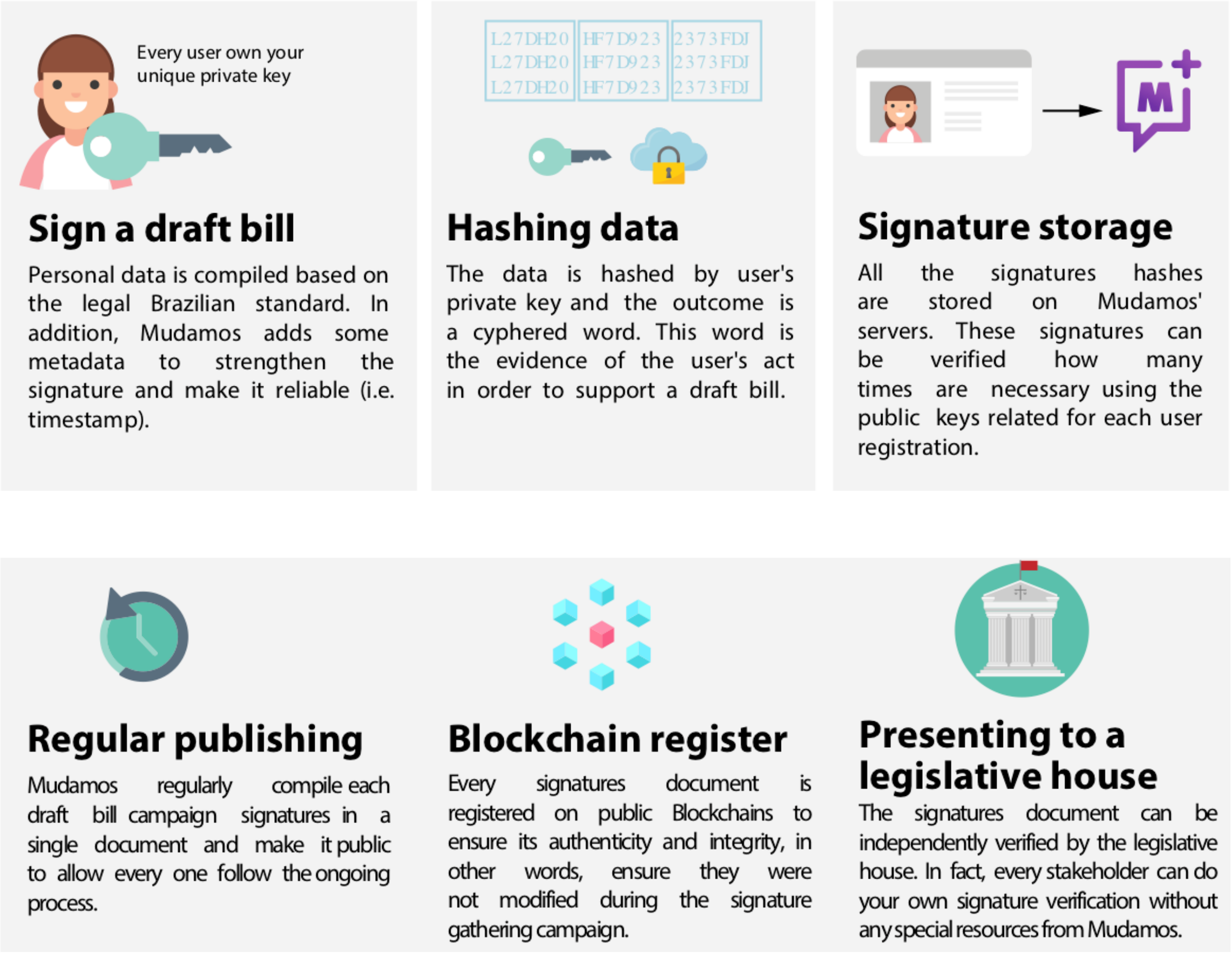
Name, e-mail, password, zipcode and electoral ID are provided by the new user. Personal data are kept secure by Mudamos and the data management procedures are transparent.

Private key

After the registration the mobile app generates a private key which only exists on the user's cell phone. Users sign draft bills using this private key.

Public key

At the same time, Mudamos stores the public key pair related to the user's private key. This key is used to verify each signature made by the user. Since it is public, everyone can verify any Mudamos signature creating a common reliability on signatures.



Sign a draft bill

Personal data is compiled based on the legal Brazilian standard. In addition, Mudamos adds some metadata to strengthen the signature and make it reliable (i.e. timestamp).

Hashing data

The data is hashed by user's private key and the outcome is a cyphered word. This word is the evidence of the user's act in order to support a draft bill.

Signature storage

All the signatures hashes are stored on Mudamos' servers. These signatures can be verified how many times are necessary using the public keys related for each user registration.

Regular publishing

Mudamos regularly compile each draft bill campaign signatures in a single document and make it public to allow every one follow the ongoing process.

Blockchain register

Every signatures document is registered on public Blockchains to ensure its authenticity and integrity, in other words, ensure they were not modified during the signature gathering campaign.

Presenting to a legislative house

The signatures document can be independently verified by the legislative house. In fact, every stakeholder can do your own signature verification without any special resources from Mudamos.

Participants and their roles		
Actor	**Type/Role**	**Description**
1	*System Manager*	ITS Rio. Responsible to support Mudamos and make it online.
2	*Mudamos users*	Brazilian citizens registered to vote who can propose draft bills or sign for existing ones.
3	*Legislative houses*	Brazilian legislative houses in any different level (city, state and national) where draft bills and signature are addressed for.
4	*Draft bill proponents*	People who propose draft bills to be supported through Mudamos platform.

Data and information		
Data	**Type**	**Description**
1	*Documents*	Electoral Personal Data (Name, Electoral ID, ZIP Code) PDF list containing signatures compilation
2	*Payment transactions*	N/A

Security and privacy

1. Verification process can be automatized

2. On going campaigns lists have personal data anonymized

3. Signature information can be changed by man in the middle attacks due to its verifiability by its signature hash and public key.

Main Success Scenario + expected time line

Description of DLT-based solution, which potentially will be created

Conditions (pre- or post-)

1.

Performance needs

What potential performance specs (frequency of use, transactions per second, confirmation time, sync time, etc.) are expected. What scalability, interoperability, reliability, accessibility needs exist.

Legal considerations

Currently, thanks to the Internet and other technologies, it is possible to collect signatures throughout Brazil and verify them automatically. Digital signatures already had their relevance recognized and used in common civic procedures, as instituted by the Presidency Act MPV 2200/2001, and in legal acts, as instituted by Law 11419/06. However, since the cost of obtaining official digital certificates is prohibitive, they did not gain widespread adoption and a mere .005% of Brazilians have them.

Digital signatures based on certificates issued by the Brazilian government have the advantage that they are legally binding, meaning any documents signed using those certificates are recognized by any authority as authentic for any purpose, from the recognition of a debt to real estate transactions. However, when we talk about political rights, we do not need signatures to be that strong because people's support of causes are the expression of their political desire, not legal intent. Signature campaigns need only ensure that signatories have the constitutional right to sign the draft bill and signatures only need to allow for public scrutiny to audit the political support given to the bill.

Taking this into account, Mudamos created a way to allow people to sign draft bills using self-issued certificates using their own smartphones. The technology stack used by Mudamos is the same used by certificate authorities to issue certificates, excluding the fact Mudamos is not a recognized authority to issue legally-binding certificates. That is to say, while Mudamos issued certificates cannot be used to authenticate a contract in court, nonetheless the signatures are technically unbreakable and verifiable and well-suited to the purpose of ascertaining citizen wishes but without the cost of doing through one of a handful of monopoly legal certificate providers. In short, Mudamos created a secure and affordable way for people to express themselves politically through digital means.

Risks

Despite all it has to offer, Mudamos's electronic signature is not a national standard and the major risk to the Mudamos project is the contesting of the validity of its signatures by legislative bodies or in courts. Actually, Mudamos is facing a challenge from the legislative house of the Federal District, where Mudamos signatures were not accepted in support of a citizen's initiative draft bill, which called for reducing the House budget. Since an electronic signature standard is not established by law or even by a House of Representatives rule, the decision whether or not to accept Mudamos signatures is discretionary. To mitigate this scenario, ITS drafted a report about citizen initiatives bills arguing that electronic signatures should be accepted based on the current legislation. In addition, the Mudamos team has been talking to congressmen and other leaders, pushing for legislation to standardize electronic signatures. The Mudamos legal framework is another approach to build dialogue bridges between technicians, activists, and legislative houses to support local and national legislative change.

Another risk faced by Mudamos is the adoption rate of the app (350,000 active users) in relation to the number of signatures required to propose a national level draft bill (1.5 million). Despite the fact that Mudamos had at least 4 viral waves since its launch, new user registrations are not growing at a substantial rate. Continuous engagement on Mudamos requires fostering internal variables, such as better user experience and strategic communication for action, and external variables, such as the participatory will of the people which leads to more interest in collaboration and representation in the political process. Mudamos launched its second major version (2.0) in January 2019, seeking user experience improvements, especially features to make campaigns sharing easier.

Mudamos started using public Blockchain as part of its technical architecture, aiming to create a completely transparent and accountable system for verifying signatures. However, after almost 2 years running, the Mudamos team realizes that the availability of this secure infrastructure where anyone can "look under the hood" does not de facto mean anyone is actually doing so. As with the volunteer lawyers, there is a need to develop an independent, crowdsourced technical governance mechanism to ensure that the system maintains its legitimacy.

Finally, the populist, right-wing president, Jair Bolsonaro elected in 2018, has expressed authoritarian tendencies. It is, thus far unknown, how changes in politics will impact political culture in Brazil in the near and longer-term. One can surmise that the trend in government toward more autocratic behavior could end up depressing political mobilization and participation. Or, to the contrary, Mudamos may become more popular than ever if it escapes legal challenge.

Special Requirements

Business and technical requirements of use case

External References and Miscellaneous

For a complete reference of Case Mudamos see: http://congress.crowd.law/case-mudamos.html

Other Notes

Any assumptions, issues

Appendix 1:
Domains and subdomains for use cases categorization

Vertical:

1. Finance
    a. Financial management & accounting
    b. International & interbank payments
    c. Clearing and settlement
    d. Reduction of Fraud
    e. Financial messaging
    f. Asset lifecycles and history
    g. Trade finance
    h. Regulatory compliance & audit
    i. AML/KYC
    j. Insurance
    k. Peer-to-peer transactions
2. Healthcare
    a. Pharma
    b. Biotechnology
    c. Medicine
3. Industries
    a. Manufacturing
    b. Energy
    c. Chemical
    d. Retail
    e. Real estate
    f. IT and telco
    g. Supply chain management
    h. Transportation
    i. Agriculture
4. Government and public sector
    a. Taxes
    b. Government and non-profit transparency
    c. Legislation, compliance & regulatory oversight
    d. Voting
    e. Taxation and customs
    f. Intellectual property management
    g. Land Registries

Horizontal:

1. Identity management
2. Security management
    a. Public Key Infrastructure
3. Internet of Things

4. Data processing, storage and management
    a. Data Validation (includes provenance)

Real Time Tax Compliance

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-004	**Use Case Type:**	Vertical
Submission Date:	March 28, 2019	**Is Use Case supporting SDGs**	*Yes*
Use Case Title:	Real Time Tax Compliance	**Domain:**	Government and Public Sector: Taxes
Status of Case	Proof of Concept Demo	**Sub-Domain**	*N/A*
Contact information of person submitting/ managing the use-case	Priyanka Desai, VP of Business Development & Operations Anne T Griffin, Lead Product Manager Kirsten Albers-Fiedler, Law Associate & Legal Engineer E-mail addresses:priyanka.desai@consensys.net, anne.griffin@consensys.net, kirsten.albersfiedler@consensys.net Telephone number: Social media: https://twitter.com/OpenLawOfficial Web site: **https://openlaw.io/**		
Proposing Organization	OpenLaw (ConsenSys) - United States of America		
Short Description	*The premier open source protocol to rapidly build commercial relationships on blockchain technology.*		
Long description	The premier open source protocol to rapidly build commercial relationships on blockchain technology. OpenLaw makes it easy to automate agreements, collect secure e-signatures storing them on the blockchain, turn legal agreements into simple forms, tokenize assets, and execute, trigger, and halt smart contracts. Additionally, OpenLaw has free open source legal agreement library, that gives people around the world easier access to justice and the law for resources that can cost thousands of dollars elsewhere. This technology supports individuals, corporations, and governments in building powerful but simple solutions to complex problems. OpenLaw supports, but is not limited to, use cases such as automatic tax collection and alternative dispute resolution that help communities by making sure public services can be paid for and access to justice.		
SDG in Focus (when applicable)	16 Peace, Justice, and Strong Institutions		
Value Transfer:	Automatic transfer of monetary instruments to the government(s) to which they are owed	**Number of Users:**	Number of employees + Number of companies + Government Tax Agency

Types of Users:	Individual employees, corporations, government tax collection agencies
Stakeholders	Government tax collection agencies, employers
Data:	Data saved to distributed ledger: Employee First Name, Employee Last Name, Employee Ethereum Address, Salary in Wei per Minute, Amount of Income Tax Withheld in Wei per Minute, Medicare Tax Threshold Amount in Wei, Medicare Tax below Threshold Amount in Wei per Minute, Medicare Tax above Threshold Amount in Wei per Minute, Social Security Tax Base Limit in Wei, Social Security Tax in Wei per Minute, Additional Withholding Amount in Wei per Minute, FUTA Tax Cap Amount in Wei, FUTA Tax in Wei per Minute Our system would interact with any HR systems of the employer, the employee's wallet, the government's wallet, and any government systems that track the payment of taxes.
Identification:	Individual paying taxes is identified in the agreement, however, their signature is hashed to keep their information private from those who are not intended to see the agreement.
Predicted Outcomes:	Will decrease the amount of infrastructure needed to support the payment of taxes, reduce costs of maintaining systems to pay taxes, and reduce tax evasion since these calculations are happening directly in a smart contract.

Overview of the Business Problem or Opportunity
Across the world, there are issues with tax evasion or those who would pay taxes but the lack of infrastructure creates barriers to payment. With OpenLaw's blockchain-based protocol, we're creating a more efficient future, where an employer can pay an employee in ether every minute, eliminating the costs of payroll processors or the need for other centralized intermediaries in the process, while at the same time decreasing the tax gap and the needless waste of resources associated with tax compliance.
Why Distributed Ledger Technology?
Using smart contracts on the blockchain allows the process to be more direct and more efficient. It also decreases the number of intermediaries, and the tax gap.

Section 2: Current process

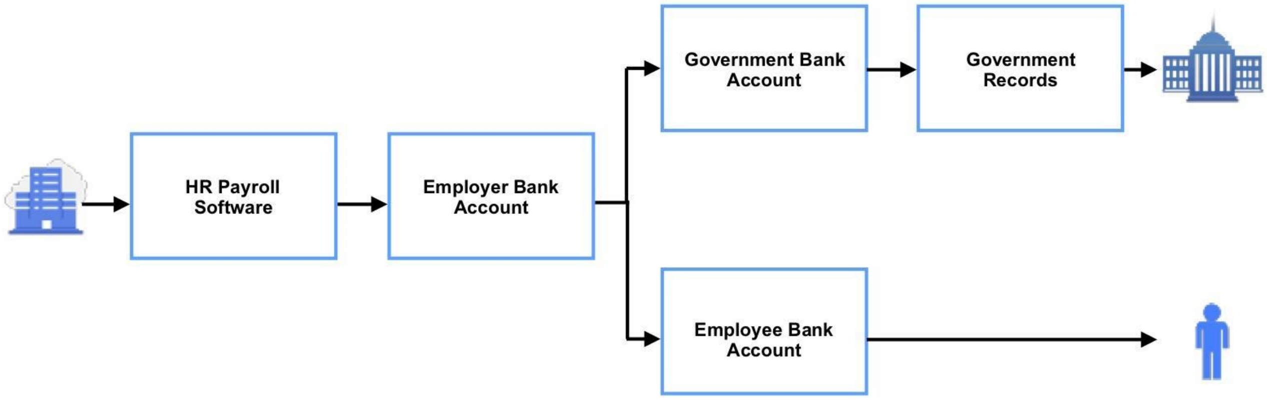
Current Solutions
Existing solutions usually involve several systems within HR software within different companies and several systems within a tax collection agency within the government.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	Employer creates agreements and forms for employee to provide information about self and bank account	Generation of employment agreement.

2.	Employee and employer sign the agreement	Agreement saved to database via agreement software.
3.	Employer enters the information into HR payroll system and sends applicable paperwork to the government	HR payroll system saves employee information.
4.	Company triggers payment process automatically every two weeks	Payroll system looks up employee information.
5.	Automated	Payroll system determines the amount owed to the employee and amount owed in taxes.
6.	Automated	Employer bank account triggers payment to employee bank account.
7.	Automated	Employee bank processes payment.
8.	Automated	Employer bank account triggers payment to government with information.
9.	Automated	Employer bank account processes payment.

Process scheme (as-is)



Data and information (as-is)		
Data	**Type**	**Description**
1.	Employee information	Name, bank account information, income.
2.	Taxes	Types of taxes owed, quantity of taxes owed.

3.	Record of payment to employee, and government tax agency	Records that show the employee was paid and the government tax agency was paid.
4.	Government Tax Agency information	Bank account information for payment.

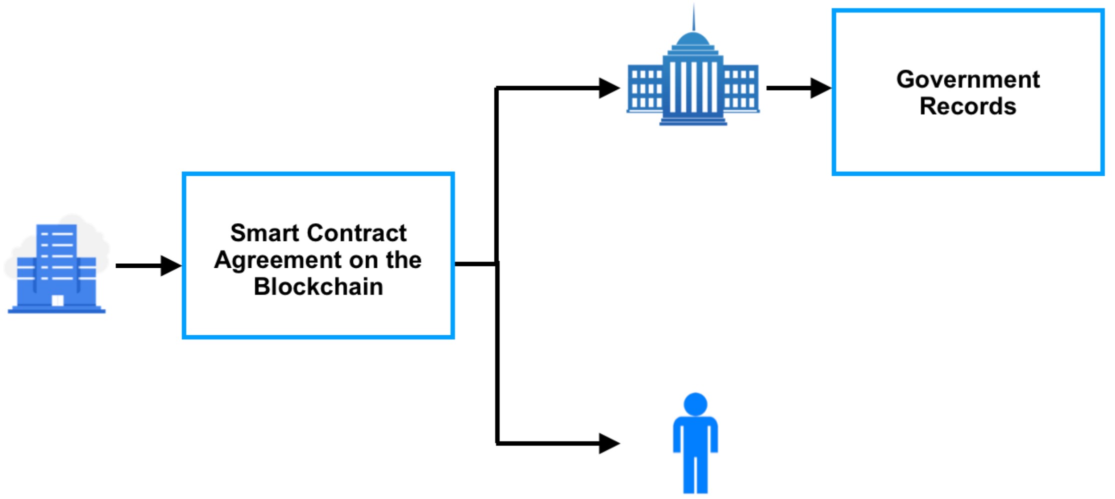
Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1.	Employee	Individual employed who needs to have taxes paid to the government.
2.	Employer	Employer who pays the employee and responsible for withholding taxes from the employee’s paycheck
3.	Government Tax Collection Agency	Government entity responsible for receiving tax payments and keeping tax records for employees and employers.
4.	Bank	Responsible for sending and receiving payments on behalf of the employee, employer, and government.

Other Notes
Any assumptions, issues

Section 3: Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	Employer generates employment agreement	Employment agreement is generated as a smart contract
2.	Employee and employer sign agreement	System saves signature and start date to the blockchain
3.	Automated	Payment automatically paid to the employee’s wallet for the agreed upon amount and start date via the smart contract
4.	Automated	Payment automatically paid to the government tax collection agency’s wallet based on the taxes owed

Process scheme (to-be)



Participants and their roles		
Actor	**Type/Role**	**Description**
1.	Employee	Individual employed who needs to have taxes paid to the government.
2.	Employer	Employer who pays the employee and responsible for withholding taxes from the employee’s paycheck
3.	Government Tax Collection Agency	Government entity responsible for receiving tax payments and keeping tax records for employees and employers.

Data and information

Data	Type	Description
1.	Employee information	Name, ethereum address, income.
2.	Taxes	Types of taxes owed, quantity of taxes owed.
3.	Record of payment to employee, and government tax agency	Records that show the employee was paid and the government tax agency was paid.
4.	Government Tax Agency information	Government Ethereum address.

Security and privacy
All information on the Ethereum blockchain is stored as a cryptographic hash on a distributed public ledger.

Main Success Scenario + expected timeline
Ideally, many businesses will begin using this technology with their employees and respective governments. Those businesses and governments will see a cost reduction in the systems needed to maintain the old way of handling payments and taxes, and employees and tax collection agencies can be paid in real time as value is being contributed to the economy, instead of on a schedule that only aligns with intermediary institutions. It should take most businesses less than a year to implement these solutions. For small businesses with less legacy technology, it could take less than six months to implement.

Conditions (pre- or post-)
1. Access to the Internet 2. Access to the Ethereum online wallet.

Performance needs
N/A

Legal considerations
In the United States, there aren't laws explicitly banning cryptocurrency or their use for payment, however not all local governments have explicitly stated they accept them. Outside of the United States, some countries have banned cryptocurrencies such as Bolivia, or allow cryptocurrency, but do not treat them as a currency. Influence of policy could help governments around the world accept cryptocurrencies so they can use blockchain technology in combination with payments in cryptocurrency or conversion from cryptocurrency to fiat currency. In addition to policy changes, stablecoins can help mitigate concerns around cryptocurrency. They can be tied to fiat currencies, which lowers their volatility, and can tie their value to the fiat currencies of the respective countries that are interested in implementing this solution. https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory

Risks

Current laws do not include withholding amounts for cryptocurrencies, and the conversion rate of ether into USD is subject to volatility, we have converted the salary that an employee receives in ether into USD based off the conversation rate as of May 21, 2018 in order to make the appropriate tax calculations. We then converted the tax and adjusted salary amounts back to ether using the same conversion rate. Depending upon how laws shape themselves around cryptocurrencies in the future, the conversion of ether to USD may require the use of an oracle or, possibly, stable coins.

Also risks regarding security of smart contracts so they aren't hacked and money is sent to the incorrect address.

Special Requirements

Access to the Ethereum

External References and Miscellaneous

State of Ohio Allowing Payment of Taxes in Crypto - http://ohiocrypto.com/

Arizona Senate Bill Allowing Crypto Payment - https://legiscan.com/AZ/bill/SB1091/2018

Illinois House Bill Allowing Crypto Payment - https://legiscan.com/IL/bill/HB5335/2017

Georgia State Senate Bill Allowing Crypto Payment - https://legiscan.com/GA/bill/SB464/2017

Other Notes

N/A

Regtech Improving Governance Authenticating Identities, Authorization Signatures and Digital Content

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-005	**Use Case Type:**	Government and Public Sector
Use Case Title:	OriginalMy Blockchain	**Is Use Case supporting SDGs**	*Yes*
		Domain:	*List 1 Appendix 1*
Status of Case	Running/Production	**Sub-Domain**	*If necessary*
Contact information of person submitting/ managing the use-case	Full Name: Edilson Osorio Junior Job Title: CEO E-mail address: osoriojr@originalmy.com Telephone number: +372 5709-5771 Social media: https://www.linkedin.com/in/osoriojr/ Web site: **https://originalmy.com**		
Proposing Organization	OriginalMy Blockchain OÜ Registry Code: 14450907		
Short Description	A LegalTech engine platform that builds Trust in e-Governance seamlessly authenticating: identities, authorisation signatures, and digital content		
Long description	Founded in 2015, OriginalMy envisions a world in which individuals and entities have a balanced alignment of interests and are empowered to take necessary actions that build Trust in the e-Governance for the benefit of the entire organisation. The challenge to achieve that vision is building Trust and increase the overall governance process while providing compliance, risk management and cybersecurity tools that cannot be flawed, corruptible, temperable and non-verifiable - because of centralisation. The solution is presenting a trusted and immutable blockchain framework with: - The next generation of Digital Identity & storage of assets; - Seamlessly authentication with proof-of-authorship; - Single Sign-On, with control of delivering of personal data; - Authentic signed documents, contracts and transactions ; - Proof-of-authenticity for digital content; - Blockchain-enabled e-voting systems; This approach is trustful because it improves the overall e-Governance reducing costs and saving time, is flexible to address an array of risk and compliance needs, performs traceability of all digital acts performed and has the security provided by blockchain cryptography protocols.		

SDG in Focus (when applicable)	*Enter one or more number (1-17) and specific corresponding indicator/s as applicable* *See https://www.un.org/sustainabledevelopment/sustainable-development-goals/* Use your right to elect the leaders in your country and local community **Goal 16: Promote just, peaceful and inclusive societies** 16.3 Promote the rule of law at the national and international levels and ensure equal access to justice for all 16.4 By 2030, significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime 16.5 Substantially reduce corruption and bribery in all their forms 16.6 Develop effective, accountable and transparent institutions at all levels 16.7 Ensure responsive, inclusive, participatory and representative decision-making at all levels 16.8 Broaden and strengthen the participation of developing countries in the institutions of global governance 16.9 By 2030, provide legal identity for all, including birth registration 16.10 Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements 16.A Strengthen relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime 16.B Promote and enforce non-discriminatory laws and policies for sustainable development Call out sexist language and behaviour **Goal 5: Achieve gender equality and empower all women and girls** 5.1 End all forms of discrimination against all women and girls everywhere 5.2 Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation 5.B Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women 5.C Adopt and strengthen sound policies and enforceable legislation for the promotion of gender equality and the empowerment of all women and girls at all levels Raise your voice against discrimination **Goal 10: Reduce inequality within and among countries** 10.2 By 2030, empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin,

	religion or economic or other status 10.3 Ensure equal opportunity and reduce inequalities of outcome, including by eliminating discriminatory laws, policies and practices and promoting appropriate legislation, policies and action in this regard 10.6 Ensure enhanced representation and voice for developing countries in decision-making in global international economic and financial institutions in order to deliver more effective, credible, accountable and legitimate institutions 10.7 Facilitate orderly, safe, regular and responsible migration and mobility of people, including through the implementation of planned and well-managed migration policies Partnership for the goals **Goal 17: Revitalize the global partnership for sustainable development** 17.7 Promote the development, transfer, dissemination and diffusion of environmentally sound technologies to developing countries on favourable terms, including on concessional and preferential terms, as mutually agreed 17.8 Fully operationalize the technology bank and science, technology and innovation capacity-building mechanism for least developed countries by 2017 and enhance the use of enabling technology, in particular information and communications technology		
Value Transfer:	It allows the tokenization of all of your own resources, assets and attributes carrying it on your identity, avoiding the needing of a third party to certify/comprove what belongs the to you. It reduces costs, bureaucracy, time and empower people.	**Number of Users:**	*30.000*
Types of Users:	natural person and entities		
Stakeholders	natural person, entities and government		
Data:	*What data are expected to be stored in distributed ledger in terms of types, record structure, privacy, etc.* *How DLT solution would interact with external data and other systems.* Stores the link between the document id and the blockchain id, mantaining history of changes. Stores the hashes of digital documents, the signatures made on documents and authorisations and, in the future, the reputational system. It don't store any personal data on the ledger. Thus, OriginalMy will use tokens to reward users who made tasks, like working on the decentralised network of validation being constructed.		
Identification:	Identity validation automatically or using own bureau. After the validation, the personal data is stored just with the user. There's no possibility of anonymous use.		

Predicted Outcomes:	

Overview of the Business Problem or Opportunity

Explanation of the business problem or opportunity.

The problem is the lack of trust on digital content and on who is performing the digital act or transaction, in situations where the authenticity, authorship or ownership is critical.
It opens a window for corruption, bureaucracy and expending of money and time.

Fines and compliancy divergences costs:

- **$300 billion post 2008 crisis regulatory fines**
  FT Research
- **492% volume of regulatory change between 2008 and 2015**
  Thomsom Reuters
- **45x increase of regulatory fines in 20 large US and EU banks**
  McKinsey
- **10-15% of total workforce dedicated to governance, risk and compliance**
  McKinsey
- **Proxy voting remains "noisy, imprecise and disturbingly opaque"**
  Barrons - about $60m P&G proxy fight costs

The opportunity:

- **$780 billion** per year regulatory divergence costs Thomson Reuters: Cost of Compliance 2018 Report
- **ROI of 600%** in regulatory software investment
  LPT Research: Strategic Analysis of RegTech - A $100b Opportunity
- **$118.7 billion** per year revenue stream by 2020
  LPT Research: Strategic Analysis of RegTech - A $100b Opportunity

On the Identity field, a McKinsey report identified that until 2030, countries will spend up to 13% of the GDP on Digital Identity and related services, to avoid identity and payroll fraud and improving the onboarding systems.

Why Distributed Ledger Technology?

How distributed ledger technology would improve the current solutions (if they exist) or enable new solutions which were previously unavailable.
Please also specify which DLT features are required (immutability, security, verifiability, resilience, transparency, etc.)

The full solution is only possible because of blockchain technologies.

- Allows the full decentralisation of the identity and being the future generation of digital identity (where the identity will store itself all of your resources, assets and attributes).
- Allows the transaction of personal data being tracked and rewarded.
- Allows the proof-of-authenticity of digital content and transactions
- Allows proof-of-authorship for authorisation signatures on documents, and contracts
- Single sign-on systems with delivering (transacting) of personal data with proof-of-agreement
- Improves trust on e-voting, where the main problem is the lack of trust just after casting the vote to the blinded ballot box and in the centralised tallying phase (see Hääl - the

worldwide first protocol for Secret E-Voting on Public Blockchains, with running PoC: https://github.com/eddieoz/haal)

- Allows decentralised reputation system and dispute resolution
- Security provided by many layers of strong cryptography
- Immutability and integrity of all data stored, as resilience and redundancy for contingence.
- Transparency and auditability of all data and transactions
- High availability of all network

Section 2: Current process

Current Solutions

If there are existing systems which automate the above business problem/opportunity.

- OriginalMy: providing end-to-end digital governance

And other systems who addresses part of the solutions:
UPort: digital identity
Civic: digital Identity
Signatura: signing contracts and documents
BlockNotary: notarisation of documents

Existing Flow (as-is): Signing documents and contracts

Step	User Actions	System Actions
1.	Local authentication	User goes to a notary
2.	Sign a contract	User register the contract on a notary

Existing Flow (as-is): Signing public petitions

Step	User Actions	System Actions
1.	Signature collecting	User signs a paper
2.	Validation	Impossible to validate
3.	Acceptability	Representative endorses the petition

Existing Flow (as-is): Proof-of-authenticity of web content + notarization (avoiding fake news dissemination, harassment and other on social media)

Step	User Actions	System Actions

1.	Collecting the legal proof	User goes to a Notary Notary transcribe the page on a report The report can be attached to a case and sent to the justice

Existing Flow (as-is): Platform: Notarization of documents		
Step	**User Actions**	**System Actions**
1.	Authenticating documents	User goes to a Notary Notary makes a copy of the document Notary authenticates the copy of the document

Existing Flow (as-is): E-voting		
Step	**User Actions**	**System Actions**
1.	Voter casts the ballot	Send to a centralised platform Needs to Trust on the platform; Too much power on a centralised entity No transparency and verification in real-time Black-boxes of voting

Data and information (as-is)		
Data	**Type**	**Description**
1	*Documents*	In paper
2	*Web content*	Must go to a Notary
3	*Certificate of Signatures*	Must go to a Notary to verify the signatures
4	*Certificate of Authenticity*	Provided by a notary, in paper
5	*Notary Authentication*	Digitally stamped document issued by a notary
6	*Notary declaration*	Report issued by the notary, with the description of the service provided
8	*Collecting Signatures on Public petitions*	On paper

9	*Voting ballot*	On-paper on electronic by centralised trusted entity

Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	*Lawyers*	Collect evidence to attach to the process
2	*Bank*	Pre-authenticate documents to send to the notary
3	*Government*	Preserves the authenticity of your papers and documents
5	*Users*	Has the needs of authenticating documents, verifying theirselves or their signatures
6	*Notary*	Provides the service for authenticating documents and signatures

Other Notes
Any assumptions, issues

Section 3: Expected process

Existing Flow (to-be): Mobile app: Signing documents and contracts		
Step	**User Actions**	**System Actions**
1.	Local authentication	User uses local biometrics to validate him/herself
2.	Sign a contract	User proves the ownership of the document to be signed (using pin-code) System verifies on-chain if the user is allowed to sign and if the document is authentic System stores the digital signature and the blockchain id on the smart-contract, together to the other signatures of that document

Existing Flow (to-be): Mobile app: Authentication system with delivering of personal data		
Step	**User Actions**	**System Actions**
1.	Local Authentication	User uses local biometrics to validate him/herself
2.	Scans a QR-code	Opens a popup showing all the data that will be collected by the platform
3.	User agree on deliverying of the data	Authenticates user using cryptography challenges Sign the data to be transferred Transfer the data to the desired platform Registers the transaction The desired platform checks the authenticity of the data, as the reputation.

Existing Flow (to-be): Mobile app: Mudamos+ (created by ITS-Rio) internally using our engine for identity, signatures and authentication, for signing public petitions (+600k downloads, 2 laws approved)		
Step	**User Actions**	**System Actions**
1.	User selects the public petition	verifies the authenticity of public petition on-chain
2.	User decides signing	System uses the stored and previously validated Blockchain ID for signing the petition App does proof-of-work, generating a block to be accepted by the network (avoiding hacking, spam and brute-force on the network) Sends the block to network.

		If the block is valid, the network stores the block on a sidechain In the selected times, the system scan the sidechain, revalidates all user signatures, and generates and publish a new version of the PDF report with all signatures collected for all open public petitions System authenticates each generated new version of the report on blockchain
3.	User submits the signatures report to verify the authenticity	System verifies the authenticity of the report on-chain System validates each signature in the report: user validity and integrity of the user signature

Existing Flow (to-be): Chrome Plugin: Proof-of-authenticity of web content + notarization (avoiding fake news dissemination, harassment and other on social media)		
Step	**User Actions**	**System Actions**
1.	Click on Chrome Plugin	Scans the page Generates a report which contains the permalink, timestamp and the copy of the page Authenticates the report in blockchain Send the report to the notary Notary verifies the authenticity in on-chain Notary extracts the permalink, access the page, copies the page, authenticates the copy of the page and delivers back to the user

Existing Flow (to-be): Platform: Notarization of documents		
Step	**User Actions**	**System Actions**
1.	User submits a document	Extracts the hash Verify on-chain the authenticity of the document If document is already authenticated, returns the full information If the document is not authenticated yet, goes to the checkout
2.	User goes to the payment page	System detects if the user is staking the token ABC - Anti Bureaucracy Coin If yes, system recalculates the discount

3.	User makes the payment	System authenticates the hash of the document in on or more blockchains

Existing Flow (to-be): Platform: Registration of documents to be signed		
Step	**User Actions**	**System Actions**
1.	User submits a document	Extracts the hash Verify on-chain the authenticity of the document If document is already authenticated, returns the full information If the document is not authenticated yet, goes to the checkout
2.	User goes to the payment page	System detects if the user is staking the token ABC - Anti Bureaucracy Coin If yes, system recalculates the discount
3.	User makes the payment	System authenticates the hash of the document in on or more blockchains System opens a session on a smart-contract to start collecting the signatures System notifies all signatories Signatories make the signature System stores the signature together on the smart-contract After collecting all signatures, system generates a report and send to each signer.

Existing Flow (to-be): Platform and app: Public e-voting		
Step	**User Actions**	**System Actions**
1.	Voter submits the filled voting ballot for signing	Extracts the hash Register the ballot for signature by the selected BlockchainID on the smart-contract and wait for the signature
2.	Voter sign the ballot with BlockchainID	System stores the user signature on the smart-contract After confirmation, system provides a certificate of signature to the user
3.	User submit the ballot and the certificate to the voting	off-chain process

	administration for tallying purposes	

Expected Flow (to-be): Secret voting on public blockchain **PoC and paper: https://github.com/eddieoz/haal**		
Step	**User Actions**	**System Actions**
1.	User authenticates to voting session	Validate the user identity Open the voting session Unlink user identity Generates the stealth addresses for voting and register it on chain to be discovered
2.	User cast the vote through stealth wallet	System creates the zero-knowledge proof-of-vote Encrypts the ballot with homomorphic encryption Casts the encrypted ballot and store in blockchain Validates the zkProof-of-Vote on chain User verify own vote Closes the voting session
3	Voting administrator closes the election session	Smart-contract automatically the result Smart-contract publishes the result
4	Auditor retrieve all results to check	Decrypts all votes Calculates the final result Generates the proof-of-result Publish the proof-of-result on chain

Expected Flow (to-be): Decentralized network of validation		
Step	**User Actions**	**System Actions**
1.	User A collect the web-content proof and send to the platform	Opens a collecting proofs session System authenticates the proof on blockchain System asks for how many people must access and collect proofs System calculates how much ABCs must be deposited to reward the network for collecting proofs
2.	User A deposits the amount	System randomly notifies the network to collect proofs
3.	Users from network receive the notification and agrees on collecting proof from their device	System generates automatically the proof System asks for user to sign the proof with the Blockchain ID to prove it is a real person
4.	User from network agrees on signing	System sign the proof using the Blockchain ID System authenticates the generated proof on blockchain Stores the proof to the proofs repository
5.	User A collects the proofs collection	After aproval, rewards user from network Delivers all signed proofs to the User A Closes the collecting proofs session

Process scheme (to-be)

Participants and their roles		
Actor	**Type/Role**	**Description**
1	*Government/Institution*	Voting system administrator: Setup the voting infrastructure, open and closes the voting session
2	*Natural person*	Vote, request webcontent proofs participate on the decentralized network for collecting webcontent proofs.
3	*Lawyer*	Request webcontent proofs from decentralized network
4	*OriginalMy*	It is the first validator of user identity
5	*Auditor*	Audit the voting process in real time, compute the result and the proof-of-result to check if it matches with the automatically calculated by the smart-contract, count users, count open voting sessions, verify if user validation is correct
6	*Notary*	Executes a digital process of authenticating documents and signatures

Data and information		
Data	**Type**	**Description**
1	*Web Content*	Content collected on Web Browser
2	*Proof-of-Authenticity of Web Content*	PDF report that contains the permalink, timestamp and the copy of the web content.
3	*Ballot*	Ballot that contains all the races and candidates
4	*Encrypted Vote*	The ballot with each vote encrypted
5	*Proof-of-Vote*	Zero Knowledge proof-of-vote issued optionally after voting, used as vote receipt
6	*Proof-of-Result*	Zero-knowledge proof-of-result, proves the voting administrator decrypted all votes and calculated the result for auditing purposes
7	*Digital Document*	Any kind of digital media, to be authenticated
8	*Digital Signature*	Signature made using the private-keys owned by the user

9	*Digital Identity*	Digital certificate where the private-keys are located. It must be stored just with the user

Security and privacy
1. User validates the identity for using the BlockchainID 2. User casts the vote, unlinked to identity 3. No participant can see the content of the vote of another user 4. No possibility of double-voting 5. User can keep the (zk)proof-of-vote, to prove the vote without exposing the vote 6. Vote buying and vote coersion avoided if the voting session is open for many days and user have the possibility of changing vote anytime (Estonia example) 7. OriginalMy dont store user personal data, content or documents, for privacy purposes 8. User delivers own personal data, signing the data delivered. Destination platform has proof-of-agreement for all received data. 9. Decentralized identity and decentralized storage of personal data. No single point of failure

Main Success Scenario + expected time line

Actual Key Achievements

The main key achievements are:

- having blockchain proofs accepted in the Court of Appeals (Superior Court),

- new laws created that started on our engines (through Mudamos+),

- marriages and child born registrations,

- used by presidential candidates to fight against fake-news dissemination,

- shareholders e-voting on Brazilian Fintechs Association,

- mentioned in books and academic papers,

- Brazilians no longer need to go to the notary to authenticate documents, because of the first notary integration,

- featured on a US documentary of Reason.tv: "3 Ways Bitcoin is Promoting Freedom in Latin America"

- featured on a documentary of Globo, the second largest commercial TV: "Estonia has a pioneering project to end bureaucracy and facilitate citizens' lives"

Awarded:

- Google.org Social Impact Challenge in 2016 (through Mudamos+ by ITS-Rio - app for signing public petitions powered by our engine for identity, signatures and authentication),

- Financial Personality of the Year in 2017

- Most Innovative Startup in 2018

Future Success Scenario

An anonymous electronic voting system on public blockchains with the transparency and auditability provided by a public blockchain like Ethereum to bring another level of trust and security because everything can be auditable during the voting process. The smart-contract starts the tally phase and verify it using distributed computing if needed. The voting privacy is granted by stealth wallets, homomorphic encryption, at the same time that zero-knowledge proofs grant the and the proof-of-vote and the proof-of-result.

We expected until the end of 2019 having a open capital company doing the shareholders proxy-voting through our platform

Conditions (pre- or post-)

For using Blockchain ID:

1. Download OriginalMy app

2. Validation of the identity of the user through automated or manual process

For authenticating documents

1. Create an account on the website

For authenticating web-proofs

1. Installing the Chrome Browser extension

Performance needs

What potential performance specs (frequency of use, transactions per second, confirmation time, sync time, etc.) are expected. What scalability, interoperability, reliability, accessibility needs exist.

- Improving the confirmation time for contract and signatures
- Improving the fee & gas of blockchain/smart-contracts
- Scale the identity validation
- Implement another public blockchains (Waves, Litecoin and others)
- Interoperability with x509 certificates
- reducing fee for using ABC token

Legal considerations

For each issue, please describe the name of the legal act containing the identified barrier, what is the negative impact and a proposal to overcome this negative impact.

1. Compliance with MP 2200-2/2001
2. Compliance with Civil Law Arts. 104-107, 219 and 220
3. Legal opinion for digital authentication with notaries

   No law barriers with negative impact, but laws expressly approving the format of authentication could be helpful, like the case of Wyioming https://www.forbes.com/sites/caitlinlong/2019/03/04/what-do-wyomings-new-blockchain-laws-mean/#2943280e5fde

Risks

Legal, business and technical risks related to use case

Risks of lobby by notaries, banks and congressmen

Lack of regulations in Brazil creating an insecure environment for crypto-startups

Tech risks:

- 0-day in Bitcoin, Ethereum or EDSA curves,
- 51% attack,
- expensive fee costs because of cryptocurrency prices

Special Requirements

No special requirements

External References and Miscellaneous

List of references for standards or well-defined mechanisms if any of requirements calls for the implementation of a standard or protocol or other well-defined mechanism. If the use case needs non-standard consensus mechanisms or cryptographic tools, such information should be included here. Also such section may be used to provide more information regarding the use case including links to any kind of related materials, terms and descriptions or any other related information.

Albrecht, Martin, et al. Homomorphic Encryption Standard. 21 Nov. 2018, http://homomorphicencryption.org/wp-content/uploads/2018/11/HomomorphicEncryptionStandardv1.1.pdf.

A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper. Accessed 13 Jan. 2019.

Aztec Protocol Specification. https://github.com/AztecProtocol/AZTEC/blob/master/AZTEC.pdf. Accessed 13 Jan. 2019.

Baudron, Olivier, et al. "Practical Multi-Candidate Election System." Proceedings of the Twentieth Annual ACM Symposium on Principles of Distributed Computing - PODC '01, 2001, doi: 10.1145/383962.384044.

Bitcoin-Development | Stealth Addresses. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-January/004020.html. Accessed 14 Jan. 2019.

Blum, Manuel, et al. "Noninteractive Zero-Knowledge." SIAM Journal on Computing, vol. 20, no. 6, 1991, pp. 1084–118.

Camenisch, Jan, et al. "Efficient Protocols for Set Membership and Range Proofs." Lecture Notes in Computer Science, 2008, pp. 234–52.

Dahlin, Taylor Fox, and daylighting society. "Paillier Zero-Knowledge Proof."

Https://paillier.daylightingsociety.org, 17 Dec. 2016,

https://paillier.daylightingsociety.org/Paillier_Zero_Knowledge_Proof.pdf. Damgård, Ivan. On Σ-Protocols.

http://www-cs.ccny.cuny.edu/~fazio/F15-csc85030/readings/Dam10.pdf. Accessed 13

Jan. 2019.Decentralised Applications.

https://github.com/ethereum/wiki/wiki/Decentralized-apps-(dapps).Developer Guide - Bitcoin | Blockchain.

https://bitcoin.org/en/developer-guide#block-chain. Accessed 14 Jan. 2019.

Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret

MacAlpine, J. Alex Halderman. Security Analysis of the Estonian Internet Voting

System. https://jhalderm.com/pub/papers/ivoting-ccs14.pdf. Accessed 13 Jan. 2019. Goldwasser, S., et al. "The Knowledge Complexity of Interactive Proof-Systems." Proceedings

of the Seventeenth Annual ACM Symposium on Theory of Computing - STOC '85, 1985,

doi:10.1145/22145.22178.

Goldwasser, Shafi, et al. The Knowledge Complexity of Interactive Proof Systems. Feb. 1989,

http://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/

The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf.

Heiberg, Sven, et al. "Improving the Verifiability of the Estonian Internet Voting Scheme."

Lecture Notes in Computer Science, 2017, pp. 92–107.Introduction – Homomorphic Encryption Standardization.

http://homomorphicencryption.org/introduction/. Accessed 14 Jan. 2019.

Lai, Wei-Jr, et al. "DATE: A Decentralized, Anonymous, and Transparent E-Voting System."

2018 1st IEEE International Conference on Hot Information-Centric Networking

(HotICN), 2018, doi:10.1109/hoticn.2018.8605994.

Racanelli, Vito J. "Proxy Voting Is Broken and Needs to Change." Barrons Online, Barrons, 7

July 2018, https://www.barrons.com/articles/proxy-voting-is-broken-and-needs-to-change-1530924318.

Rivest, Ronald L. The ThreeBallot Voting System. 1 Oct. 2006, https://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf.

Tsang, Patrick P., and Victor K. Wei. "Short Linkable Ring Signatures for E-Voting, E-Cash and Attestation." Lecture Notes in Computer Science, 2005, pp. 48–60.

What Are Zk-SNARKs? https://z.cash/technology/zksnarks/. Accessed 14 Jan. 2019. Wu, Wei-Jr Lai Ja-Ling. An Efficient and Effective Decentralized Anonymous Voting

System. 18 Apr. 2018, http://arxiv.org/abs/1804.06674.

Yu, Bin, et al. "Platform-Independent Secure Blockchain-Based Voting System." Lecture

Notes in Computer Science, 2018, pp. 369–86.Zcash Protocol Specification.

https://github.com/zcash/zips/blob/master/protocol/protocol.pdf. Accessed 13 Jan. 2019.

Other Notes
Any assumptions, issues

Diploma Verification

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-006	**Use Case Type**	*Vertical*
Use Case Title:	Diploma Verification	**Is uUse Case supporting SDGs**	*Yes*
		Domain:	*Government and public sector*
Status of Case	*Pilot*	**Sub-Domain**	*Education*
Contact information of person submitting/ managing the use case	*Full Name* ***Pierre-Yves Burgi*** *Job Title* Directeur SI adjoint *E-mail address:* *Pierre-Yves.Burgi@unige.ch* *Telephone number:* **+41 22 379 75 09** *Website:* ***https://www.unige.ch/stic/acteurs/organigramme/direction/burgi/***		
Proposing Organization	*University of Geneva, Switzerland*		
Short Description	*Pilot for verification of diplomas by Ethereum smart contract and legally recognized electronic seal. Possibility of revocation of diplomas.*		
Long description	The falsification of university certificates is a major problem. Since diplomas are often only presented as scans, forging them has become very easy. As a result, the University of Geneva is being confronted with an increasing number of verification requests. A pilot application has been developed that uses a legally regulated seal and a timestamp on a public blockchain (Ethereum) to prove the authenticity of a diploma. The document is verified by using the original PDF/A-file or a short summary of the diploma. The use of a public blockchain ensures that the diploma can be proven even in the case of the university not being able to confirm its validity anymore		
SDG in Focus (when applicable)	*SDGs in Focus are SDG 4 – education and SDG 8 – decent work.*		
Value Transfer	*No transfer of value*	**Number of Users:**	*40 (currently in the pilot), several thousand planned in the future*
Types of users	Students and everybody to whom they present their diplomas		
Stakeholders	*Students, universities, employers*		
Data:	For diplomas, only hashes are stored with no metadata added. This will only allow the verification of the originality of a document that is presented to the users. Only in the case of revocation is the information about the revocation added. However, even then, this information can only be linked to a student when somebody is in the possession of a copy of the diploma and therefore has a legitimate reason to verify its validity.		

	External recruitment systems may access the smart contract directly to verify that the documents they receive are original and have not been revoked.
Identification	Education certificates are bound to an identity and cannot be transferred. There are no anonymous certificates. The system however, needs proof that the user is already in the possession of a copy of the certificate in order to allow the verification of the certificate. Without a copy of a diploma, no personal information can be derived from the blockchain. With a copy of a diploma, only the information about the originality and the revocation status can be derived from the blockchain.
Predicted Outcomes	Less forged diplomas, less unqualified people in jobs, more trust in education, less work in verifying university certificates.

Overview of the Business Problem or Opportunity

When the recruitment process becomes digital, the proof of the authenticity of university degrees is lost. Scanned PDFs are easy to forge. The number of verification requests is rising.

Why Distributed Ledger Technology?

The solution combines a server at the University of Geneva, a regulated digital seal according to the Swiss law ZertES and a smart contract on the Ethereum blockchain. This combination was chosen for the pilot project to reach a maximum durability and to evaluate the advantages and disadvantages of the different solutions. The ultimate goal is to replace paper certificates.

The advantages of DLT in this context are:

- Certificates can be revoked
- Certificates can be verified even when the university server is down
- The blockchain-based proof does not need any maintenance by the university

Section 2: Current process

Current Solution

Until now, diplomas have only been issued on paper

Existing Flow

Step	User Actions	System Actions
1.	Generate und print diploma	Provide data and template
2.	Apply manual seal	No automation
3.	Distribute paper diploma to students	No automation

Participants and their roles

Actor	Type/Role	Description
1	*Students*	Students currently scan their diplomas and use the scan in the recruitment process

Participants and their roles		
Actor	**Type/Role**	**Description**
2	*Employers*	Employers either trust the scans or manually send a verification request to the University of Geneva

Section 2: Pilot process

Pilot Solution
The pilot does not disrupt the diploma generation but is an add-on to the current process

Flow (pilot)		
Step	**User Actions**	**System Actions**
1.	Generate und print diploma	Provide data and template
2.	Apply manual seal	No automation
3.	Scan diploma	Add third page with description and generate PDF/A
4.	Confirm electronic seal	Add electronic seal
5.	Sign blockchain transaction	Calculate hashes and send them to the smart contract
6.	Send PDF/A by email and distribute physical diploma to students	Partly automated
7.	Employers receive a digital or printed copy of the diploma	
8a.	Verification of the PDF/A by employer	An employer can • verify the digital seal on the PDF/A • verify the PDF/A through the university website • calculate the hash value of the PDF/A and verify it directly against the smart contract on the Ethereum blockchain
8b.	Verification of a link (ID) by employer	The student can send a special link to the employer which acts like a key. This link will confirm the information on the diploma. The link can be deactivated
8c.	Verification of the information on the diploma	An employer can verify the information on the diploma • through the university website • by calculating the hash value of this information and verifying it directly against the smart contract on the Ethereum blockchain

Section 3: Final process

Expected Flow (Production)		
Step	**User Actions**	**System Actions**
1.	Confirm diploma to be generated	Generate PDF/A
2.	Confirm application of digital seal	Apply digital seal
3.	Sign blockchain transaction	Calculate hashes and send them to the smart contract
4.		Send signed PDF/A to students
5.	Optionally print diploma, apply physical seal and distribute it to students	Manual process
6.	Employers receive a digital or printed copy of the diploma	
7a.	Verification of the PDF/A by employer	An employer can • verify the digital seal on the PDF/A • verify the PDF/A through the university website • calculate the hash value of the PDF/A and verify it directly against the smart contract on the Ethereum blockchain
7b.	Verification of a link (ID) by employer	The student can send a special link to the employer which acts like a key. This link will confirm the information on the diploma. The link can be deactivated
7c.	Verification with the information on the diploma	An employer can verify the information on the diploma • through the website of the university • by calculating the hash value of this information and verifying it directly against the smart contract on the Ethereum blockchain

Participants and their roles		
Actor	**Type/Role**	**Description**
1	*University*	Creates the certification if student has complied with all prerequisites and sends it to the student
2	*Student*	Determines who shall be able to see and verify the diploma

Participants and their roles		
Actor	**Type/Role**	**Description**
3	*Employer, etc.*	Employer is able to verify the diploma even in the unlikely event that the university is not reachable anymore

Data and information		
Data	**Type**	**Description**
1	*Documents*	Diploma with digital seal
2	*Hashes*	Hashes of the PDF/A and of a short form of the relevant information will be written to a blockchain through a smart contract
3	*Revocation*	A revocation entry can be added through the smart contract

Security and privacy
1.Great care has been taken to provide a very high level of security and privacy. *There is a key management system for the keys that allows diploma hashes to be put or revoked to the Ethereum blockchain.* *Without already having access to a diploma, no information can be derived from the blockchain. With the diploma, no additional information is available except in case of revocation of the diploma*

Main Success Scenario + expected timeline
The pilot system works even for only one university using the system. However, universities should join forces, develop a common system or even interface with a system for self-sovereign IDs

Conditions (pre- or post-)
The final version requires the adaptation of the internal regulation of the University concerning the formal requirements of a diploma

Performance needs
With only a couple of thousands of diplomas being issued per year, the performance of Ethereum is sufficient

Legal considerations
An in-depth evaluation of GDPR was part of the project

Risks
Application of GDPR on DLT still involves some legal uncertainty.

There might be an evolving standard for university diplomas. Current diplomas might have to be migrated in the future

Special Requirements

Transaction fees need to stay manageable

External References and Miscellaneous

An in-depth description of the project can be found here:

https://erbguth.ch/slides/DiplomaPaper.pdf

Other Notes

Any assumptions, issues

Appendix 1:
Domains and subdomains for use cases categorization

Vertical:

1. Finance
   a. Financial management & accounting
   b. International & interbank payments
   c. Clearing and settlement
   d. Reduction of Fraud
   e. Financial messaging
   f. Asset lifecycles and history
   g. Trade finance
   h. Regulatory compliance & audit
   i. AML/KYC
   j. Insurance
   k. Peer-to-peer transactions
2. Healthcare
   a. Pharma
   b. Biotechnology
   c. Medicine
3. Industries
   a. Manufacturing
   b. Energy
   c. Chemical
   d. Retail
   e. Real estate
   f. IT and telco
   g. Supply chain management
   h. Transportation
   i. Agriculture
4. Government and public sector
   a. Taxes
   b. Government and non-profit transparency
   c. Legislation, compliance & regulatory oversight
   d. Voting
   e. Taxation and customs
   f. Intellectual property management
   g. Land Registries

Horizontal:

1. Identity management
2. Security management
   a. Public Key Infrastructure
3. Internet of Things

4. Data processing, storage and management
    a. Data Validation (includes provenance)