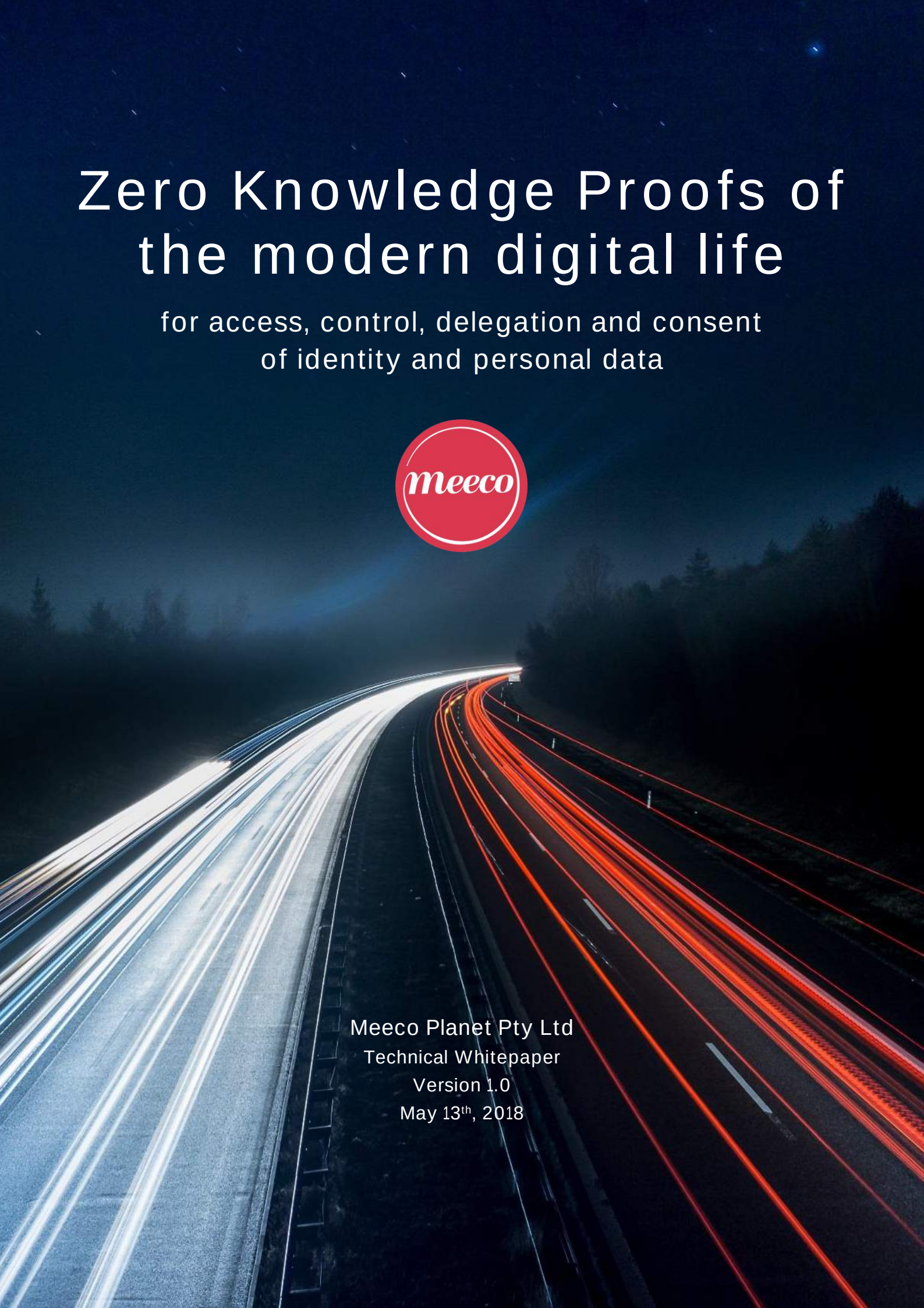
Zero Knowledge Proofs of the modern digital life

for access, control, delegation and consent of identity and personal data



Meeco Planet Pty Ltd

Technical Whitepaper

Version 1.0

May 13th, 2018

"Up until now the power to capture, analyse and profit from personal data has resided with business, government and social networks.

What if you and I had the same power?"

Meeco Manifesto, 2012

Abstract

This Whitepaper details Meeco's approach to enable a commercial, legal and technological bridge between highly regulated, trusted economic actors (government, financial services and telecommunications) and a personal data ecosystem that includes people participating directly in the value chain via the "API-of-Me".

In the last decade, the over collection of personal data has led to a steady decline in trust in governments and commercial enterprise. Data abuse, lengthy obfuscated terms and conditions have led to the European Union mandating significant changes through the General Data Protection Regulation (GDPR), effective 25 May 2018. The penalty for breaching these new laws is the greater of 4% of global revenue or €20M.

Conversely, the rise of blockchain and distributed ledger technology (DLT) has enabled agency and transparency, but not yet seen wide stream adoption. Current users of blockchain are limited to innovators and early adopters. Sociotechnical barriers such as a culture of distrust, or interoperability issues, likely contribute to this lack of adoption. Meeco is able to create verifiable trust through integrations with identity and service providers.

Zero Knowledge Proofs (ZKP) are a way to prove that something is true without revealing what the data is. Meeco's distributed ledger technology uses Zero Knowledge Proofs together with high assurance government and financial services information and identity schemes, to reduce cost and risk, whilst creating net new value.

The Meeco solution provides access, control, delegation and consent from the perspective of the individual user. Meeco enables people (data subjects) to provide their own verified records and controlled consent. This API-of-Me allows Meeco to provide a meta-data driven attribute wallet with no knowledge of the data to any authenticated identity of a user, which in turn enables an auditable personal-event chain of data interactions at scale.

It's distributed ledger technology that makes this new paradigm possible. Service Providers can trust the logic they provide through a smart contract. The smart contract can verify the authenticity of the data that the person provides against the issuer using Zero Knowledge Proofs, this allows the Service Provider to trust the output of the smart contract without seeing the persons data.

Currently, people give their data to businesses so that they can apply business logic. Meeco reverses this by having the business provide some business logic to the person to apply to their data. Through progressive disclosure, the person can reveal the minimum amount of data until they are ready to transact.

Meeco's business model drives participation where each of the key actors of this trusted ecosystem are incentivised to co-operate. The economic actors are people (data subjects), governments, service providers (financial services, telecommunications and utilities), Master

Node operators and Master Node backers. To achieve this trusted eco-system the network is comprised of the following six drivers:

1. **Tokenomics**: Economic incentives for Master Nodes, Backers, Service Providers, Identity Providers and People
2. **Treasury**: Funding for proposals from Meeco account holders to develop network utility
3. **Governance**: Verification, administration and economic incentives
4. **Recovery**: Checks and balances to enable network participants data recovery without relying on one single entity
5. **Consent Engine**: Fine-grained control over access, delegation and consent of identity and personal data
6. **Progressive Disclosure**: Multi-step data reveal process to lower risk and manage compliance prior to transaction.

These actors working together with verifiable trust in the Meeco ecosystem provide the means for all members of society to participate through the value unlocked from their data.

Authors

Ben Longstaff	**Katryna Dow**	**Claire Hoban**
Blockchain Architect	Founder & CEO	Blockchain Analyst

Acknowledgements

Behind the words and diagrams in this whitepaper is an amazing team of people. In gratitude to our wonderful engineers; Derek Munneke, Michael Drozdowski, Ricardo Santos, Brent Jacobs, Stephen de Bruin, Paul Robinson, and Ben Longstaff, they make the technology featured a reality.

Every day, Maria Rodrigues, Bjorn Halfmann, Lyndsey Jackson and Claire Hoban bring our ideas to life through design, UX and research, while Mike Page, Elizabeth Boerner and Jeanne Piacentino are the front-line, working with our partners to help keep people at the centre of their digital life.

Governance and accountability are foundations of our business, we value the rigor that Robert Collins and Glenn Smith bring as stewards of our funds and Directors of our Board.

Lastly, Meeco would not be possible without the funding and support of our incredible shareholders, especially Chris Sutton, Stephen Turner and Peter Midgley, early believers who continue to champion our cause.

Together, we've been pioneering a way forward with personal data since 2012.

Thank you,
KD

Table of Contents

1. Background

In May 2016 Meeco submitted 'Immutable Me' [1] a co-authored paper for submission at the ID2020 summit in NYC. The paper started with this Problem Statement; With the advent of blockchain, is there an opportunity to add a distributed layer between the data value and the consumer of personal data? Furthermore, does the verification and provenance of the data enable an attestation, provided by a relying party, to eliminate the need to give up Personally Identified Information (PII) at all? How can we enable people to access all the data they generate with full control of their master record and permission data on their terms using verified attributes without sacrificing their privacy?

Now two years on this new Whitepaper sets out the research, development, progress and roadmap for Meeco to provide a solution to those problems. The lack of economic incentive to accept liability for relying on a Service Provider's data, has resulted in the centralisation and duplication of data. At the same time, as the world becomes more connected the size and impact of data breaches is increasing [2, 3].

"The completed review determined that approximately 2.5 million additional U.S. consumers were potentially impacted, for a total of 145.5 million." [4]
- **Equifax**

"Consumer Financial Protection Bureau Fines **Wells Fargo** $100 Million for Widespread Illegal Practice of Secretly Opening Unauthorized Accounts" [5]
- **Wells Fargo**

"AdultFriendFinder network hack exposes 412 million accounts" [6]
- Friend Finder Network

"Facebook–Cambridge Analytica data scandal involves the collection of personally identifiable information of up to 87 million Facebook users" [7]
- **Facebook**

Meeco reverses the model so that the business provides a portion of its logic to the person so that through progressive disclosure they can decide if the business meets their needs, only revealing information to the business when they are ready to transact.

Meeco acts a bridge to self-sovereign identity from high assurance identity schemes that exist in government and financial services.

Distributed Ledger Technology (DLT) makes this new paradigm possible when combined with Zero Knowledge Proofs [8]. Service Providers can trust the logic they provide through a smart contract and the smart contract can verify the authenticity of the data that the person provides against the issuer.

Before engaging in a digital transaction, the 'Triple As' of self-sovereign identity (Anchor, Authenticity and Agency) must be wholly addressed. This is realised through verified trust in the individuals very anchor of existence, usually supplied by the government (Anchor), trust

that the individual is who they assert to be (Authenticity), and trust that they are acting both freely and independently (Agency) [9].

The process is best represented in Figure 1. The Triple A's on the left are the required inputs for Zero Knowledge Proofs (represented by the inner circle). The outer circle represents the boundary of the self-sovereign system. Finally, on the right is the output of the system; the Zero Knowledge Proof verified Digital "me" [10].

The asymmetry of the design is representative of asymmetric cryptography (public and private keys) used to transact throughout the system [10]. When self-sovereign identity is supported by governments and organizations, it allows lifetime digital identity for all members of society, that is portable, persistent, protected and independent of any central authority [11].

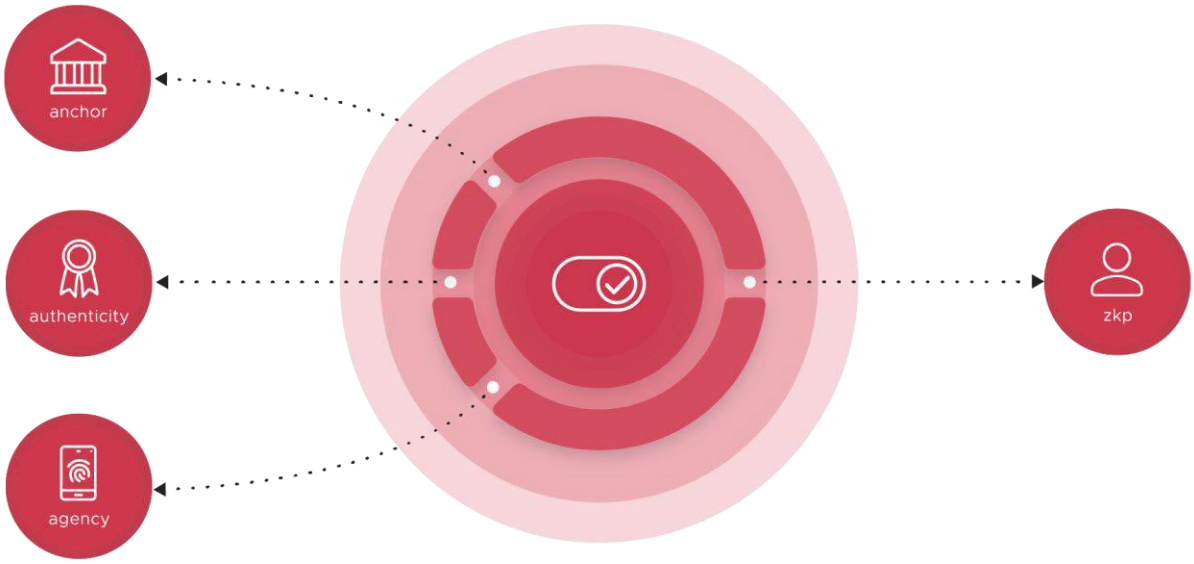


Figure 1: Self-sovereign identity [10] Anchor – the identity of the participants in the transaction must be anchored to verified identities from trusted Identity Providers. Authenticity – it is necessary to verify that the request originates from the owner of the data. Agency – process needs to be in place to ensure that the data own is acting of their own free will. [9]. Agency, Authenticity and Anchor are used with Zero Knowledge Proofs to verify the digital me.

Self-Sovereign/Zero Knowledge Proof Symbol Courtesy of: Tim Bouma, Gary de Beer, Dominik Kummer

Throughout the paper, Charlotte, Max and Mallory (the normal users), Mallory (also acting as a malicious user), Sam (the state actor), and Steve (the Service Provider) will be referred to.

1.1 Market forces

There are a number of regulatory changes acting as drivers for the adoption of data wallets, pushing more data and control back to data subjects with new user-centric business models.

The General Data Protection Regulation (GDPR) will apply from 25th May 2018, creating new rights for users regarding how they data is used [12]. The penalties for organisations that breach GDPR are either 4% of annual turnover or €20 Million, whichever is greater [13].

The Payment Services Directive 2 (PSD2) came into effect on the 13th January 2018 [14] which requires banks to open up their data to third parties. A push for Open Banking requires that banks open up their data in a standard format, this is taking place in the UK as part of Payments Services Regulations 2017 [15].

In May 2018 the Australian Government announced the official date to move to a new Open Banking regime, to commence in July 2019. This mandates all banks, commencing with the 'big 4' institutions to progressively provide customers with access to their financial data upon request to a third-party intermediary.

1.2 Benefits

Increased Collaboration and Privacy

Identity is moving beyond issued instruments like passports, social security cards and identity (ID) cards, and towards contextual identity in which "I can prove who I am" (persona) in the context of what I am doing [1]. Meeco users bring their data with them and choose what to share, who it is shared with and for how long. Distributed ledgers make user attributes verifiable in a trustless environment.

Increased Revenue and Cost Savings

Verifying the authenticity of documents against a transaction with the issuer reduces the cost of fraudulent transactions. In Australia, these "liar loans" could be worth as much as $500 billion [16]. A new level of rigor into evaluating loan serviceability can be provided with Meeco's technology.

Better Decision Making and Increased Efficiency

Middlemen whose business models are based on information asymmetry, such as mortgage brokers and credit reporting agencies, could be replaced with Meeco integrations.

Increased Data Quality and Consumer Trust

Meeco can increase integrity back to the banking sector. Charlotte is able to get a personalised offer from a Service Provider before disclosing sensitive personal information, this is examined in detail in section 2.3.3 Consent – progressive disclosure.

1.3 User stories

Applications of Meeco's technology can be applied to a wide range of use cases some of which are outlined below.

- Charlotte delegates authority to Max to interact with a Service Provider on her behalf and authorises Max to make changes to her account settings.
- Max and Mallory have a child who they grant read access to their health records, resulting in access to intergenerational health records.
- Sharing economy services like Airbnb are able to provide high assurance Know Your Customer (KYC) processes.
- Charlotte can repair her credit history after her data was stolen in the Credit Bureau hack by proving her credit worthiness.
- Max can create a persona with limited attributes for his online dating profile, but the dating site can perform a high-level KYC check.

- Charlotte wants to find the best offer to refinance her mortgage and can use a concierge service to check what the best service each bank and credit union can offer without disclosing any of her information.
- Mallory and Max are able to enrol and manage their family's access to services.

2. Technology

There are three parts to the Meeco ecosystem: Meeco Clients, the API-of-Me and the Meeco Distributed Ledger. Meeco's technology stack is designed to empower people with Access, Consent, Delegation and Control over how their data can be used with the people and organisations they trust.

Meeco never has plaintext access to a person's data. Data is only accessible in plaintext on the user's device, inside a trusted execution environment or when Charlotte chooses to transact with a Service Provider or Identity Provider. Meeco uses pairwise-pseudonymous identifiers to prevent any information about the user being leaked through addresses being reused across transactions

The Meeco Clients and the API-of-Me sit at the application layer of the technology stack built on top of the Meeco Distributed Ledger protocol.

2.1 Meeco clients

The first iOS Meeco prototype was built in 2013 and has been through many iterations of the UI/UX through Meeco labs and commercial collaborations. Meeco currently has iOS and Android clients available in the respective app stores. These apps already feature an event chain, consent engine, attribute wallet and data vault. Future development of the Meeco clients is focused on Service Provider integrations and integrating with Meeco's Distributed Ledger.

Meeco is an early pioneer in the research, development and deployment of first person data technology. It is important to note that the featured applications in sections 2.1.1, 2.1.2 and 2.1.3 is existing technology and not conceptual. Meeco has already invested significantly in the realisation of this technology.

2.1.1 Event chain

The event chain is an immutable record of a user's events that contain the type of event, the subject, when it occurred and who it occurred with (Figure 2). The types of events that are stored include: create, update, delete, view, milestone, start, stop, pause, resume, share and share request.

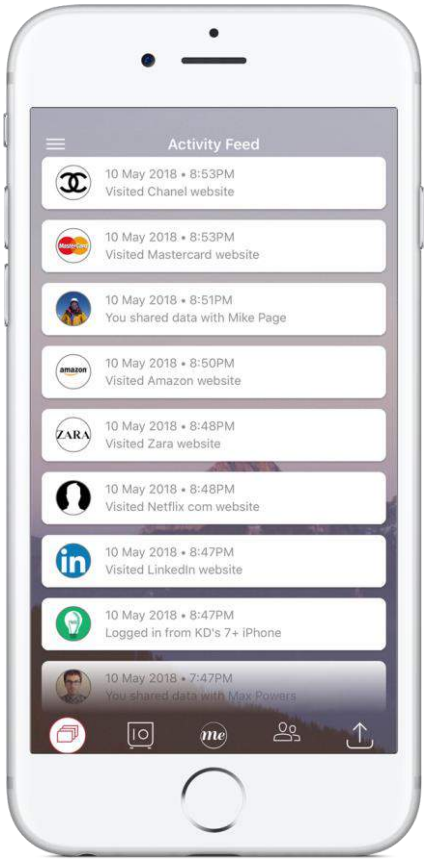


Figure 2: Immutable person event chain

All events and interactions in Meeco are recorded as immutable events, providing a personal chain of behaviour. This chain can be analysed to provide a feed of activities or scored to provide a reputation indicator for a specific purpose.

The event chain is a generated data asset for the individual. As every event chain is unique, this provides strong assertion for fraud management, identification, authorisation and authentication. The event chain can record devices in use, share date, web history, data requests and consent receipts.

Events can include (but not limited to) which device is in use, when data is shared, a consent receipt for data shared, when a connection is made, integrations with social networks, web browsing and when data is amended or deleted.

2.1.2 Permissions and consent engine

The value of a user's data is unlocked by sharing. Meeco stores the terms that a user agrees to share their data and provides a record of the consent (Figure 3). Selective sharing enables progressive disclosure, allowing users to select the minimum attributes to share in exchange for the maximum benefit.

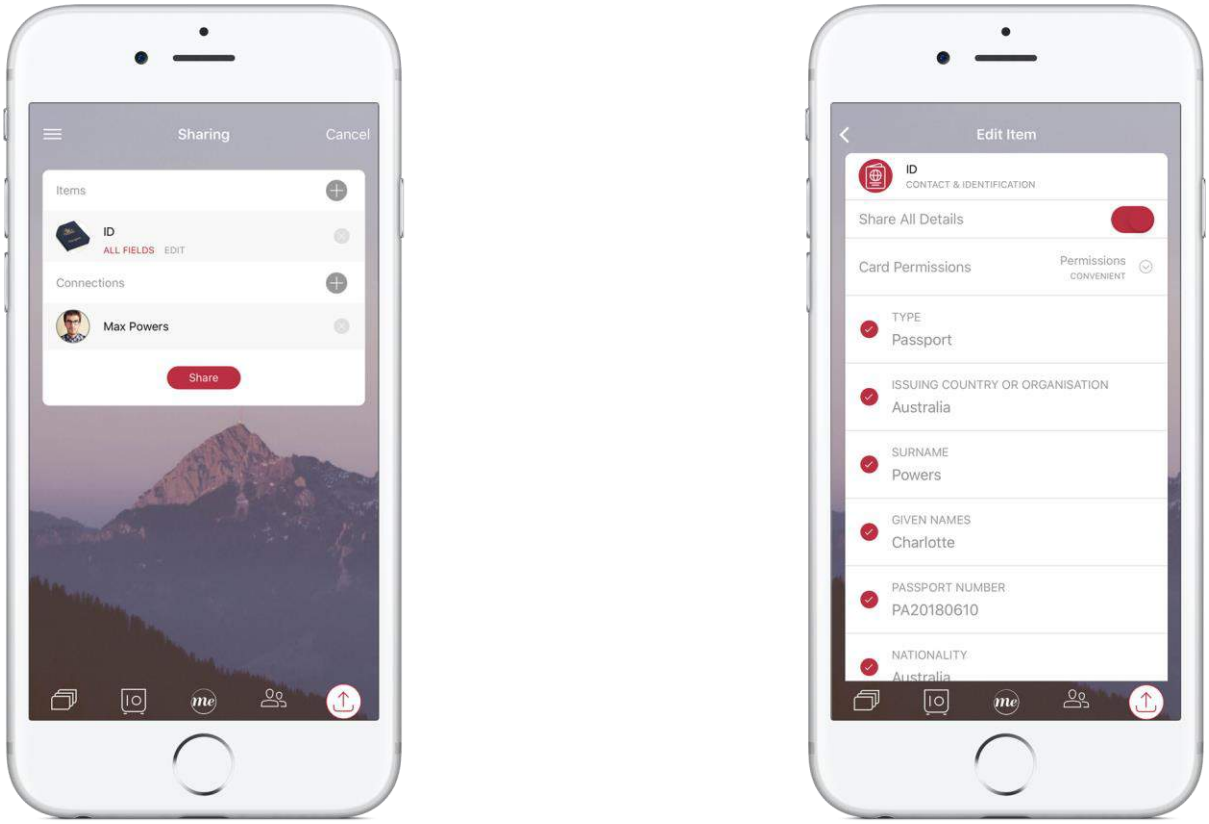


Figure 3: Meeco consent engine

The Meeco consent engine can enforce rules such as duration and on-sharing in the system, a receipt of consent is stored in the event chain. Permissions enable data to be shared for minutes, hours, until a set-date or for the duration of service and can be edited before, during or after data is shared.

2.1.3 Attribute wallet and data vault

A card is created from a template and holds specific data about a user in the data wallet (Figure 4). These cards are analogous to the cards that you carry in your physical wallet. The tile can contain slots (key value pairs), which are a dynamic way to add data to the tile. This is similar to how a coffee club card has new information added each time you use it. Data can be added in three ways; (i) pushed to the wallet via APIs e.g. bank provisioned customer data (ii) connecting to data integrations via authenticated APIs e.g. social, fitness or IoT data (iii) self-asserted data e.g. adding directly to wallet. Meeco's data wallets also support tags, notes and attachments.

Meeco enables verified attributes from the issuer or verifier to be shared with a user for use in future transactions. Meeco's data vault is a flexible API accessible key value store with categorisation for semantic interpretation. The vault stores encrypted data that is only accessible in plaintext on the user's device.

Each data item and slot are individually addressable and can be referenced via a pairwise pseudonymous identifier for protected sharing, this is shown in the following examples.

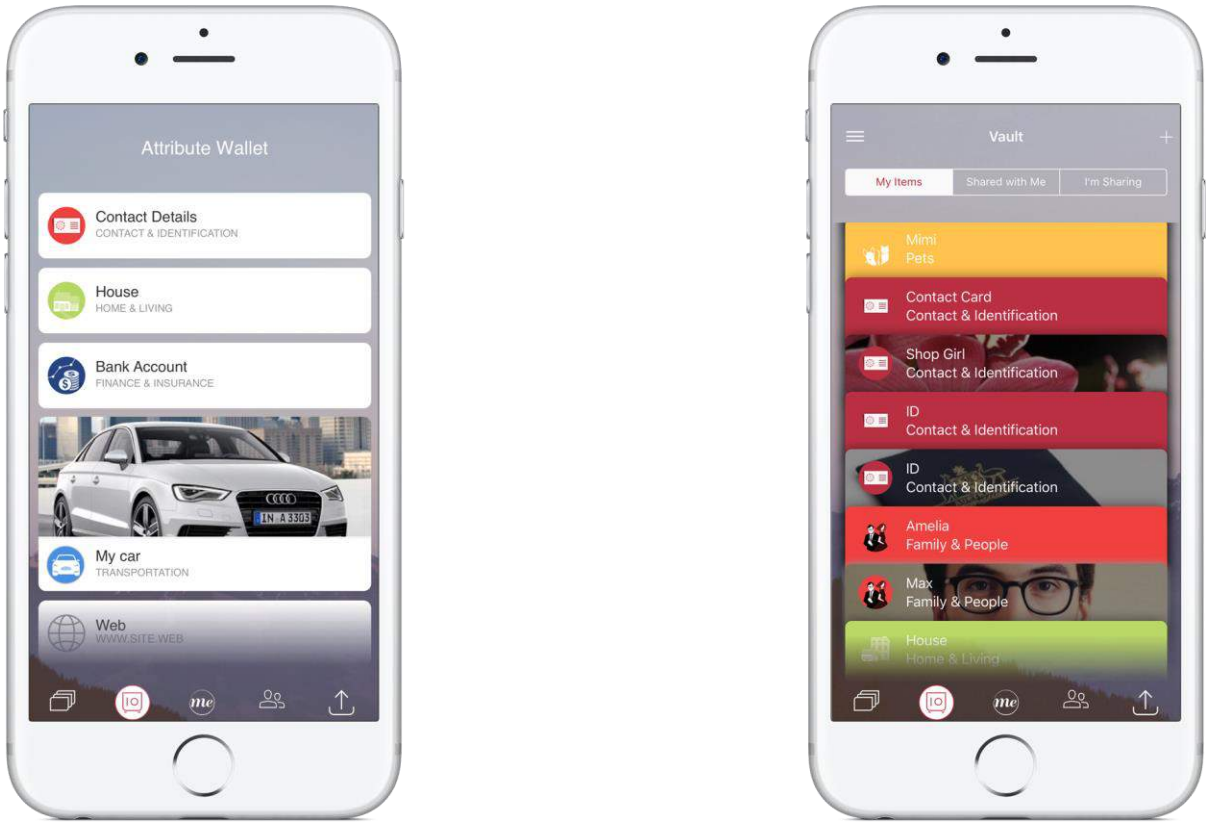


Figure 4: Data vault cards

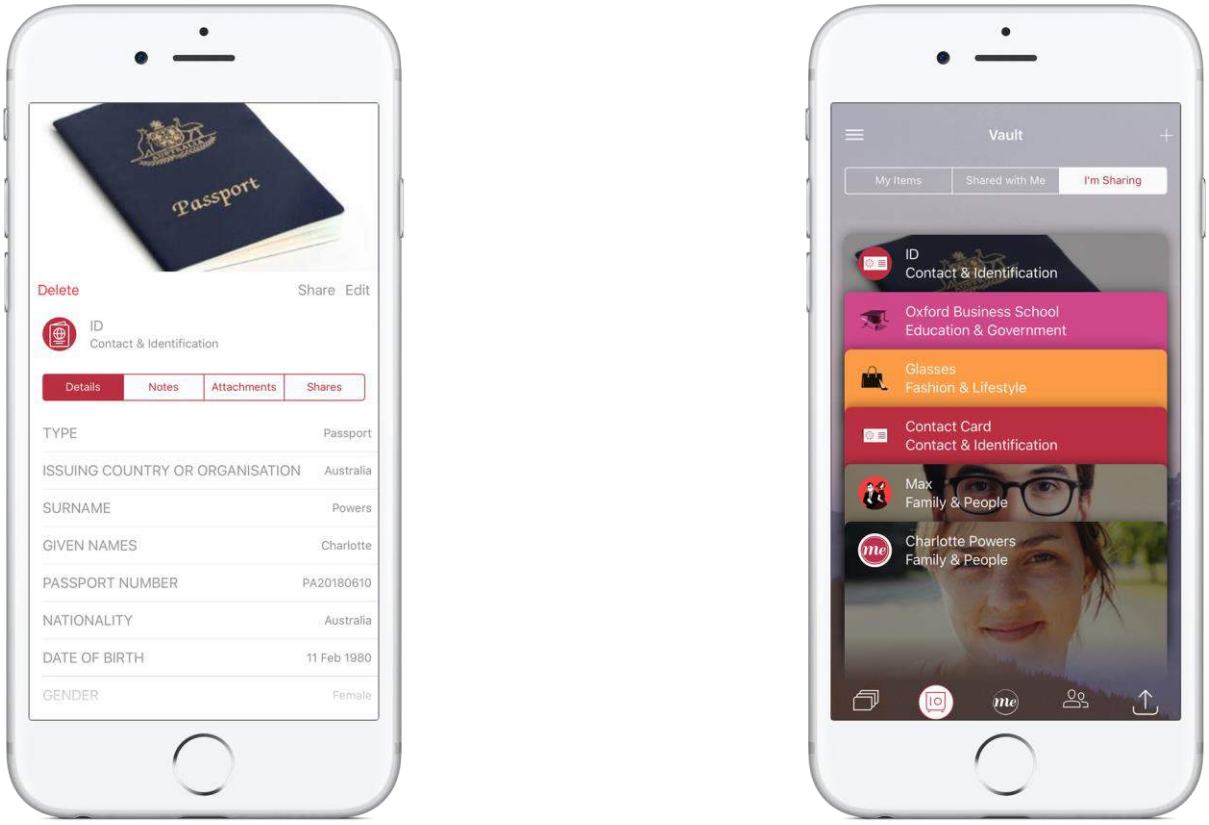


Figure 5: Screenshots from the existing Meeco app. An example attachment on the left, these can be a letter of authority, certificates of incorporation, passport, driver's license or e-identity cards. This acts as a backup for key documents. The permission dashboard is shown on the right.

The Permission dashboard shown in Figure 5 (on the right) is a user dashboard for the consent engine, allowing Charlotte to view and control her data's use. Charlotte is able to see what attributes have been shared with other people or organisations, together with the permissions set.

Meeco released the first version of the Consent Engine (enabling user asserted terms in October 2015), with the ability to provide fine-grained permission (by attribute) for data access based on duration (till deleted), time (minutes, hours) or fixed date. Data shared will automatically delete based on the access terms. Meeco's Consent Engine is a key business enabler for GDPR and Open Banking compliance.

2.2 Permissioned distributed ledger

Identity providers are able to create verified attributes for:

- Inherent characteristics e.g. date of birth, gender, and biometrics
- Assigned attributes e.g. name, social security number, passport number, employer ID
- Acquired attributes e.g. address, purchase history, device location, device attributes

A Service Provider can be a government or a private company. Meeco is focused on integrating with banks, telcos, utility providers and government services to bootstrap the network. Service providers are able to create verified claims for attributes like:

- Individual preferences e.g. favourite bands, taste in music

- Acquired attributes e.g. address, purchase history, device location, device attributes

Storing a hashed identifier in a Distributed Ledger means that verifying the authenticity of data can be done in isolation.

Zero Knowledge Proofs [8] can be used with a Merkle Hash [17] and the person's data to prove their claims are true without having to reveal the data to the Service Provider. The Service Provider can trust the authenticity of the data as it has been verified against the issuer. The output of the smart contract can be trusted as it contains the Service Provider's business logic and is executed with verified data.

Different Service providers will opt to make use of different parts of the Meeco ecosystem. Table 1 shows the responsibilities of the Service Provider and how the level of integration changes between the different types. Note that each row is independent, and a Service Provider may opt to do multiple types of integrations.

Integration	Requirements	Responsibilities
Running a Node	Deploy a high availability server.	Keep server online. Governance participation
Using Smart Contracts	Design and deploy smart contract logic through Meeco services. Integrate with the API-of-Me to make calls to smart contract. Purchase tokens to fund smart contract execution.	Update smart contract logic as business logic changes.
Consent Engine	Integrate with the API-of-Me	none
No Integration	Meeco may write a proxy integration to the Service Providers existing APIs if it adds sufficient utility value to the network.	none

Table 1: Types of Meeco integrations

2.2.1 Transactions

When the authenticity of data needs to be verifiable, a transaction is made between the data issuer and a unique wallet address for the user. The transaction contains the public key for the sender, the public key for the recipient and a Merkle tree root hash [17] for the data.

The data stored on the Distributed Ledger will be a Merkle tree root hash or the output of a smart contract, the standard for the outputs will initially be similar to http codes. When the output of a smart contract is written to the Distributed Ledger, a hash of the inputs is included with the output code. This allows the challenge protocol to prove if a Master Node is not processing the transactions correctly.

Public Key Registry

The public key registry is a list of public keys for the Master Nodes, Service Providers, Identity Providers and Data Concierge. Users are able to use public key encryption to send encrypted messages to the listed Service Provider, Identity Provider or Master Node that they wish to interact with.

Wallet Registry

The wallet registry is a list of wallet addresses that are owned by different Service Providers and Identity Providers. This enables verification of where the issued data originated.

Smart Contracts

The functionality of smart contracts is separated into three components as shown in Figure 6. The Dispatcher contract's role is to store the address of the smart contract with the functionality and contain the logic to change the functionality contracts address.

This makes it easy to upgrade the functionality without having to change the smart contract address that is called by dApps. The governance contract contains the logic for the relevant stakeholders to vote in upgrading the functionality, and the mechanism to execute the upgrade. The final component is the actual functionality.

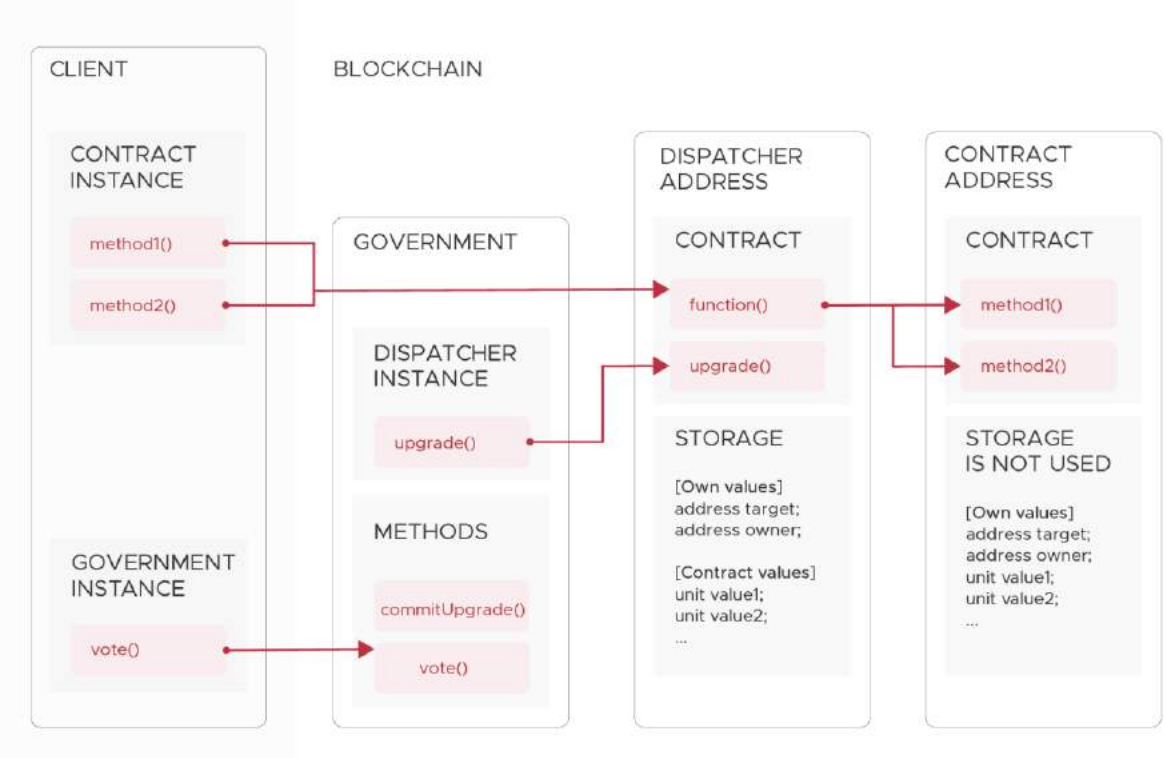


Figure 6: Splitting functionality for upgradability is based on NuCypher's approach [18].

2.2.2 Challenge protocol

The purpose of the challenge protocol is to introduce work into the network where the output of executing the smart contract is known so that it can be objectively proved if a Master Node is processing transactions correctly. If the Master Node is found to be incorrectly processing transactions, then the participants in the challenge process receive a portion of the Master Node's stake.

When a challenge request is made, the requestor knows what the output from the smart contract should be. If the output is different, the requestor can make a second call to a challenge contract with the input they submitted and proof that the Master Node has processed it incorrectly. The result can be re-evaluated by other nodes to verify if the output was incorrect, the inputs are validated against the input hash that was written to the Distributed Ledger with the output.

Token holders have two economic incentives to challenge Master Nodes; the challenge reward and ensuring the integrity of the network's utility. The value of their tokens will increase as the value of the network's utility increases.

2.3 Operations

The following sections outline how people are able to use Meeco for Access, Consent, Delegation and Control of their data.

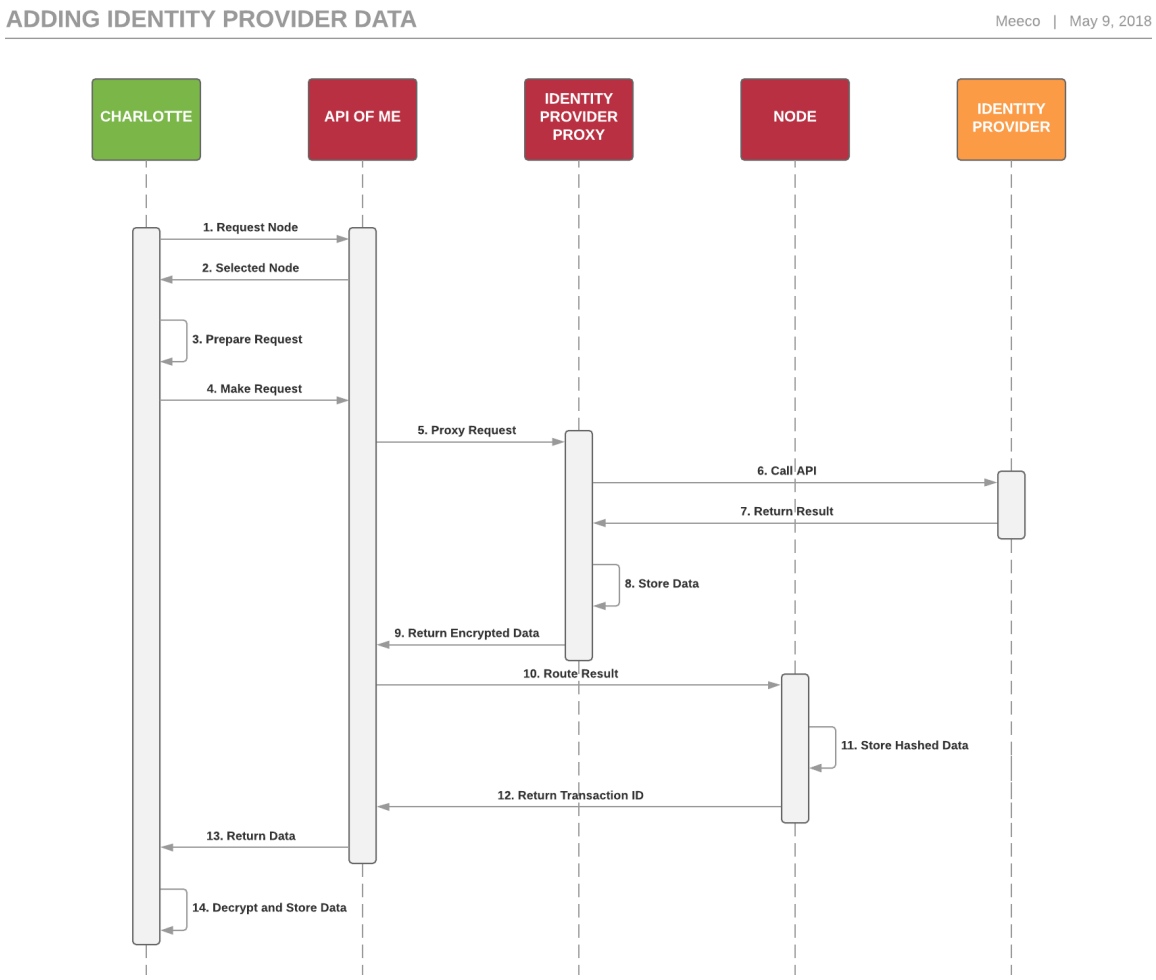
2.3.1 Access – adding data from an identity provider

This section outlines how data from an Identity Provider is verified and added into Charlotte's data wallet and Event Chain. Note that the Identity Provider does not receive the blockchain transaction ID or Charlotte's wallet address.

This section only assumes that the Identity Provider has an API and does not assume that the Identity Provider has done any work to integrate with Meeco. The Identity Provider proxy is a thin API that bridges the Identity Provider's API and Meeco (it is separate from the API-of-Me).

The Identity Provider proxy sends the encrypted data to the API-of-Me, instead of to the node directly. This allows the API-of-Me to handle retrying the request if the node goes offline.

In the description below, the **public key for Charlotte's wallet** refers to the wallet that has been created specifically to interact with the Identity Provider. Charlotte has one wallet per Identity Provider. The **public key for the node** refers to the node that is selected to process the result of the interaction.



1. A request is made to select a node to process the request.
2. The **public key for the node** is returned.
3. The **public key for Charlotte's wallet** is encrypted with the **public key for the node**. The **public key for the Identity Provider** is found in the Meeco Public Key Registry on Charlotte's device, this is used to encrypt a payload containing:
    a. A **public key for Charlotte's device**
    b. The **encrypted public key for Charlotte's wallet**
    c. The identity documents to be verified by the Identity Provider
4. The encrypted payload is sent to the API-of-Me.
5. The request is then sent to the Identity Provider's proxy.
6. The **private key for the Identity Provider** is used to decrypt the encrypted message. The identity documents are then sent to the Identity Provider via the API.
7. The Identity Provider's response is returned to the Identity Provider proxy.
8. For an Identity Provider where attributes can change, Charlotte must consent to an identifier being stored to received updates, so Charlotte's identity is stored by the Identity Provider proxy with a device identifier. This is so that updates can be pushed by the Identity Provider.
9. The **public key for the node** is used to encrypt a payload containing:
    a. The response from the Identity Provider
    b. A transaction request from the **Identity Providers wallet** to the **encrypted public key for Charlotte's wallet**

c. A **public key for Charlotte's device**

The encrypted payload is sent to the API-of-Me.

10. The API-of-Me sends the encrypted payload to the node.
11. The **private key for the node** is used to decrypt the payload. The **encrypted public key for Charlotte's wallet** is decrypted with the **private key for the node**. The payload from the Identity Provider is used to create a Merkle tree and the root hash is written into the blockchain as part of the transaction data from the **Identity Provider's wallet** to **Charlotte's wallet**.
12. The **public key for Charlotte's device** is then used to encrypt a payload containing:
    a. The blockchain transaction ID
    b. The response from the Identity Provider
    c. The **Identity Provider's wallet**
    d. The **public key for Charlotte's wallet**

    The encrypted payload is sent to the API-of-Me.
13. The encrypted payload is returned from the API-of-Me to Charlotte's device.
14. The encrypted payload is decrypted with the **private key for Charlotte's device**, the blockchain transaction details and the response from the Identity Provider are stored in Charlotte's data wallet and Event Chain.

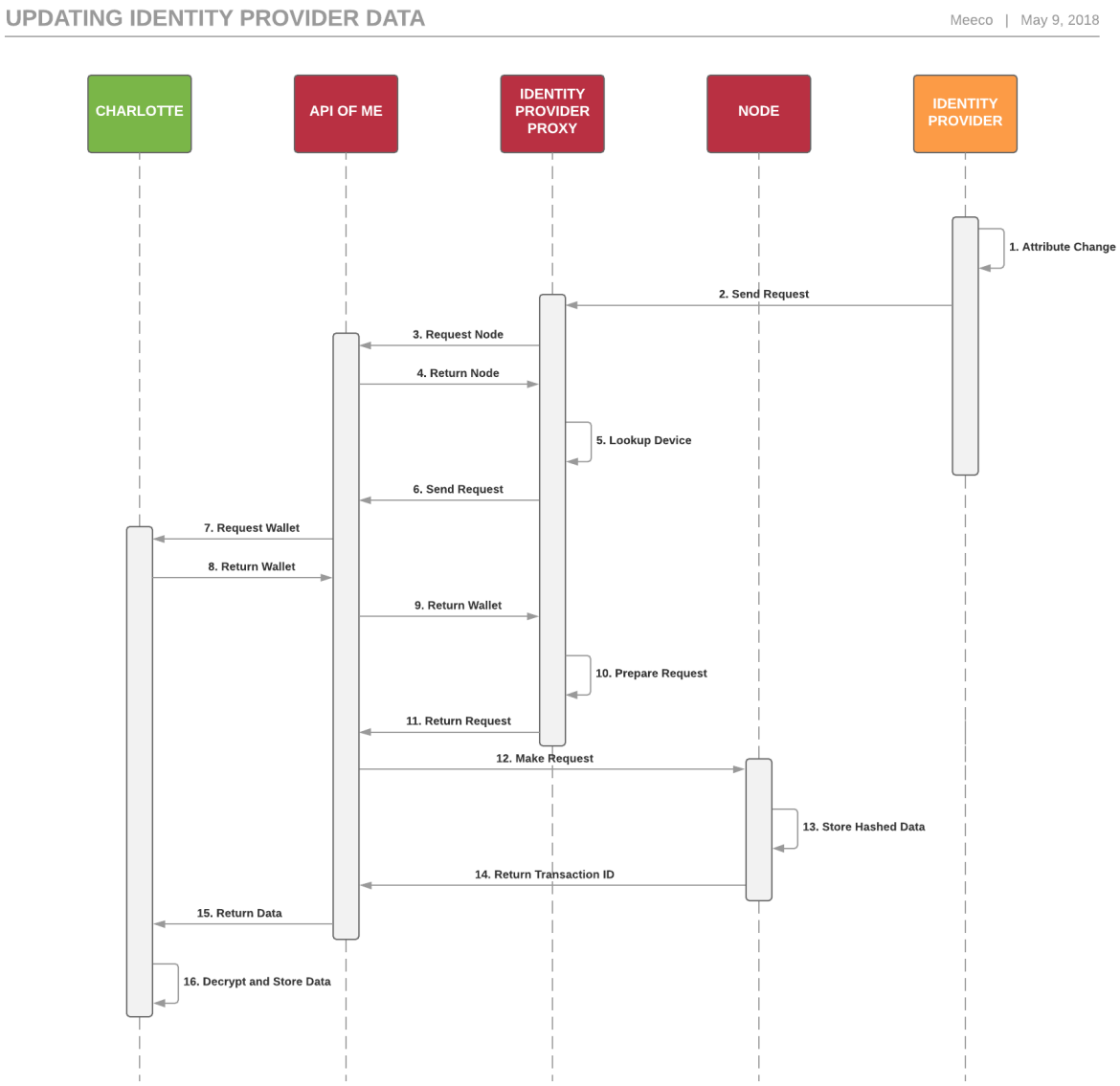
2.3.2 Access – updating data from an identity provider

This section shows how an Identity Provider can push updates to a transaction. Example use cases are: Charlotte changed her address or had her license revoked. The Identity Provider does not receive the transaction id or the user's wallet information. When a smart contract verifies attributes, it gets all of the transactions between Charlotte's wallet address and the Identity Provider's wallet address so that it has an up to date view of the state of Charlotte's attributes.

This functionality requires that the Identity Provider has integrated with Meeco to push updates.

For an Identity Provider to send updates, Charlotte has to consent to the Identity Provider pushing updates. The Identity Provider proxy stores a relationship between Charlotte's identity, her wallet address and her device. The next time that Charlotte's device connects to the API-of-Me, it will pull down the new information.

In the description below, the **public key for Charlotte's wallet** refers to the wallet that has been created specifically to interact with the Identity Provider. In this example, Charlotte has one wallet per Identity Provider. The **public key for the node** refers to the node that is selected to process the result of the interaction. The public key for Charlotte's device is not stored in the public key registry.



1. An event triggers a change in state of one or more attributes in Charlotte's identity.
2. A request is sent from the Identity Provider to the Identity Provider proxy.
3. The proxy requests a node to process the transaction.
4. The **public key of the node** is returned to the Identity Provider proxy.
5. The device identifier is looked up from the proxy's records based on Charlotte's identity.
6. The device identifier is sent to the API-of-Me to request an **encrypted public key for Charlotte's wallet**.
7. The API-of-Me sends the request to Charlotte's device.
8. When Charlotte's device next connects to the API-of-Me, it receives the request and returns the **encrypted public key for Charlotte's wallet.**
9. The **encrypted public key for Charlotte's wallet** is sent to the proxy.
10. The **public key of the node** is used to encrypt a payload containing:
    a. The identity data change
    b. A transaction request from the **Identity Providers wallet** to the **encrypted public key for Charlotte's wallet**
    c. The **public key for Charlotte's device**

    d. A device identifier
11. The encrypted payload is sent to the API-of-Me.
12. The request is sent to the selected node.
13. The **private key for the node** is used to decrypt the payload. The **encrypted public key for Charlotte's wallet** is decrypted with the **private key for the node**. The payload from the Identity Provider is used to create a Merkle tree and the root hash is written into the blockchain as part of the transaction data from the **Identity Provider's wallet** to **Charlotte's wallet.**
14. The **public key for Charlotte's device** is then used to encrypt a payload containing:
    a. The blockchain transaction ID
    b. The payload from the Identity Provider
    c. The **Identity Provider's wallet**
    d. The **public key for Charlotte's wallet**

    The encrypted payload is sent to the API-of-Me.
15. The encrypted payload is returned from the API-of-Me to Charlotte's device.
16. The encrypted payload is decrypted with the **private key for Charlotte's device**. The blockchain transaction details and the response from the Identity Provider are stored in Charlotte's data wallet and Event Chain.

Attack Vector – Provider collusion to build metadata

The Identity Provider proxy needs to store a link between Charlotte's device and her identity. If Charlotte's identity was able to be linked to her transaction, then providers could collude to build metadata around who Charlotte is. This is mitigated by the Identity Provider proxy only seeing the encrypted public key for Charlotte's wallet.

Attack Vector –manipulating distribution of work

If the Identity Provider proxy did the node selection, they could always choose to select a node that is owned by the Identity Provider to do the work. In addition to monopolising the work, the Identity Provider could potentially link Charlotte's identity to her device identifier. This is mitigated by the requests having to go through the API-of-Me.

2.3.3 Consent – progressive disclosure

To minimise the amount of information Charlotte has to reveal, Meeco supports progressive disclosure. This allows the interaction with a Service Provider to be broken into three interactions. In the case of a mortgage this might look like:

1. **Drive-By** – evaluate Charlotte's current situation. Does she have a mortgage? What is the value of her new mortgage and her income range? The output determines whether the Service Provider has products that apply to Charlotte without disclosing any information.

2. **Tell-Me-More** – supply documents and proof of income to create an offer that Charlotte is eligible for.

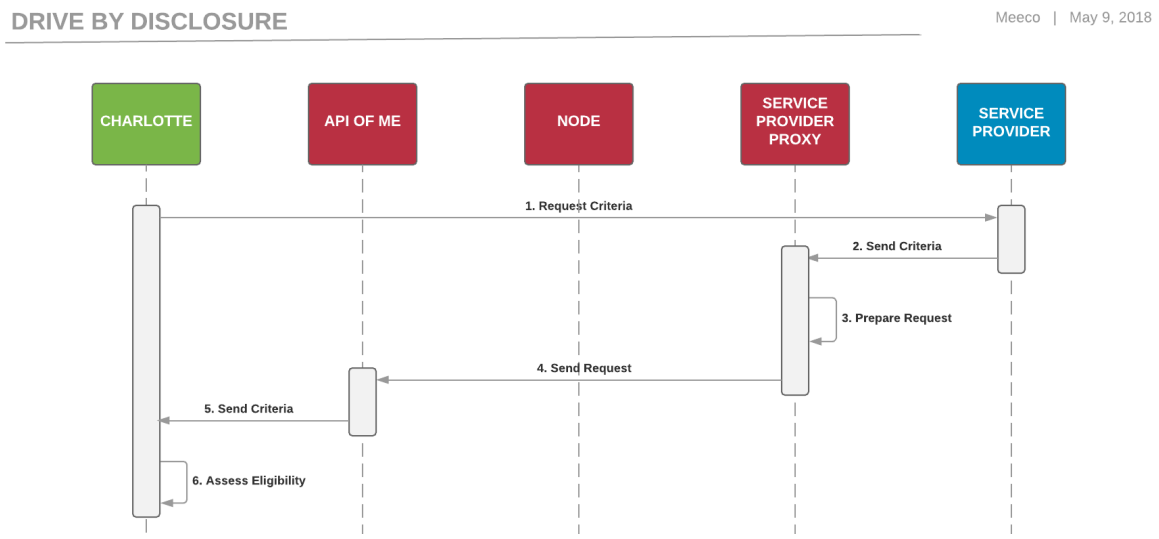
3. **Transact** – Charlotte reveals her identity, documents and proofs to execute the offer to get a mortgage.

The three stages differ in where the computation takes place, what type of verification is done and if Charlotte's data is disclosed. These stages of progressive disclosure are detailed in Table 2.

	Drive-By	Tell-Me-More	Transact
Computation	User's device	Blockchain	Blockchain and Provider
Verification	Unverified check	Zero Knowledge Proof	Verified attributes
User data disclosed	No	No	Yes[1]
Purpose	Check requirements	Determine eligibility	Take action

Table 2: Progressive disclosure summary

2.3.4 Drive-By disclosure



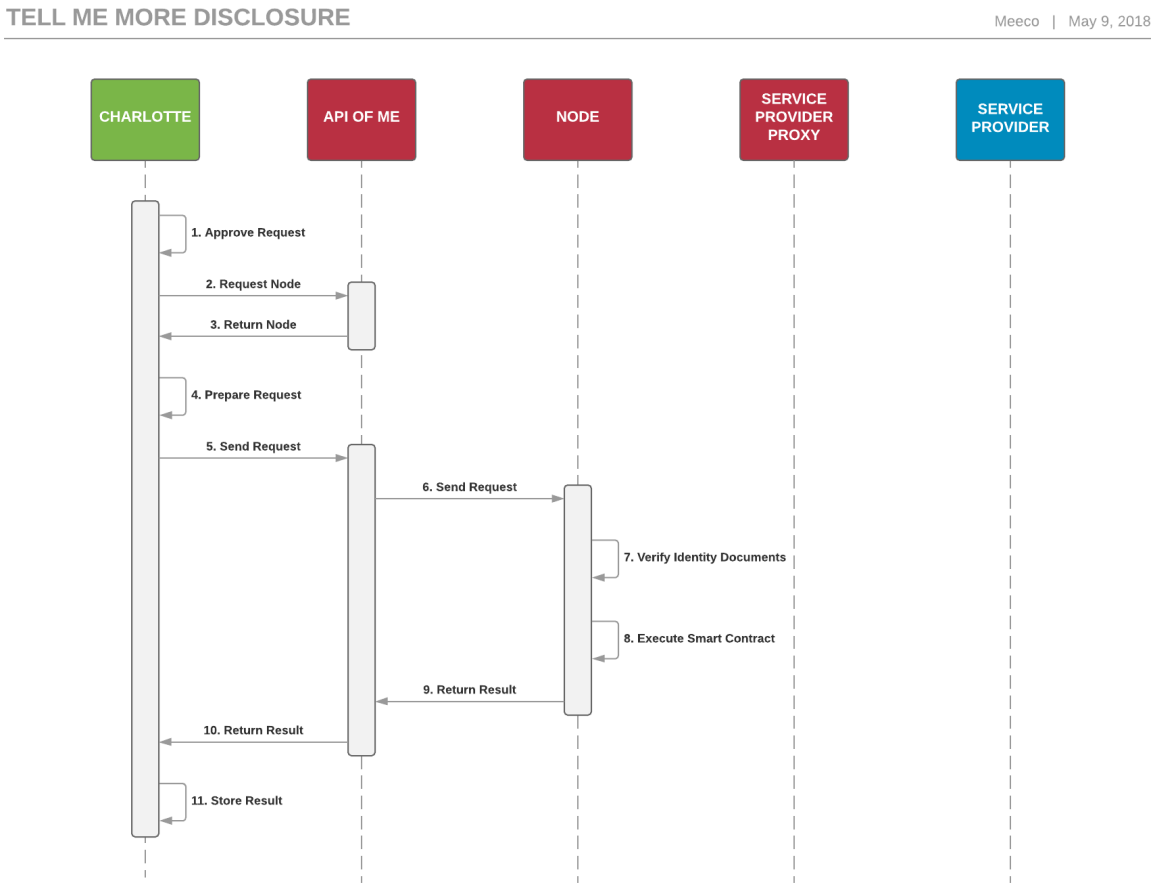
1. Charlotte initiates a request for the criteria to open an account on the Service Provider site.
2. The request is sent from the Service Provider to the Service Provider proxy.
3. The Service Provider looks up the appropriate smart contract, the required verified attributes and the acceptable range of values and approved Identity Providers.
4. The payload is sent to the API-of-Me.
5. The API-of-Me sends the criteria to Charlotte's device.
6. The requirements are assessed against the contents of Charlotte's data wallet. A result is displayed to Charlotte with an estimated likelihood of approval. This includes what data will be used to undertake a "Tell-Me-More Disclosure" assessment. Charlotte can then cancel or proceed to the next step.

[1] The reason that some user data is disclosed when transacting is that the Banks, Telcos, and Utility providers have a shared right to access the data required to meet the legal and regulatory obligations to be KYC and AML compliant.

2.3.5 Tell-Me-More Disclosure

The “Tell-Me-More” disclosure occurs after Charlotte has completed the “Drive-By” disclosure.

The **public key for the node** refers to the node that gets selected to process the result of the interaction with the Service Provider and commit it to the blockchain.



1. After Charlotte has done the “Drive-By” disclosure, she selects to proceed.
2. A node to process the request is requested.
3. The information about the node that will process the request is returned.
4. The **public key for the node** is used to encrypt a payload containing:
    a. A **public key for Charlotte’s device**
    b. A **public key for Charlotte’s wallet** with the Service Provider
    c. A **public key for Charlotte’s wallet** with the Identity Provider
    d. A proof that Charlotte owns the wallet with the Identity Provider
    e. A proof that Charlotte owns the wallet with the Service Provider
    f. **Charlotte’s identity documents**
    g. The transaction ID from the **Identity Provider’s wallet** to **Charlotte’s wallet**
5. The request is sent to the APIof-Me.
6. The request is sent to the selected node.
7. The **private key for the node** is used to decrypt the payload. **Charlotte’s identity documents** are hashed by the smart contract. The hash value is then compared with the hash that is attached to the transaction from the **Identity Provider’s wallet** to **Charlotte’s**

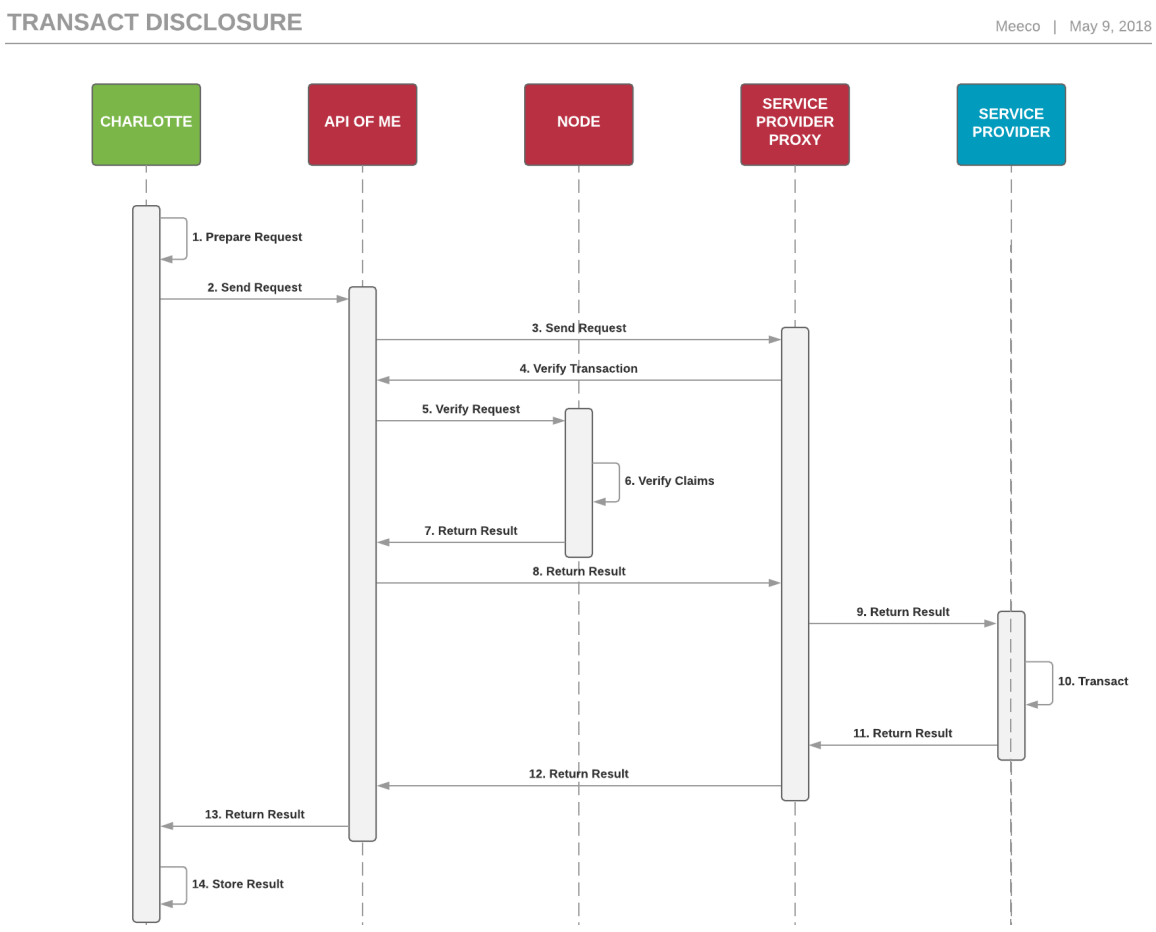
wallet. The smart contract then verifies Charlotte's proof of ownership of the wallet that interacted with the Identity Provider. If the two hashes match, then the smart contract can trust the identity documents provided by Charlotte.

8. The Service Provider's smart contract is executed, and the result is written to the blockchain.
9. The **public key for Charlotte's device** is then used to encrypt a payload containing:
    a. The transaction ID from the **Service Provider's wallet** to **Charlotte's wallet**
        a. The Service Provider smart contract address
        b. The **Service Provider's wallet**
        c. The **public key for Charlotte's wallet** with the Service Provider

    The encrypted payload is sent to the API-of-Me.
10. The encrypted payload is returned from the API-of-Me to Charlotte's device.
11. The encrypted payload is decrypted with the **private key for Charlotte's device**, the blockchain transaction details and the response from the Identity Provider are stored in Charlotte's data wallet and Event Chain. Charlotte is then presented with the outcome, the data that she will need to disclose to the Service Provider in order to transact and the option to execute the transaction.

2.3.6 Transact disclosure

The Transact Disclosure occurs after Charlotte has determined that she wants to transact with the Service Provider. In this interaction Charlotte reveals her data to the Service Provider.

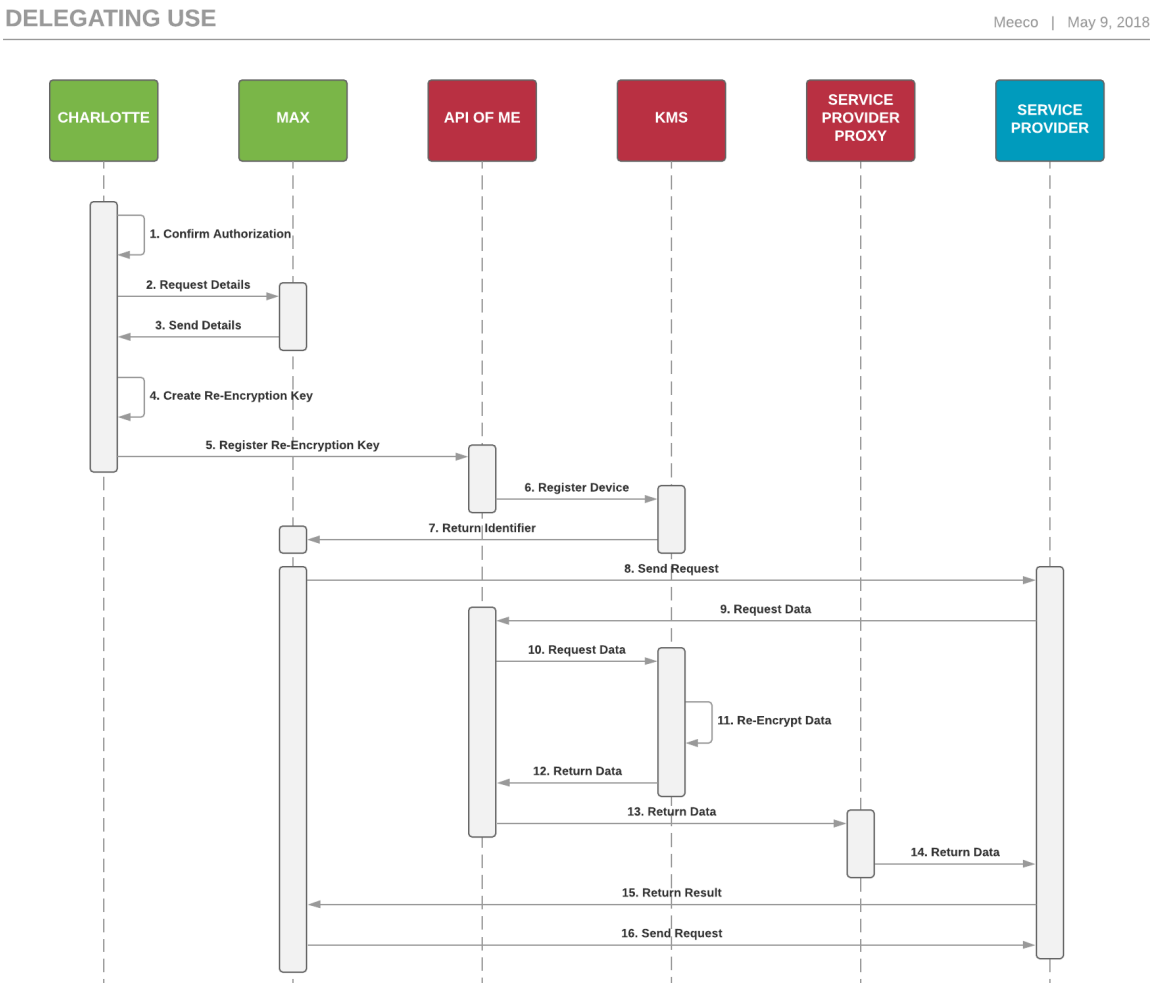


1. After Charlotte selected to transact with the Service Provider, the **public key for the Service Provider** is used to encrypt a payload containing:
    a. The "Tell-Me-More" transaction ID from the **Service Provider's wallet** to **Charlotte's wallet**
    b. A proof that Charlotte owns the wallet associated with the transaction ID
    c. A **public key for Charlotte's device**
    d. **Charlotte's documents** required to transact
2. The request is sent to the API-of-Me.
3. The request is sent to the Service Provider's proxy. The **private key for the Service Provider** is used to decrypt the payload.
4. The Service Provider proxy sends a request to the API-of-Me to verify the result associated with the transaction ID is and to validate the proof of Charlotte's ownership of the address.
5. The verification request is sent to the randomly selected node.
6. The result of the transaction ID is located, and the proof of ownership is validated.
7. The result is returned to the API-of-Me.
8. The result is returned to the Service Provider proxy.
9. The Service Provider proxy sends a request to the Service Provider API with Charlotte's identity documents to execute the transaction.
10. The Service Provider executes the transaction.
11. The result of the transaction is returned to the Service Provider proxy.
12. The result is returned to the API-of-Me and encrypted with the **public key for Charlotte's device.**
13. The results are returned to Charlotte's device.
14. The encrypted payload is decrypted with the **private key for Charlotte's device**. The blockchain transaction details and the response from the Service Provider are stored in Charlotte's data wallet and Event Chain.

2.3.7 Delegated use

In this section, Charlotte delegates access for Max to use her data without storing it on his device. Charlotte can revoke access to her data and has full control over its use, as it is only stored on devices that she has full authority over.

An example use case is where Charlotte wants Max to have access to her insurance policy while she is overseas so that Max is able to file a claim on her behalf. This access is granted with an expiry date in Charlotte's Consent Engine. Encrypted data can be shared between Charlotte and Max without having to decrypt the data by using proxy re-encryption services like NuCypher [19] and Besafe [20].

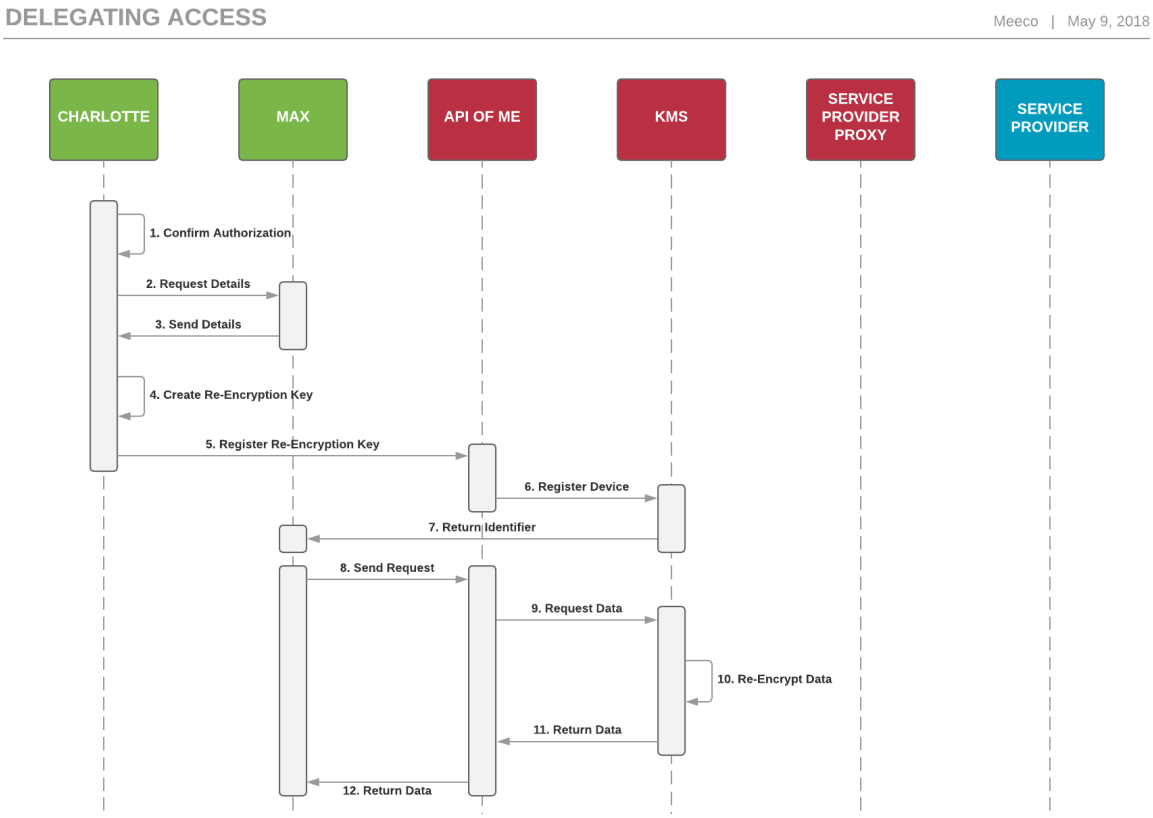


Charlotte initiates a request to delegate authority to Max's device so that he is able to act on her behalf with her insurance Service Provider. The delegation of Authority is written into Charlotte's Event Chain.

1. A request is sent to Max to provide an identifier for his device.
2. The identifier is supplied to Charlotte.
3. A re-encryption key is created from Charlotte's private key and the Service Provider's public key.
4. The re-encryption key is sent with Max's device details to the API-of-Me.
5. The re-encryption key is registered against Max's Meeco account and his device details with the Key Management System.
6. An identifier for interacting with Charlotte's insurance Service Provider is sent to Max so that he is able to initiate a claim. This is stored in Max's event chain.
7. Max initiates a claim through the Service Provider with his approved device.
8. The request data is sent to the API-of-Me.
9. The request is sent to the KMS to validate if Max's device is valid.
10. Charlotte's encrypted data with the insurance Service Provider is re-encrypted for the Service Provider's public key.
11. The re-encrypted data is sent to the API-of-Me.

12. The re-encrypted data is sent to the Service Provider proxy and decrypted with the Service Provider's private key.
13. The data is returned to the Service Provider.
14. The Service Provider returns a response to Max so that he can now transact on Charlotte's behalf.
15. Max begins the transaction on Charlotte's behalf.

2.3.8 Delegated access



In this section, Charlotte wants to allow Max to view and store her data. She is granting Max the right to store a copy of her data. If Charlotte revokes that access in the future it does not delete data on Max's device. An example of this is if Charlotte might want to delegate access for Max to access her medical history.

1. Charlotte initiates a request to delegate authority to Max's device so that he is able to access some of her data. The delegation of Authority is written into Charlotte's Event Chain.
2. A request is sent to Max to provide an identifier for his device and his public key.
3. The identifier and public key are supplied to Charlotte.
4. A re-encryption key is created from Charlotte's private key and Max's public key.
5. The re-encryption key is sent with Max's device details to the API-of-Me.
6. The re-encryption key is registered against Max's Meeco account and his device details with the Key Management System.
7. An identifier for interacting with Charlotte's data is sent to Max. This is written to Max's event chain.

8. Max sends a request to the API-of-Me for access to Charlotte's data from his approved device.
9. The request is sent to the KMS to validate if Max's request is valid.
10. Charlotte's encrypted data is re-encrypted for Max's public key.
11. The re-encrypted data is sent to the API-of-Me.
12. The re-encrypted data is sent to Max's device and decrypted with his private key.

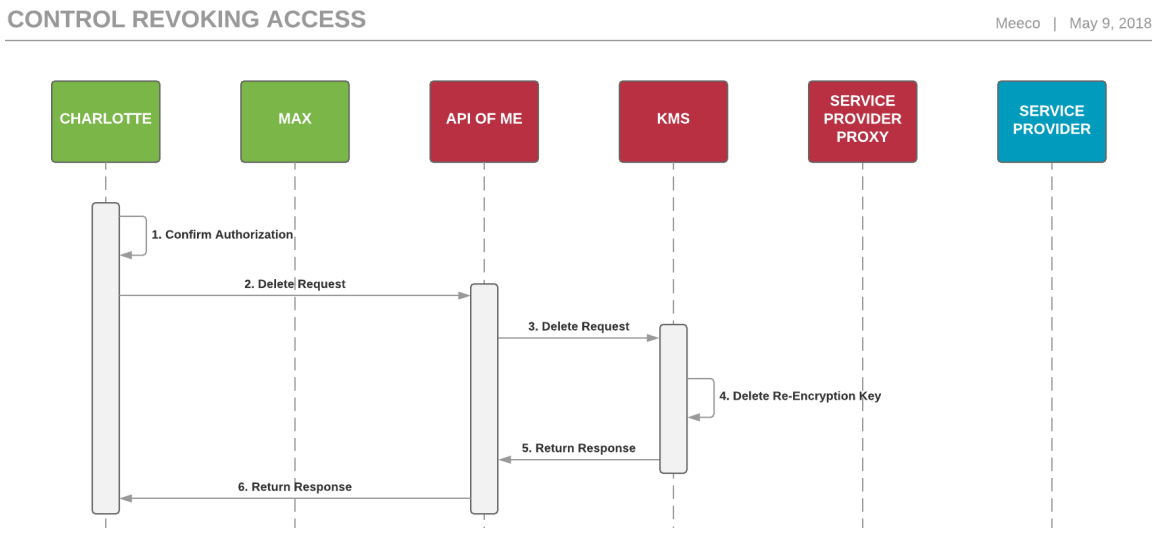
Delegated Access has an extensive range of real-world use-cases that are currently difficult or impossible in a digital form. This includes Power-of-Attorney, Proxy, Child Services, Guardianship (children and elderly family members), Estate Planning and Management.

An area of significant opportunity in Digital Delegation is pre-birth and post-life management. Increasingly the unborn have a digital footprint (pre-birth medical data) and post-life it is difficult to take control of or turn off social accounts.

Delegation Smart Contracts make these phygital (physical-digital) experiences transparent, auditable and actionable.

2.3.9 Control – revoking access

This section demonstrates when Charlotte wants to revoke the access that she had granted to Max. For example, revoking access to a shared utility account after Max moves out.



1. Charlotte selects the user who's access she wants to revoke and confirms the action.
2. A request to delete the re-encryption key is sent to the API-of-Me.
3. The request is sent to Key Management Service.
4. The Key Management Service deletes the re-encryption key.
5. The result of the operation is returned to the API-of-Me.
6. The result is returned to Charlotte's device.

2.3.10 Control – device selection

If Charlotte has multiple devices she may not want to have all of her personas and their data on each device. For example, if Charlotte has an iPad setup to control the music system in her living room she may not want it to have access to her medical data.

When Charlotte's device has new data to store, she is given the option to choose the devices she would like to share it with. This is done with the Key Management System and a re-encryption key for each device.

2.4 Token curated registry and governance

A protocol is agnostic to the purpose of the applications built on top of it. The purpose of a protocol is to create a set of rules for communication, not to enforce how those rules are used.

"*The blockchain has no morals. To it, you are just a key*." – Ryan Shea [21]

Meeco operates at the protocol and application layers in the tech stack. At the application layer, there is a responsibility, where possible, to protect users from fraud, bad business practices, identity theft and scammers.

The output of a Token Curated Registry [22] is a curated list. The governance mechanisms of Meeco create a list of approved Service Providers.

Approved Service Providers can integrate with Meeco and make calls to request data in Charlotte's data wallet. Sites and services that are outside of the Meeco providers network will not be able to send requests to Charlotte's data wallet. Facebook, Twitter, LinkedIn and many others offer self-service integrations, so anyone can create an integration. Meeco requires the regional governance board to approve the request to integrate, as discussed in section 5.1 Provider governance.

This reduces the attack vectors for scammers. Even if Charlotte clicks on a link in an email that takes her to a convincing site and tricks her to logging in with her Meeco credentials, there is no way for the scammers to use the credentials to access her data wallet or provision a new device. This is discussed in more detail in section 2.5.9 Device Initialisation.

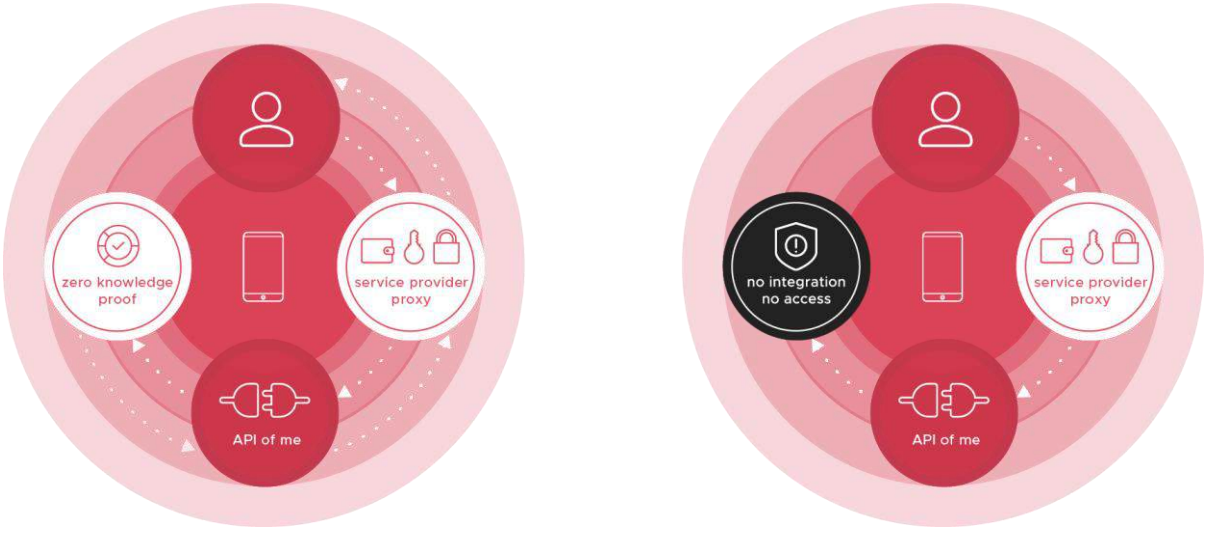


Figure 7: How the provider whitelisting protects people's data

Self-service integrations allow scammers to build integrations so that people can be tricked into consenting to hand over their data.

Meeco requires informed consent.

Not all users are able to evaluate the legitimacy of a request that is being made. Implementing a Token Curated Registry creates certainty, accountability and a way to economically punish bad actors.

Initialisation of the provider whitelisting for a region will be done by Meeco. This is achieved by creating proxies to integrate with Identity Providers and core Service Providers, such as banks, telcos and utility companies (Figure 7).

Meeco has a responsibility to provide users with a safe experience that protects all users from scammers by default and design. **Meeco should not dictate how users can use their data**. If an advanced user chooses to take their data outside of the jurisdictionally approved whitelisted providers, that is their right to do so. Over time, nationless chains that are interoperable with Meeco may emerge. Charlotte may choose to take her data outside of the jurisdictional protection that the whitelists provide, at her own risk. This type of interaction would require Charlotte to confirm that she understands that she is using her data in a way that is not safe guarded by Meeco or her chosen governance body.

Taking Charlotte's data outside of the Token Curated Registry is something that can be disabled by her digital power of attorney. This is discussed further in section 2.5.1 Remote device management policies.

2.4.1 Multi-chain

Each jurisdiction is essentially a chain with its own Token Curated Registry. The benefits of this approach are smaller chains and fast consensus. Each region has its own governance so that it can determine what is appropriate for its people.

Figure 8 shows that there are three different types of chains in the Meeco ecosystem;

1. Public blockchains

2. Meeco private chains and;

3. The personal event chain on the user's device.

Jurisdiction 'A' will have a separate group of Master Nodes, made up of regional Service Providers and Identity Providers for that jurisdiction. If government agencies wish to have representation in the governance process but do not have the capacity to run a node, Meeco will offer this as a service.

Jurisdiction 'B' will have a different group of nodes to Jurisdiction 'A'. The cross-chain bridges require the node to run each of the chains that are required in the interaction.

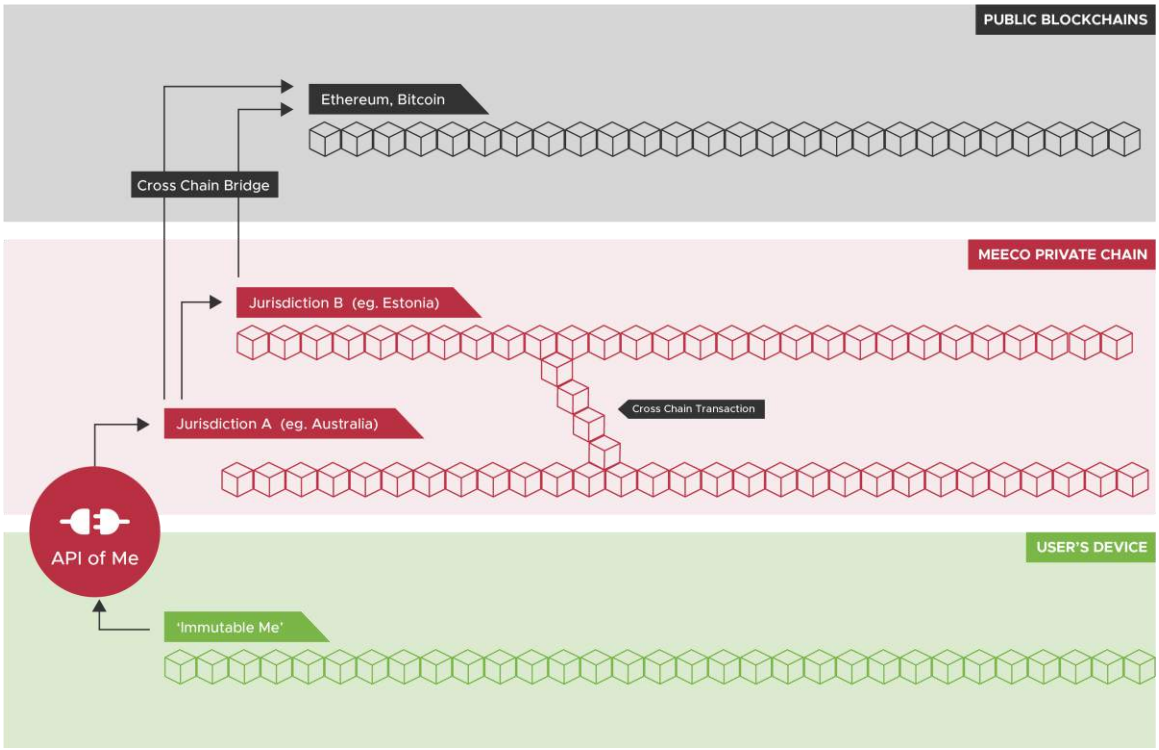


Figure 8: Meeco Chains

Initially, the cross-chain interoperability will be between Meeco jurisdictional chains (e.g. I want to use my Australian Identity claims to open a bank account with an Estonian Service Provider). The Service Providers will be able to specify which identity claims they will accept from different providers in the smart contract.

An Estonian Service Provider might specify that they will accept any government Identity Providers on the Australian chain but will only accept a passport Identity Provider from the Zimbabwe jurisdiction.

Master Nodes are able to submit a proposal to fork a jurisdiction if there are laws that result in an unresolvable conflict. When a fork occurs, the Service Providers and Identity Providers will then have to choose which jurisdiction(s) they will participate in.

2.5 Device management

This section covers what happens when Charlotte has lost access or wants to provision a new device. Not all users will be able to manage their account and may choose to delegate management of their account to a digital Power-of-Attorney.

The requirements to implement data recovery or to lock a data vault remotely without access to Charlotte's device require being able to:

- Prove her identity
- Locate her recovery policies
- Access her encrypted data
- Reconstruct her private key

Charlotte has the ability to enable and customise her recovery and remote lock options, these are captured as digital policies (an example is shown in Figure 10). Digital policies are written to the Distributed Ledger to enable Charlotte to prove her intentions without access to a device.

2.5.1 Remote device management policies

These settings are disabled by default. The scope and type of digital policies will depend on Charlotte's level of digital literacy, existing relationships with Service Providers and the level of trust in friends and family. Identity management is not a one size fits all problem. Meeco provides a series of Token Curated Registries for users with varying levels of protection so that Charlotte can choose the right level of protection for her circumstances.

Meeco retains a plain text record of the parties involved in the issuing, execution or alteration policies so that law enforcement can investigate any claims of illegal activity. This plain text record also allows Meeco to identify unusual behaviour and raise it for investigation with law enforcement.

Due to the potential impact of policy abuse relating to digital power of attorney, transparency is important to protect vulnerable people from being taken advantage of. When an attempt to access a policy is made, it is logged against the device that the request is being made for. This event is recorded into the user's event chain.

Trustees

A trustee is a person who Charlotte entrusts to either store a shard of her secret or to act as a co-signer in her recovery policies.

Power of Attorney Policies

Some users will have a policy to delegate a digital power of attorney. For example, a teenager to their parents, an elderly person to their children, or a young professional might grant joint digital power of attorney to their lawyer and accountant. The ability to delegate responsibility to a trusted party makes self-sovereign identity accessible to those who need a higher degree of protection.

In the event that the trustee is no longer able to fulfil their role as Charlotte's digital power of attorney, she still has full control of her identity and can appoint a new digital power of attorney. To protect Charlotte, changes to her digital power of attorney policies will need to be physically witnessed by a recognised authority, such as a Lawyer or Justice of the peace, to ensure that Charlotte is acting of her own free will.

Self-Enforceable Policies

The policies for remote access allow Charlotte to specify different settings for each Service Provider. The threshold for the number of trustee signatures can be adjusted per Service Provider. An example of the policy list stored on a device is shown in Figure 10. The public keys in Charlotte's policy are pairwise pseudonymous identifiers to protect the identities of trustees.

Charlotte can choose which state-issued credentials the Service Provider can use to verify her identity along with how many people from the Service Provider must co-sign that they have physically verified her identity.

Service provider employee requirements may also be specified (e.g. has been an employee for more than 5 years or that at least one of the Service Provider signatories has signed for a minimum of 20 policy requests).

The default configuration will include local law enforcement and other government Service Providers who have the processes to verify government credentials in person. Charlotte may elect to replace or supplement the list of Service Providers with other organisations that she trusts, like her local church or bank.

A library of verified and audited enforceable policies will be developed by Meeco in conjunction with:

- Privacy Lawyers
- Financial institutions
- Health care providers
- Researchers
- Government Policy
- Telcos
- Third Party Application Providers
- Privacy Specialists
- Security Specialists

This is an extension of Meeco's existing consent engine.

Change Notifications

Charlotte is able to specify change notification settings in Meeco so that when a policy is changed or created, a password is changed, or a remote device action is requested she receives a notification on her devices.

2.5.2 Locating user policies

When Charlotte initiates a remote access request, the smart contract needs to be able to access her recovery settings without access to her device. This means that her settings must be accessible with only access to Charlotte (herself) at an approved Service Provider. An example of a policy for a Service Provider that would be stored on the blockchain is shown in Figure 9. Note that the policy on the blockchain is stored on a per Service Provider basis.

```
{
  "region": "Australia",
  "policies": [
    { // bank
      "allowed_documents": ["drivers_license"],
      "type": "remote_access",
      "scope": ["public_persona"],
      "service_provider": "0x281055afc982d96fab65b3a49cac8b878184cb16",
      "signature_thresholds": {
        "provider": 2,
        "trustee": 3
      },
      "trustees": [
        "0xfe9e8709d3215310075d67e3ed32a380ccf451c8",
        "0xf27daff52c38b2c373ad2b9392652ddf433303c4",
        "0xa380ccf451c8e8709d321fe9d325310075d67e3e",
        "0x522b9392652f27daffddf433303c4c38b2c373ad"
      ]
    }
  ],
  "devices": [
    "0xe53d2c8a3d84357ec70ce511289d6d64134dfac8",
    "0x5310075d67e3ed32a380ccf451c8fe9e8709d321",
    "0xf52c38b2c373ad2b9392652ddf433303c4f27daf"
  ]
}
```

Figure 9: Example policy stored on the blockchain

To prevent identity collisions, the index that points to Charlotte's data is created from Charlotte's full name, date of birth, hospital of birth and the Service Provider's private key.

Attack Vector – Data Export

A malicious actor, Mallory, has access to a Master Node and could attempt to use a dictionary attack with every name, date of birth and hospital to brute force every combination to create a list of Meeco users. This risk is mitigated by:

- The index being a function of the Service Provider's private key
- Service providers only being able to locate Charlotte's policy if she has a policy with the Service Provider

An example of policies for Service Providers as stored on the user's device are shown in Figure 10.


```
{
  "region": "Australia",
  "policies": [
    { // telco
      "type": "anomaly_access",
      "service_provider": "0x47172d896f46cf5569aefa1acc1009290c8e0437",
      "signature_thresholds": {
        "provider": 1,
        "trustee": 2
      },
      "trustees": [
        "0xa380ccf451c8e8709d321fe9d325310075d67e3e",
        "0x522b9392652f27daffddf433303c4c38b2c373ad",
        "0x310075d67e3ed32a380ccf451c8fe9e8709d3215"
      ]
    },
    { // bank
      "allowed_documents": ["drivers_license"],
      "type": "remote_access",
      "service_provider": "0x281055afc982d96fab65b3a49cac8b878184cb16",
      "signature_thresholds": {
        "provider": 2,
        "trustee": 3
      },
      "trustees": [
        "0xfe9e8709d3215310075d67e3ed32a380ccf451c8",
        "0xf27daff52c38b2c373ad2b9392652ddf433303c4",
        "0xa380ccf451c8e8709d321fe9d325310075d67e3e",
        "0x522b9392652f27daffddf433303c4c38b2c373ad"
      ]
    },
    { // local law enforcement
      "allowed_documents": ["passport", "drivers_license"],
      "type": "remote_access",
      "service_provider": "0x6f46cf5569aefa1acc1009290c8e043747172d89",
      "signature_thresholds": {
        "provider": 2,
        "trustee": 2
      },
      "trustees": [
        "0x289d6d64134dfac8e53d2c8a3d84357ec70ce511",
        "0xfe9e8709d3215310075d67e3ed32a380ccf451c8",
        "0x522b9392652f27daffddf433303c4c38b2c373ad"
      ]
    },
    {
      "type": "power_of_attorney",
      "trustees": [
        "0x53d284357ec70ce289d6d64134dfac8e511c8a3d"
      ]
    }
  ],
  "devices": [
    "0xe53d2c8a3d84357ec70ce511289d6d64134dfac8",
    "0x5310075d67e3ed32a380ccf451c8fe9e8709d321",
    "0xf52c38b2c373ad2b9392652ddf433303c4f27daf"
  ]
}
```


Figure 10: Example policies as stored on the user's device. The public keys for the devices, trustees and Service Providers are pairwise pseudonymous identifiers

2.5.3 Data vault lock

Both Android [23] and iPhone [24] have remote wipe options, however, these solutions are not turned on by default. As such, Meeco offers a way to remotely lock a data vault on an inaccessible device that is turned on by default.

Considerations

If Mallory has access to Charlotte's login details, Mallory should not be able to lock Charlotte's device.

If Charlotte leaves her device unlocked, Mallory should not be able to lock Charlotte out of her devices without her login details.

Charlotte should be able to access the benefits of Meeco's remote data vault lock with a single device and not have to rely on her social network of friends and family.

Requirements

If the remote Data Vault lock options are enabled, Charlotte should be able to securely:

- Prove her identity
- Locate her recovery policies
- Execute a lock

These requirements need to be met without relying on Charlotte owning multiple devices. It is necessary to have multiple options with differing proof of identity challenge requirements. The identity challenge when requesting a remote lock should be sufficiently difficult that if Charlotte's Meeco login credentials where compromised, or she had left her device unlocked, a third party could not execute the data vault lock. The options to execute a remote lock in order of difficulty are:

1. One of Charlotte's other known devices
2. A trustee's known device
3. A whitelisted Service Provider, countersigned by a telco verifying unusual activity
4. A whitelisted Service Provider, countersigned by trustees
5. An overseas Service Provider partner, countersigned by trustees

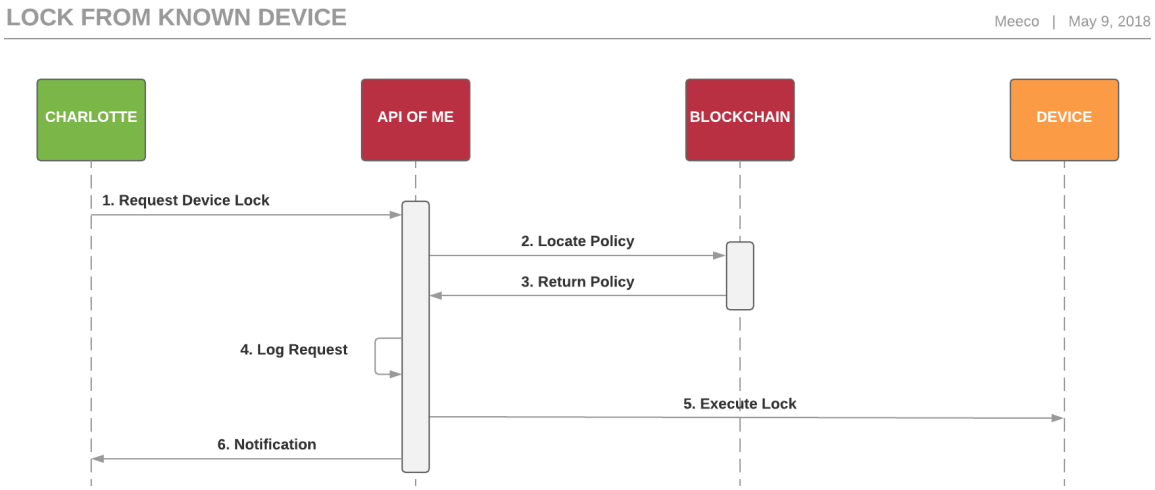
Charlotte should never disclose her Meeco login details. In the event that Charlotte has shared her login details, the responsibility is with Charlotte to update them.

2.5.4 Lock from a known device

Charlotte accesses Meeco through a device that has previously been logged into Meeco and initiates a remote lock on the inaccessible device.

Requirements

- Charlotte must authenticate to confirm her identity
- Charlotte's password must not have changed in the previous 7 days
- Charlotte's known device must have had Meeco installed for a minimum of 7 days



1. Charlotte Authenticates on one of her other devices to initiate a remote device lock.
2. The index to the policy is a function of the private key of the requesting device.
3. The policy is returned to the API-of-Me.
4. The details about the request are logged in plain text.
5. The API-of-Me sends a request to lock the data vault on the device the next time it connects to the API-of-Me.
6. Charlotte's device receives a notification about the outcome of the request.

Attack vector – Shared Password

If Charlotte has shared her login details with Mallory (who has recently become a malicious user) then Mallory will be able to lock Charlotte's device with access to one of Charlotte's other devices.

This is mitigated by:

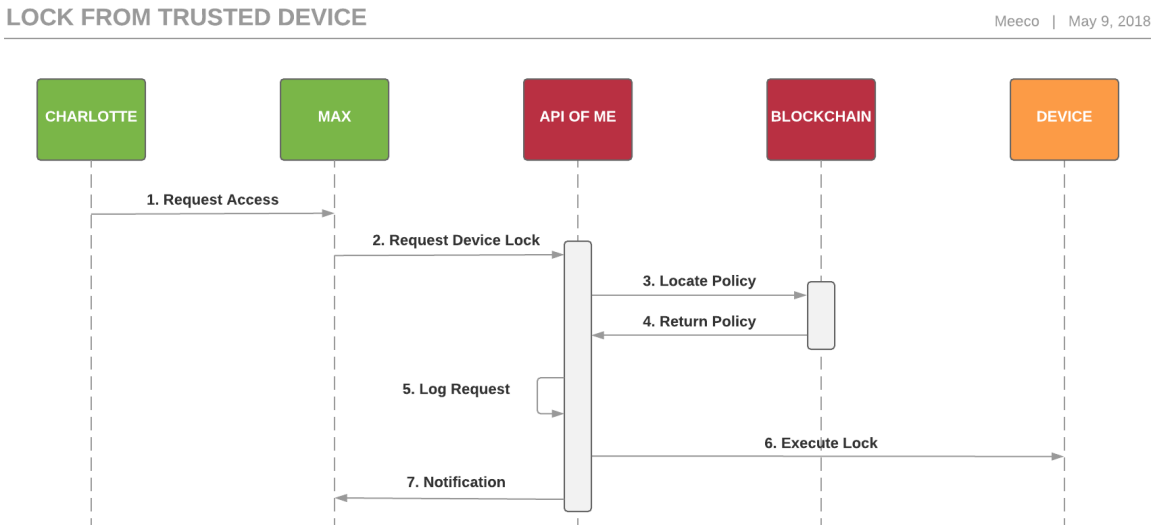
- Charlotte being able to report the device as stolen through the steps in 2.5.7 Service provider lock countersigned by trustees

2.5.5 Lock from a trusted device

Charlotte is able to configure her remote lock settings to include a whitelist of trustees. If Max is in Charlotte's whitelist, then she can initiate a remote lock from Max's device.

Requirements

- Max's device must have had Meeco installed at least 7 days before Charlotte's request
- Max must have been in Charlotte's whitelisted for at least 7 days
- Both Max and Charlotte's passwords must not have changed in the previous 7 days
- Both Max and Charlotte must authenticate on Max's device to send the request.



1. Charlotte requests access to Max's device.
2. Charlotte Authenticates with her Meeco login details on Max's device to initiate a remote device lock.
3. The request includes the index to the policy which is a function of Max's private key.
4. The policy is returned to the API-of-Me.
5. The authority of Max's claim is validated and the details surrounding the request are logged.
6. The API-of-Me sends a request to lock the data vault on the device.
7. Max's device receives a notification about the outcome of the request.

Attack vector – Malicious users

Mallory is a malicious user who is listed as a trustee for Charlotte. If Mallory gains access to Charlotte's Meeco login details, she is able to lock Charlotte's device.

This is mitigated by:

- The request from Mallory's device being logged for fraud detection
- Mallory being known to Charlotte.

Attack vector – Trustee Being compromised

Mallory is a malicious user who has compromised Max's device. If Mallory gains access to Charlotte's Meeco login details she could execute a lock from Max's device on Charlotte.

This is mitigated by:

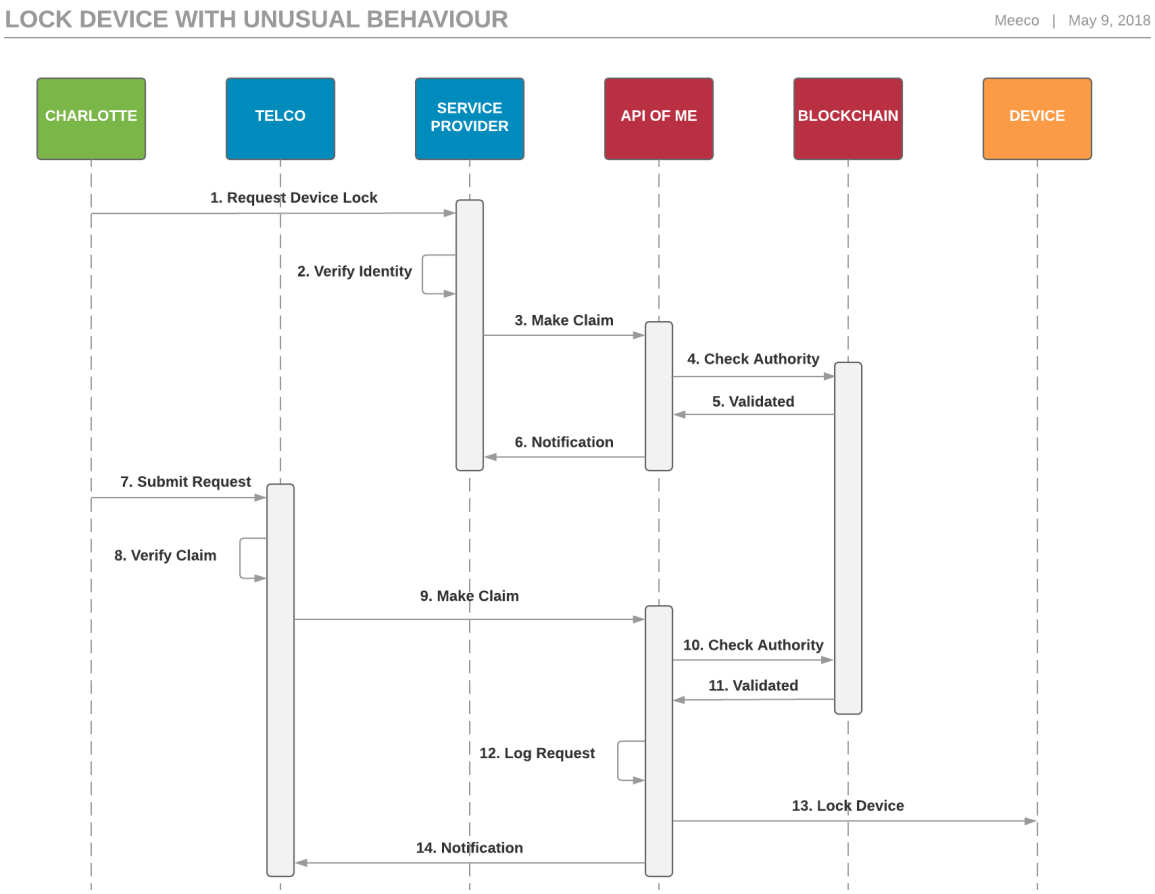
- The request from Max's device being logged for fraud detection
- Mallory would need to know Charlotte's full name, date of birth, hospital of birth and Meeco login details. If she was to try and brute force these values, it would be picked up by the fraud detection systems that analyse the request logs.

2.5.6 Service provider lock countersigned with unusual activity

In the event that Charlotte's device is stolen, her telco may be able to automatically verify (with a high degree of certainty) that Charlotte no longer has control of her device if the cell towers that her device is connecting to are unusual for her behaviour profile.

Requirements

- The Service Provider must have had a policy for Charlotte for at least 7 days
- The telco offers the anomaly verification service
- Charlotte must have authorised the telco to provide anomaly verification
- Charlotte's passwords must not have changed in the previous 7 days
- A whitelisted Service Provider must physically witness Charlotte's identity verification
- Multiple Service Provider employees must sign that they have verified Charlotte's identity.



1. Charlotte requests a device lock from a Service Provider.
2. The Service Provider does a physical identity check against a state issued passport or driver's license.
3. An authorised employee at the Service Provider lodges a request with the API-of-Me to lock Charlotte's data vault on the missing device. Depending on Charlotte's settings, this may require the employee's manager to witness the request.
4. The API-of-Me checks that the Service Provider and the employee have the authority to make the request on behalf of Charlotte by executing a smart contract.
5. The result of the smart contract validating the request is returned to the API-of-Me and the request is opened.
6. A notification is sent to the Service Provider that the claim has been successfully initiated.
7. Charlotte is then able to make a request to her Telco to make a supporting claim that the location data from her device does not match her usual behaviour.
8. The Telco is able to verify Charlotte's claim about unusual behaviour.
9. The Telco then asserts its support of Charlotte's claim.
10. The Telco's authority to act on behalf of Charlotte is verified against Charlotte's remote access policy.
11. The Telco's claims are validated.
12. Writing the outcome of the remote access control request is written to the blockchain.
13. The API-of-Me sends a request to lock the data vault on the device the next time it connects to the API-of-Me.
14. The Telco is then notified of the status of the claim.

Attack Vector - Malicious Service Provider

One of Charlotte's whitelisted Service Providers could attempt to initiate the lock of Charlotte's data vault without her consent. This risk is mitigated by:

- Requiring the initiating Service Provider to sign the request with the employees' identity
- Offering the service that the Service Provider accepts the liability of their employees' actions
- Locating Charlotte's policy requiring personal data and the Service Provider's private key
- Logging the details of who initiated and supported the claim for fraud detection
- Requiring a counter signature from the Telco to corroborate unusual behaviour of the device.

Attack Vector – State Actors

Sam is a state actor that wants to gain access to Charlotte's personal data. Through regulatory pressure, Sam coerces the Service Provider employee, Steve, to lock Charlotte's device. Sam is also able to apply pressure to the Telco to corroborate the claim.

This is mitigated by:

- Logging both Steve's personal details and the Telco's data in Meeco
- Notifying Charlotte through her listed communication channels when the request is made.

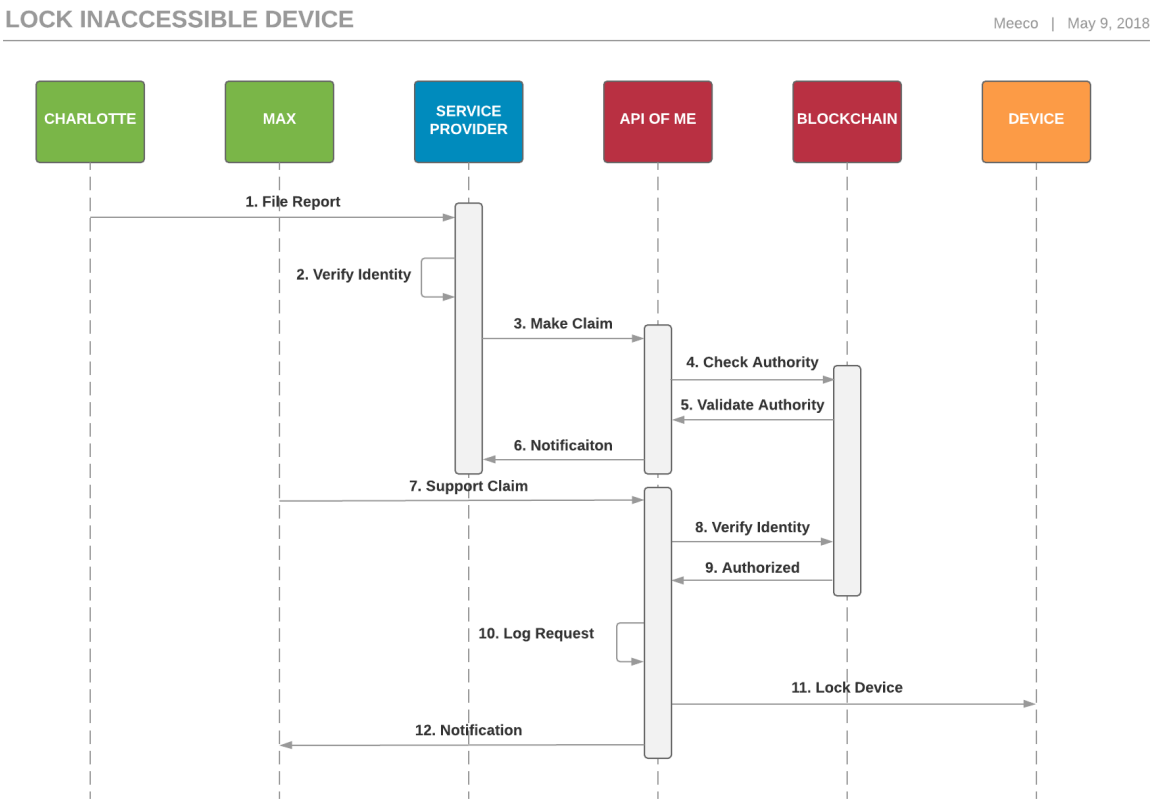
2.5.7 Service provider lock countersigned by trustees

Charlotte has her device stolen and wants to prevent unauthorised access to her data. To lock her identity on the stolen device it is necessary for Charlotte to prove who she is to Steve (who works at one of her authorised Service Providers) and have her claim supported by a whitelisted trustee, Max.

This is limited by the requirement of Charlotte to have a sufficient number of friends and family that she trusts to reduce the risk of attack. The users in Charlotte's whitelist could be narrowed down based on who Charlotte interacts with in the real world.

Requirements

- The Service Provider must have had a policy for Charlotte for at least 7 days
- Max and Charlotte's passwords must not have changed in the previous 7 days
- Max must authenticate to co-sign the request
- Steve must physically witness and verify Charlotte's identity
- Steve and his supervisor must both sign that they have physically verified Charlotte's identity.



1. Charlotte files a police report that her device has been lost, damaged or stolen and takes it to one of her approved Service Providers.
2. The Service Provider does a physical identity check against a state issued passport or driver's license.
3. Steve (an authorised employee) lodges a claim with the API-of-Me that Charlotte's device is inaccessible to her and requests to put a freeze on the device's data vault.
4. The API-of-Me checks that the Steve and the Service Provider have the authority to make the request on behalf of Charlotte by executing a smart contract.
5. The result of the smart contract validating the request is returned to the API-of-Me, and the request is opened.
6. A notification is sent to the Service Provider that the claim has been successfully initiated.
7. Max is then able to make a supporting request to the API-of-Me asserting that he has spoken to Charlotte and that her device is no longer accessible.
8. Max's identity is verified against the list of approved witnesses.
9. The approved authorisation is returned to the API-of-Me.
10. Max's corroboration meets the threshold requirements of Charlotte's witness threshold, so the action is logged with supporting information, such as the police report number, Service Provider, Steve and Max's information. If the request is denied, all of the relevant information will still be logged.
11. The API-of-Me sends a request to lock the data vault on the device.
12. The trustees receive a notification of the status of the claim once it has been successfully countersigned.

Attack Vector - Malicious Service Provider

Mallory is Steve's supervisor at one of Charlotte's whitelisted Service Providers. She could attempt to initiate the lock of Charlotte's data vault without her consent. This risk is mitigated by:

- Requiring Mallory and Steve to both sign the request with their identity
- Requiring the initiator to be able to look up Charlotte's policy by suppling her data
- Logging the details of who initiated and supported the claim for fraud detection
- The trustees are stored as pairwise pseudonymous identifiers
- Requiring a threshold of trustees to corroborate the claim asserted by the Service Provider.

Attack vector – Malicious users

Mallory is a malicious user and has stolen Charlotte's identity. Mallory attempts to initiate a request with the Service Provider's employee, Steve, to remotely lock Charlotte's data vault using forged credentials.

This is mitigated by:

- Requiring Steve to physically check the requestor's state issued credentials
- Requiring Steve to verify Mallory's claim, and assume liability for ensuring that Mallory's credentials are accurate
- Requiring an in-person interaction between Charlotte and Steve to lock Charlotte's data vault, making it more difficult for Mallory to impersonate Charlotte
- Steve being only able to locate Charlotte's policy with her full name and date of birth which must both match her state issued credentials.
- Mallory being able to convince Steve to issue the claim she would still need to identify, locate and convince Max to countersign the fraudulent claim.

Attack Vector – State Actors

Sam is a state actor that wants to gain access to Charlotte's personal data. Through regulatory pressure, Sam coerces the Service Provider employee, Steve, to lock Charlotte's device. Sam is able to identify Max as a probable trustee based on Charlotte's social media footprint to apply pressure to get the request countersigned.

This is mitigated by:

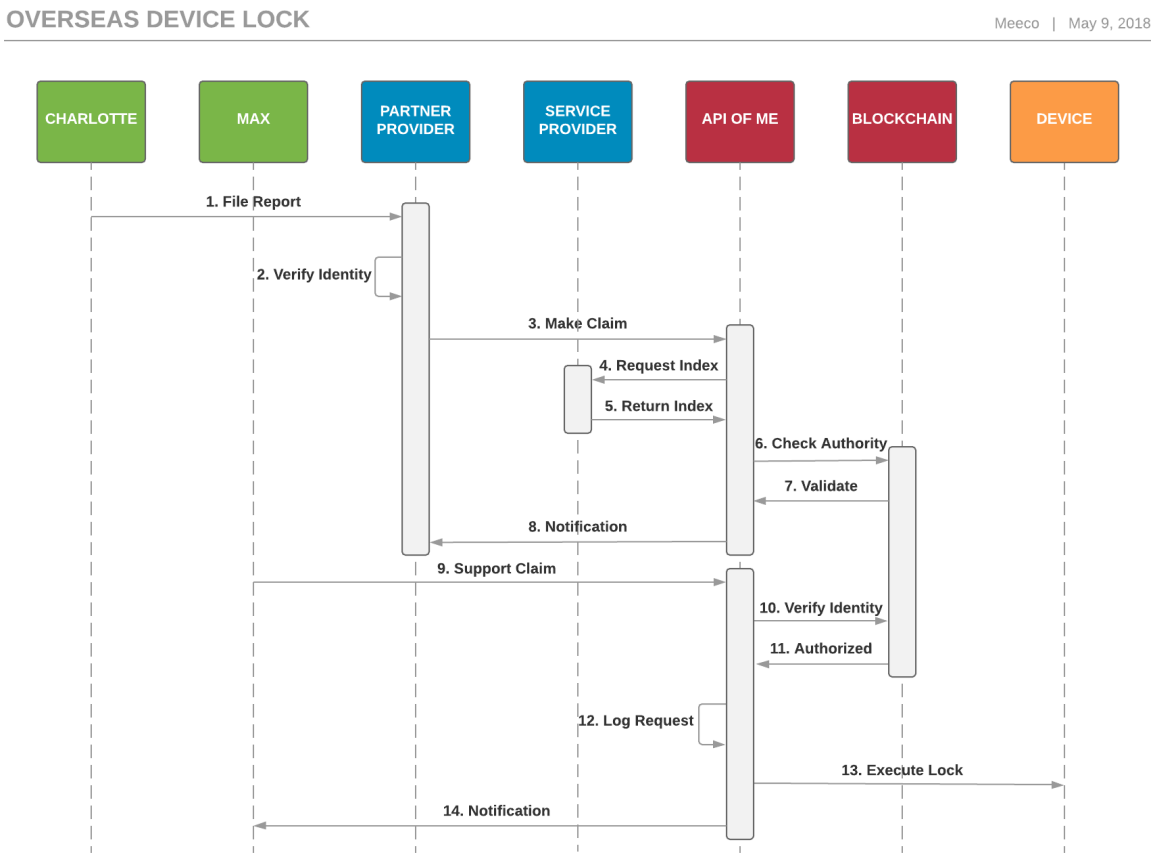
- Logging both Steve and Max's personal details in Meeco
- The whitelist of Charlotte's trustees being pairwise pseudonymous identifiers
- Notifying Charlotte through her listed communication channels when the request is made
- Ensuring the remote lock can't access the contents of the data wallet.

2.5.8 Partner provider lock countersigned by trustees

When Charlotte is traveling overseas, she can enable the network of recovery providers that have partnership agreements with her recovery policy providers. In the same way that you need to notify the bank when travelling overseas, Charlotte needs to enable the overseas recovery network before travelling.

Requirements

- The Service Provider must have had a policy for Charlotte for at least 7 days
- The country that Charlotte is visiting must have Service Providers with partnership agreements with the Service Providers that she has policies with
- The service must be enabled before travelling
- Charlotte's passwords must not have changed in the previous 7 days
- A partnered Service Provider must physically witness Charlotte's identity verification
- Multiple Service Provider employees must sign that they have physically verified Charlotte's identity.



1. Charlotte files a police report that her device has been lost, damaged or stolen and takes it to a Service Provider that has a partnership agreement with one of the Service Providers that she has a recovery policy with.
2. The partner provider does a physical identity check against a state issued passport.

3. An authorised employee at the partner provider lodges a claim with the API-of-me that Charlotte's device is inaccessible to her, and requests that the Service Provider locate and execute her remote lock policy.
4. The Service Provider uses the information provided by the partner provider, along with their private key, to create the index to lookup Charlotte's policy.
5. The index for the policy is returned to the API-of-Me.
6. The API-of-Me checks that the service provide, and the partner provider's employee have the authority to make the request on behalf of Charlotte by executing a smart contract.
7. The result of the smart contract validating the request is returned to the API-of-me and the request is opened.
8. A notification is sent to the Service Provider that the claim has been successfully initiated.
9. Max is then able to make a supporting request to the API-of-me asserting that he has spoken to Charlotte and that her device is no longer accessible.
10. Max's identity is verified against the list of approved trustees.
11. The approved authorisation is returned to the API-of-me.
12. Max's corroboration meets the threshold requirements of Charlotte's witness threshold, so the action is logged with supporting information, such as the police report number, Service Provider, partner provider, partner provider employee and Max's information. If the request is denied, all of the relevant information will still be logged and accessible to the bounty program.
13. The API-of-Me sends a request to lock the data vault on the device.
14. The trustees receive a notification of the status of the claim once it has been successfully counter signed.

2.5.9 Device Initialisation

Initialising a new device with an existing Meeco account requires access to the encrypted data and being able to reconstruct the private key.

2.6 Private key recovery

Private key recovery needs to be simple enough that it is accessible to non-technical users, but safe from attackers. The Hyperledger DKMS architecture document [25] puts forward two approaches: offline recovery and social recovery. There is no way to reset a password in a decentralised key management system.

2.6.1 Social recovery through secret sharing

The basic principle of secret sharing is that the secret can be split into pieces ("shards") that individually cannot be used to determine the secret. Each piece of the secret is then distributed amongst a group of trustees. Reconstructing the secret requires gathering a number of the pieces, greater than the threshold that has been previously established.

A simple example of how secret sharing works is solving the equation for a straight line. The equation for the line can be determined from any two points that are on the line. So, if there are five trustees and each is given a point on the line, the secret can be determined whenever two of the five points are gathered from the trustees.

This is one approach to storing secrets that is being implemented by Keep Network [26] and Enigma [27] through the use of secure multi party computation (sMPC) so that the secret can be used without any party having access to it.

Meeco does the secret reconstruction on a new device. This is done by the trustee's phone displaying a QR code for the secret owner to scan. The trustee's shard is encoded using the GPS coordinates and a Wi-Fi finger print. When the secret owner scans the QR code, the data is then decoded with the GPS coordinates and Wi-Fi finger print of the scanning phone. This ensures that the owner and trustee are in the same physical location.

Attack Vector – Social Engineering

Social engineering is a complex challenge since scams have become more convincing. This is compounded as the value of the contents in the data wallets increase over time, only further incentivising scammers. This risk is mitigated by:

- Requiring the piece of the secret to be collected in person
- Encoding the secret with the GPS location of the device creating the code and decoding it with the GPS location of the device receiving the data (this is still susceptible to social engineering asking for a screenshot and then brute forcing the location)
- The Wi-Fi networks available to the device creating the QR code are used in the encoding of the data as this is not something that an attacker can't brute force.

Attack Vector – Trustee Denial of Service

The trustees could prevent Charlotte from being able to collect enough pieces of her secret for reconstruction. This is mitigated by:

- Allowing Charlotte to set a low threshold for reconstruction
- Giving Service Providers the ability to act as a trustee for customers
- Allowing Charlotte to choose the number of pieces to distribute.

Attack Vector – Trustee Collusion or Coercion

The trustees could collude to steal Charlotte's identity. This is mitigated by:

- The list of trustees who have a piece of Charlotte's key not being recorded anywhere
- Allowing Charlotte to set the threshold
- Having a separate process with additional checks and balances in order to access the encrypted data (this is further outlined in section 2.7 Data initialisation).

2.6.2 Digital power of attorney

The digital power of attorney is achieved through proxy re-encryption across all of Charlotte's data, such that Max is able to initialise a new device for Charlotte with his login credentials.

This type of relationship requires a high degree of trust and will mostly likely occur primarily with family members, for example, a parent managing their child's data.

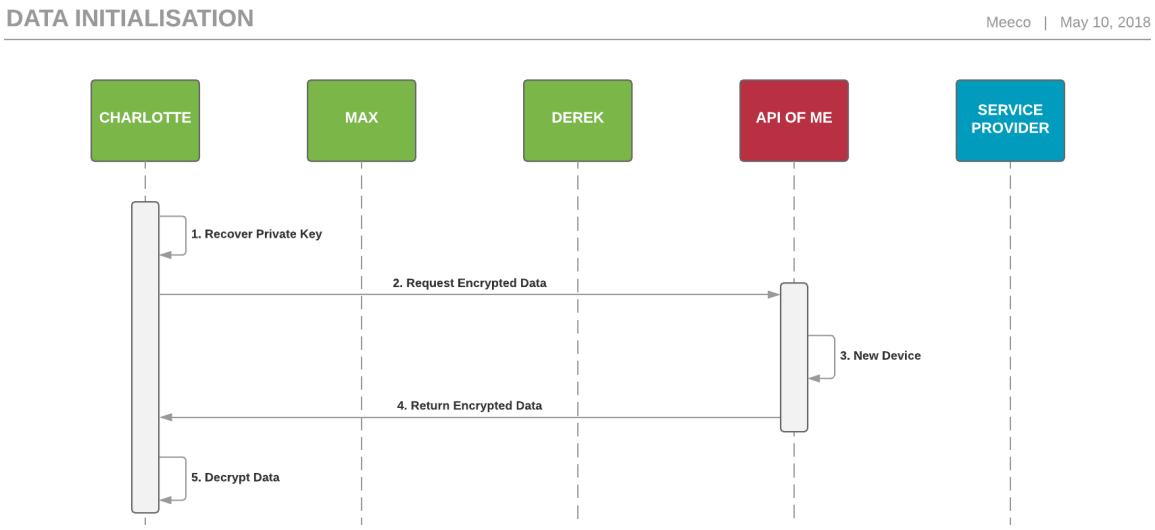
This is a role where the parent may need to give informed consent on their child's behalf.

2.6.3 Offline recovery

The offline recovery option is intended for advanced users who want a recovery option that is completely independent of interacting with other parties. A paper wallet can be used to store a backup of the person's private key. However, this may be difficult for most users to securely manage.

2.7 Data initialisation

To initialise a device requires access to Charlotte's encrypted data and her private key. Charlotte is able to reconstruct her private key with the three methods explained in section 2.6 Private key recovery. If there is no device lock in place, then Charlotte is able to restore the data onto a new device by logging into Meeco once she has reconstructed her private key.



1. Charlotte recovers her private key on her new device.
2. Charlotte sends a request to the API-of-Me, authenticating who she is and requesting her encrypted data.
3. The new device is registered against Charlotte's Meeco account.
4. The encrypted data is returned to Charlotte's new device.
5. The data is decrypted with Charlotte's recovered private key and the data wallet for the device is initialised.

If there is a device lock in place, then Charlotte needs her request to access her encrypted data to be co-signed by a trustee.

3. Comparisons

The concept of a blockchain was introduced by Satoshi Nakamoto (in 2008) to create an immutable, censorship resistant, decentralised currency. It consists of a chain of blocks, where each block contains unchangeable records [28].

This is distinct from distributed ledgers, which are ledgers maintained by a group of peers, rather than a central agency [29].

There are over 1,600 tokens and coins listed on CoinMarketCap at the time of writing.

This section covers two areas; comparing existing data wallet projects (Table 3) and data exchange projects (Table 4) with Meeco and examining the mechanics of successful Master Node projects.

	Meeco	Sovrin	uPort	Trusted Key	Verified.Me	Pillar Project	UniquID	SelfKey	Veres One
Progressive Disclosure	✓	✗	✓	✓	✗	✗	?	✓	✗
Integration with ID provider	✓	✓	?	✓	✓	?	?	In progress	?
Integration with service provider	✓	✓	✗	✓	✓	?	?	In progress	?
Consent Engine	✓	✓	✓	✓	?	?	✗	✓	✗
Personas	✓	✓	✗	?	?	?	?	✗	✗
Granularity of disclosure	✓	✓	✓	✗	?	?	?	✗	?
Token curated registry of service providers	✓	✗	✗	Can be both	?	✗	✗	✓	✓
Supports claims with verified attributes	✓	✓	✓	✓	✓	?	?	✓	✓
iPhone app	✓	✗	✓	✓	In progress	✗	✗	In progress	✗
Android app	✓	✗	In progress	✓	In progress	✗	✗	In progress	✗
Blockchain state	White paper	Pilot	test net	?	In progress	alpha	beta	beta	test net
Blockchain	TBD	Hyperledger	Ethereum	Ethereum	Hyperledger	Ethereum	?	Ethereum	?
Access	Private	Public	Public	Public and Private	Private	Public	Private	Public	Public
Treasury	✓	✗	✗	?	?	✓	?	?	✓
Integrations	✓		Demo App	?	?	?	?	?	?
Account recovery	Secret Shards, Paper Wallet, Digital Power of Attourney	Secret Shards, Paper Wallet	Paper Wallet	Paper Wallet	✗	✗	✗	?	?
Remote data vault lock	✓	✗	✗	✗	✗	✗	✗	✗	✗

✓ yes, feature built and in use
✗ no
In progress white paper stipulates that the feature is in the roadmap
? unclear

Table 3: Data wallet feature comparison

Progressive Disclosure: only the necessary or requested information is disclosed at a given time ('Drive-By', 'Tell-Me-More' and 'Transact' stages).
Consent Engine: users can revoke access to claims made.
Personas: different personas within the app e.g. one for browsing with a pseudonym, one for shopping with real identity.
Granularity of disclosure: users can reveal only one verified attribute at a time e.g. verifies that a user is over 21 years old, rather than revealing their date of birth.
Token Curated Registry of Service Providers: Having a governance mechanism to approve integrations.

	Meeco	Datawallet	DataCoup	Citizen Me	PikcioChain	Datum	Ocean Protocol
iPhone App	✓	✓	✗	✓	✗	✓	✗
Android App	✓	✓	✗	✓	✗	✓	✗
Blockchain	TBD	Ethereum	TBD	?	NEO	BigChainDB	BigChainDB
Data types	Commercial Financial Personal Social	Commercial Financial Social	Commercial Financial Social	Financial Personal Social Survey	Personal	IoT Personal Social	Commercial Financial Healthcare Infrastructure IoT
Data access	Lease	Purchase	Purchase	Purchase	Purchase	Purchase	Purchase

Table 4: Data market places comparison

3.1 Master node tokenomics

"*Blockchains are incentive machines*" [30].

The tokenomics of a project create the economic incentives and market forces for the participants in the ecosystem. The market will optimise for these incentives. Bitcoin was setup to optimise for security by maximising the hash rate, which had the unfortunate consequence of maximising the electricity required to run the network.

Tokens with a high velocity have low incentives to hold them and carry the risk of price volatility. Without an incentive to hold them, even if the utilisation of the network increases, the price will not grow proportionately.

The velocity of a token can be reduced with a buy and burn mechanism (Augur), staking mechanisms (FunFair), burn and mint mechanisms (Factom), gamification that rewards holding (YouNow) and becoming a store of value (Bitcoin) [31].

3.1.1 Token supply

The Master Node projects selected for analysis where chosen based on their market cap. Table 5 shows the application, market cap, price and total supply for each Master Node project.

Name	Utility	Market Cap [32]	Price (0USD) [32]	Supply [32]
NEM[2]	blockchain	$3,444,957,000	$0.38	8,999,999,999
Dash[3]	payments chain	$3,394,545,686	$423.32	8,018,940
Stratis	platform	$549,383,674	$5.56	98,825,299
PIVX[4]	private transactions	$287,308,849	$5.13	56,028,450
ZCoin[5]	private transactions	$181,694,216	$39.79	4,566,650
Blocknet[6]	cross chain bridge	$93,898,948	$18.39	5,105,618
ION[7]	in game tokens	$58,153,942	$2.81	26,628,548
XTRABYTES[8]	blockchain	$33,806,127	$0.08	650,000,000
Crown[9]	currency	$28,383,307	$1.57	18,055,654
Diamond[10]	currency	$21,234,176	$7.74	2,742,229

Table 5: Master Node supply metrics

[2] https://nem.io/
[3] https://www.dash.org
[4] http://www.pivx.org/
[5] https://zcoin.io/
[6] https://www.blocknet.co/
[7] https://ionomy.com/
[8] https://www.xtrabytes.global/
[9] http://crown.tech/
[10] https://bit.diamonds/

3.1.2 Master node requirements

It can be seen from Table 6 that a large portion of the available tokens are locked into the stakes for Master Nodes. This increases the average hold time of the token. The longer the average hold time, the more susceptible the price is to surges when there is growth in the utilisation of the token. Even though there is a large variation in the number of Master Nodes between projects, the percentage of the total supply that have been staked does not have the same level of variation.

Name	Stake	Stake as % of Total Supply	Cost (USD)	Master Nodes	Staked Tokens	Annual Return
Stratis [33]	250,000	0.2529%	$1,457,500	174	44%	-
NEM	3,000,000	0.0333%	1,148,319	566	19%	3.01% [34]
Dash	1,000	0.0125%	$423,316	4,774	60%	6.99%
PIVX	10,000	0.0178%	$51,279	2,084	37%	11.35%
ZCoin	1,000	0.0219%	$39,787	2,718	60%	29.01% [35]
Blocknet	5,000	0.0979%	$91,957	397	39%	18.5%[11]
ION	20,000	0.0965%	$56,110	496	48%	27.69%
XTRABYTES	500,000	0.1163%	$39,309	492	57%	-
Crown	10,000	0.0554%	$15,720	1,078	60%	19.45%
Diamond	10,000	0.3647%	$77,434	130	47%	25.25%

Table 6: Master Nodes staking costs and impact on the token supply, data source is [32] except for Stratis

The minimum number of Master Nodes to remain byzantine fault tolerant depends on the consensus algorithm. Tendermint [36] is byzantine fault tolerant (as long as at least two thirds of the validators are honest). **A minimum of seven validator nodes** has been suggested [37].

3.1.3 Master node distribution

The tokenomics will determine the market forces that influence the distribution of Master Nodes on a geographic basis. Looking at the distribution of Master Nodes for Dash (in Figure 11) and NEM (in Figure 12), it can be seen that Japan, Germany and the United States make up approximately 65% of the Master Nodes in NEM, and the United States, Netherlands, Germany and Lithuania make up 68% of the Master Nodes in Dash.

This has the potential to impact on the types of projects that get funded by the treasury. In the known peers for Stratis, United States, Germany, Netherlands and Czech Republic make up 58% of the nodes [38].

[11] 525,600 new blocks created annually, 70% of the block rewards go to Master Nodes.

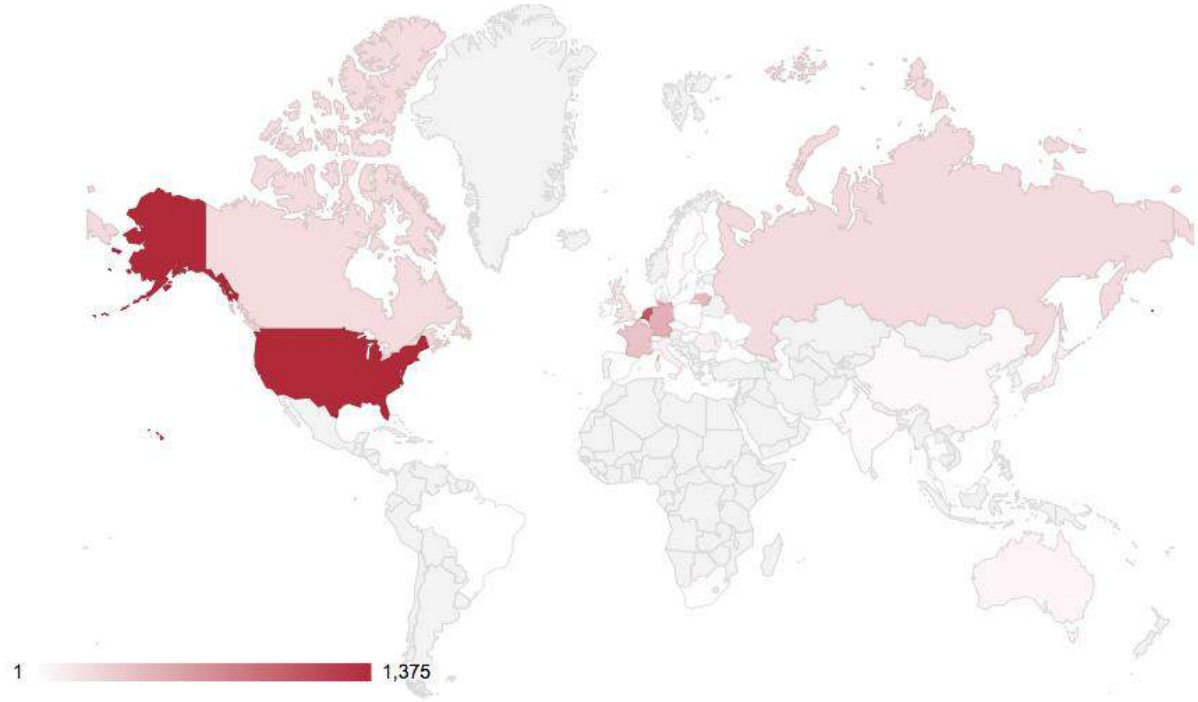


Figure 11: Dash Master Node distribution [39]

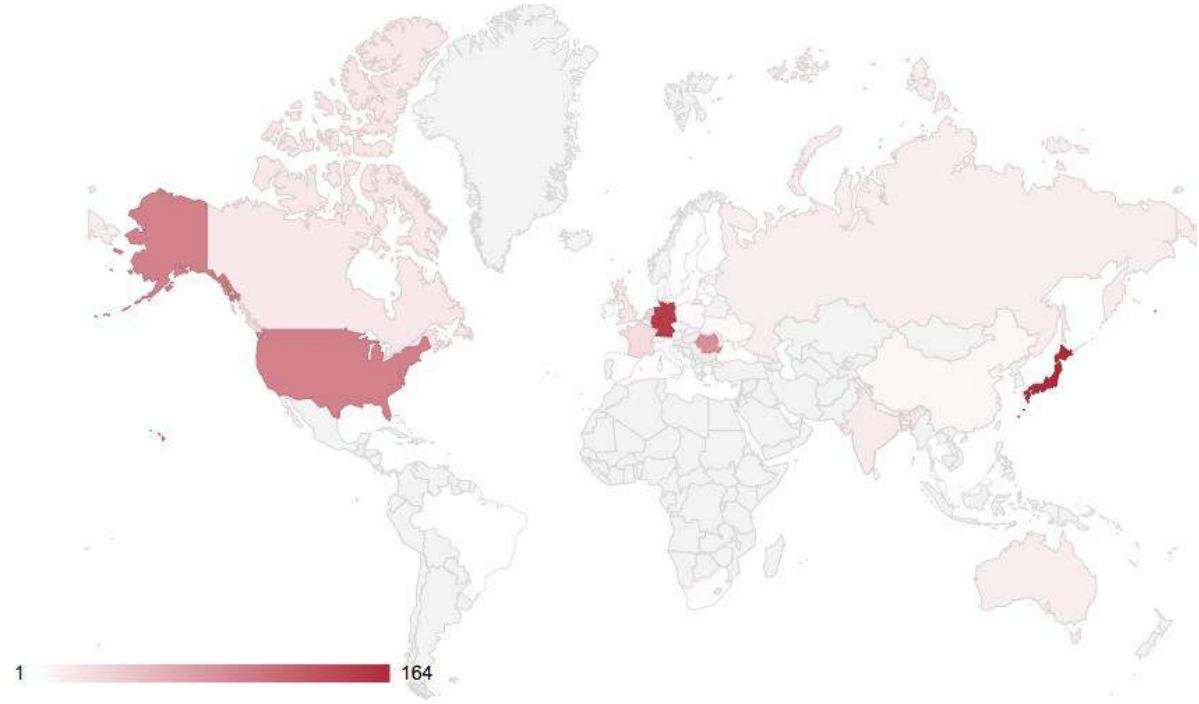


Figure 12: NEM Master Node distribution [40]

3.1.4 Project treasury

Some projects have a Treasury that manages funds for technical and community development. In the case of Dash, PIVX, Blocknet, NEM and Crown, users from the community are able to submit proposals for funding.

Submitting a proposal requires outlining what the funds are for and how the proposal will benefit the community. Proposals are voted on by the Master Node owners (usually a no vote cancels a yes vote). If the proposal gets more than the required threshold, then the project is funded, usually in milestones. Often a pre-proposal submission is made in a public forum and discussed by the community.

To prevent spam and reduce the number of proposals that Master Nodes need to review, there is usually a submission fee (these are shown in Table 7).

To fund the Treasury there are four main mechanisms; allocating tokens during the token generation event, a portion of the transaction fees, a portion of the block reward and periodic minting of new tokens specifically for the Treasury.

Name	Funding	Amount (USD)	Budget Cycle	USD Proposal Fee (Tokens)
NEM [41]	Genesis	$114,831,900 (minted)	On going	NA[12]
Dash [42]	Transaction Fees	$2,614,400 (10% of fees)	Monthly	$2,116.58 (5 DASH)
PIVX [43]	Block Reward	$112,301 (0.5 PIV / min [44])	Monthly	$256.40 (50 PIVX [45])
ZCoin [46]	Block Reward	$522,804 (6% of block reward)	Monthly	-
Blocknet [47]	Minting	$79,450 (4320 BLOCK)	Monthly	$919.57 (50 BLOCK)
ION [48]	Genesis	$7,013,750 (minted)	On going	-
Crown [49]	Transaction Fees	$67,910 (10% of fees)	Monthly	$39.30 (25)

Table 7: Treasury funding

Taking a portion of the mining fees means that the Treasury only gets funding if the network is being utilised whereas taking a portion of the block reward ensures that the treasury continues to be funded regardless of the level of utility.

[12] Initially it was proposed that submissions cost 25,000 NEM [32] which at the time of being proposed would have been approximately $2.50 USD, today that would be $9,500 USD

3.2 Utility token vs security token vs currency

Utility tokens and security tokens convey different types of rights.

A utility token conveys the right to work or the right to access. An example of the right to work are projects like Keep Network and NuCypher, where if the owner has sufficient tokens they can stake their tokens to do work, the tokens have no other utility.

This is like a taxi medallion, in that the medallion on its own has no value, but it can be used to do work to generate income. An example of the right to access are projects like Cindicator [50] (right to access predictions market), Siacoin (right to storage) and Sonm (right to computation).

Security tokens give owners the right to ownership, like BitCar (tokenisation of exotic cars) and Brickx (tokenisation of real estate). One could argue that Bitcoin is a security token as its price volatility and transaction fees make it unsuitable as a currency.

4. Meeco tokenomics

Tokenomics is an emerging field without established best practices. The design of the Meeco economic incentives is included to contribute to the existing body of work. It has been influenced by the works of Vitalik Buterin [51], William Mougayar [52], Mike Sall [53], Fred Krueger [54], Trent McConaghy [55], Jacob Horne [56] and Mike Goldin [57].

Transparency into the tokenomic incentives, costs and benefits from taking part in the different ecosystem activities are provided to analyse the long-term viability of the ecosystem. When there are multiple ways for an economic actor to make money, there is the potential for misaligned interests. As such, it is important to make sure that everyone's economic interests are correctly aligned with growing the utility of the Meeco ecosystem.

A **Data Controller** is an entity that determines the purpose, conditions and means of processing personal data.

A **Data Subject** is a person whose data is processed by a Data Controller or a Data Processor.

A **Data Processor** is an entity that processes data on behalf of a Data Controller.

Table 8 provides a high-level summary of the token design, which is explored in subsequent sections.

Attribute	Mechanism
Assumptions	Inflation of the token supply should be 2% Master Nodes will stake approximately 60% of the token supply
Goals	Incentivise utility Fast transaction speeds
Constraints	Participation as a Master Node requires meeting a threshold stake Permissioned chain with jurisdictional governance
Measurement	Proof of Stake
System agents	Data Controller – Service Provider, Identity Provider, Data Concierge Data Subject – Data Owner Data Processor – Master Node operators Meeco Team Government Master Node backers
System clock	Block reward interval (60s)
Incentives	Block rewards, transaction fees, data lease fees
Disincentives	Challenge protocol and slashing Master Node stakes, application fees

Table 8: Meeco token design attributes and mechanisms

This section outlines how participants could take part in the Meeco economy, how they could be economically incentivised and how Meeco could fund developing the ecosystem after a token generation event.

4.1 Economic actors

The monetary policy and fiscal policy mechanics for the design of a token need to be based on the economic incentives for the different economic actors. A business model canvas has been applied to the Meeco ecosystem in Figure 13 to determine the key elements.

Note that Banks, Telco's, Utility Providers, Data Concierge would all be classified as Service Providers. Government agencies may be Service Providers, Identity Providers or Master Node operators depending on how they are integrated into the ecosystem.

An entity can act as multiple types of Economic Actors. For example, one bank could be a Service Provider, liability provider and a Master Node operator, whereas another bank could just be a Service Provider.

The utility of Meeco's token is broken into six categories based on purpose and role (Table 9).

Role	Features
Right	Approved participants can access voting on jurisdictional governance Approved participants can access voting on treasury proposals To work To be a data concierge and create offers
Value Exchange	Using data to create operational efficiencies Submit treasury proposals
Toll	Running smart contracts Provisioning smart contracts
Function	Incentive to on-boarding and verifying data
Currency	Data concierge rewards
Earning	Treasury funding, mining rewards and participant compensation

Table 9: Token utility

Different participants in the Meeco ecosystem make use of the categories differently. That being the case, it is necessary to design the incentives for each type of the participants separately to make sure that the correct behaviours are rewarded. These are outlined in Table 11. The rights of different economic actors are shown in Table 10.

Economic Actor	Voting Governance	Voting Treasury	Process Transactions	Create Smart Contracts	Create Funding Proposal
Service Provider	✓	×	×	✓	✓
Identity Providers	×	×	×	✓	✓
Master Node Operators	✓	✓	✓	×	✓
Master Node Backers	✓	✓	×	×	✓
Meeco Team	×	×	×	✓	✓
Government	×	×	×	✓	✓
Data Concierge	×	×	×	✓	✓
Data Owner	×	×	×	×	✓

Table 10: Ecosystem rights of different economic actors

Economic Actor	Activities	Tokenomic Incentives	Value Proposition	Participation Costs
Service Provider (Data Controller)	Smart Contract use	-	Risk and Cost Reductions	Transaction fees Creation fee Human capital
Identity Providers (Data Controller)	Liability provider	Transaction fees	Income	Human capital
Master Node Operators (Data Processor)	Governance	-	Increase utility of the network	Human capital
	Smart Contract execution	Transaction fees and block rewards	Income	Server costs Token stake
Master Node Backers	Sales Channel - drive adoption with Service Providers.	Transaction fees	Income	Token stake
Meeco Team	Technology Development (API-of-Me, Treasury submission and voting, distributed ledger, consent engine, data wallet, data vault)	Treasury Funding	Increase utility of the network	Human capital
	Provider support	Treasury Funding	Increase utility of the network	Human capital
	Governance	-	Increase utility of the network	Human capital
	Meeco integrations	Treasury Funding	Increase utility of the network	Human capital
Government	Governance	-	Benefits to citizens	Human capital Token stake
Data Concierge (Data Controller)	Smart Contract use	-	Risk and Cost Reductions	Human capital Transaction fees Creation fee
Data Owner (Data Subject)	Engaging with Service Providers, Identity Providers and Data Concierge	Transaction fees Data lease fees	Convenience[13] Income Risk Reduction[14]	Human capital

Table 11: Economic actor activities and incentives

[13] Meeco increases convenience without compromising on privacy or security by providing personalisation through progressive disclosure.
[14] Meeco reduces the risk of data subjects by increasing security, implementing privacy by design and giving the data subject transparency.

Key Partners

Strategic alliances
Government
Banks
Telcos
Utility Providers

Joint Ventures
Identity Providers

Strategic alliances
Microsoft Azure
Unify Solutions

Coopetition
Veres.one
uPort
Sovrin (Evernym)
Pickcio
Keep Network
NuCypher

Key Activities

Network
Smart Contract Execution

Platform
Governance
Infrastructure

Key Resources

Physical
Master Nodes
Exchanges
API-of-Me

Intellectual
Data Wallet
Data Vault
Consent Engine
Distributed Ledger
Meeco Integrations

Value Proposition

Risk Reduction
Authenticity of documents are verified against transactions with the issuer

Cost Reduction
Verifications are done with a distributed ledger instead of by employees

Convenience
People can get an accurate offer without having to interact with a customer representative

Income
Some economic actors are able to generate income

Customer Relationships

Community
Online forums for providers

Personal Assistance
Meeco support

Channels

Sales Team
Meeco Team

Web
Dapps

Backers
Master Node Backers

Customer Segments

Banks
Telcos
Utility Providers
Data Concierges
Data Owners
Governments

Cost Structure

Fixed Costs
R&D
Platform Management
Provider Support

Revenue Streams

Usage Fees
Network Transaction Fees
Smart Contract Creation

Leasing Data
Data Owner Incentives

Subscription Fees
Block Rewards

Figure 13: Business model canvas applied to the Meeco ecosystem

4.2 Monetary policy

The monetary policy is concerned with managing the total monetary supply in circulation. An initial supply is minted for initialising the network, and then inflation of the supply occurs on an ongoing basis through block rewards. Table 12 shows Meeco minting allocation and lockups.

Minting Allocations	Release (Years)	Allocation
Industrial Stakers (Master Node operators and backers)	1-2	60%
Partnerships	7	7%
Marketing	7	7%
Treasury	5	10%
Meeco	5	3%
Team and Advisors*	2-5	13%
Total		100%

* Advisors and nominated key executives will be entitled to a 2-year release period

Table 12: Minting allocation and lockups

The Master Node operators and backers have different release schedules and bonuses, bonuses are not part of the circulating supply until the lockup period has passed.

4.2.1 Block reward

The reward for executing transactions and creating a block is one (1) new which is created every 60 seconds. The tokens are sub divisible to 18 decimal places. The distribution of the block rewards for the different lockup periods is shown in Table 13.

Lockup	3 months	6 months	12 months
Master Node Operator	30%	50%	70%
Treasury	70%	50%	30%

Table 13: Block Reward distribution

The purpose of the block reward is to compensate Master Node operators for their costs associated with running the infrastructure. Master Node backers are incentivised through the transaction fees, not the block reward.

The number of tokens introduced into the total supply through the block reward is determined by the number of jurisdictions, the size of the block reward decreases as the number of jurisdictions increases.

4.2.2 Total supply

The total supply of tokens that will be minted in the genesis block is 50,000,000. The supply of tokens will continue to increase as new block rewards are generated.

4.2.3 Circulating supply

Based on the Minting allocations and lock up periods, the available supply is shown in Table 14. Tokens held by the treasury may have a long hold time between collection and allocation through the budget cycle.

Year from Launch	1	2	3	4	5	6	7
Industrial Stakers (Master Node operators and backers)	26,250,000	3,750,000	-	-	-	-	-
Partnerships	500,000	500,000	500,000	500,000	500,000	500,000	500,000
Marketing	500,000	500,000	500,000	500,000	500,000	500,000	500,000
Treasury	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	-	-
Meeco (Commercial Entity)	300,000	300,000	300,000	300,000	300,000	-	-
Team and Advisors	1,300,000	1,300,000	1,300,000	1,300,000	1,300,000	-	-
Mining	910,366	1,051,200	1,287,452	1,486,621	1,662,093	1,820,732	1,966,615

Table 14: Token supply release schedule

From the genesis block, 5,000,000 tokens will be allocated to the Treasury. Meeco will bootstrap each jurisdiction by staking 7 nodes. Based on the review of projects in 3.1.3 Master node distribution, Meeco is designing assuming that 60% of the available tokens will be staked against Master Nodes.

The partnerships, marketing and treasury allocations are managed by the Treasury. The partnerships budget is administered by Meeco (and overseen by a governance board) and can be used to help setup new jurisdictions so that the required staking tokens do not have to be acquired on market.

The marketing allocation is administered by Meeco and can be used for incentivising people in new jurisdictions to participate in the ecosystem to experience the benefits first hand. The Treasury fund is administered by the Master Node owners through an online voting system to fund proposals that will help to develop the ecosystem.

The allocation to Meeco (the commercial entity, Advisors and Team) is to fund the on-going costs associated with building out the technology platform. This will be continually replenished from the income generated from Meeco running Master Nodes.

4.3 Fiscal policy

The fiscal policy determines how revenues are collected and spent to develop the Meeco ecosystem.

4.3.1 Demand and supply drivers

The minimum number of Master Nodes to process transactions for a jurisdiction is being set at seven (7). In the event that Master Node owners decide to shut down their Master Node at the end of their staking period, Meeco will run a Master Node to maintain the minimum threshold.

Customer Segments initially will include banks, telco and utility providers who have high costs associated with providing KYC and AML compliance, together with the significant business expense of on-boarding and new service set-up. This will diversify over time as more of the use cases outlined in Section 1.3 User stories, are implemented.

Additionally, post enforcement of regulatory changes for the collection and processing of personal data, new services and business models will emerge to meet the requirements of more data-educated customers. In the foreseeable future, it will be hard to imagine a time when people gave up their data without consent or reward.

The Key Partners that will initially create the utility in the network are the Service Providers and Identity Providers. The value proposition for the providers are centred around reducing the cost of doing business and increasing the level of certainty in the authenticity of documents being used for business processes. This will form the basis from which to build and develop new services.

Staking Costs, Lockup, Block Rewards and delegated staking

To allow more entities to participate in the benefits of staking a Master Node, approved backers are able to lock up a stake against an existing Master Node that they have nominated to participate in the network as a delegate on their behalf. If the Master Node has their stake slashed by the challenge protocol, this creates an additional layer of trust by creating an economic incentive for backers to keep the operators honest. Stakes can be slashed for failing the challenge protocol, or from Meeco users sacrificing their own tokens to down vote a governance actor who they believe is not acting in the best interests of the network.

Having backers as an actor in the system has a benefit to the ecosystem by creating economic incentives for substantial token holders to lobby their local Service Providers and Identity Providers to join the Meeco network which increases the overall utility of the network.

The minimum staking period is 3 months, and the incentive for staking is shown in Table 12. The compensation received for doing work is a function of the stakes lockup time, in order to incentivise token holders (who are backing the operation of the network) to commit to a longer-term stake.

The addition of a Master Node into the network requires approval (as outlined in section 5.1.1 Adding a master node). The addition of more nodes introduces additional computation resources required to reach consensus. Being a permissioned distributed ledger tied to real world providers adds an additional level of trust into the network.

Delegated Staking Approximations

Number of jurisdictions	50
Nodes per jurisdictions	10
Maximum nodes	500
Maximum backers per node	15
Maximum backers	7,500

Based on existing Master Node projects, the target amount of the token supply to be locked up by staking is 60%. Using the theoretical maximum number of backers where the network was operating at full capacity in every country, this makes the staking cost 0.008% of the total token supply at the token generation event.

The maximum stake that a Master Node could support is 0.12% of the total token supply at genesis (which is similar to the other projects examined in Table 5).

Transaction Fees

The distribution of the transaction fees between the Master Node operator, backers, treasury, bounty programs, the data owner in the transaction and the insurer are distributed based on the lockup time of the node's stake, as shown in Table 15. Unlike the block reward, the party wearing the cost of the liability is rewarded from the transaction fees.

Lockup	3 months	6 months	12 months
Master Node Operator	30%	35%	40%
Backers (up to 15)	30%	35%	40%
Insurer	5%	5%	5%
Treasury	29%	19%	9%
Bounty	1%	1%	1%
Data Owner	5%	5%	5%

Table 15: Transaction fees and lockup incentives

This creates an economic incentive for Identity Providers to participate in the ecosystem.

Costs need to vary per jurisdiction based on the local purchasing power, functionality and liability differences. Given that KYC in Australia can cost up to approximately AUD$150 per person and in India it cost approximately $3 USD [58], it must also be considered that a can of Coke in Australia in 2015 cost $0.94, whereas in India it cost $0.48 [59]. Figure 14 shows this globally.

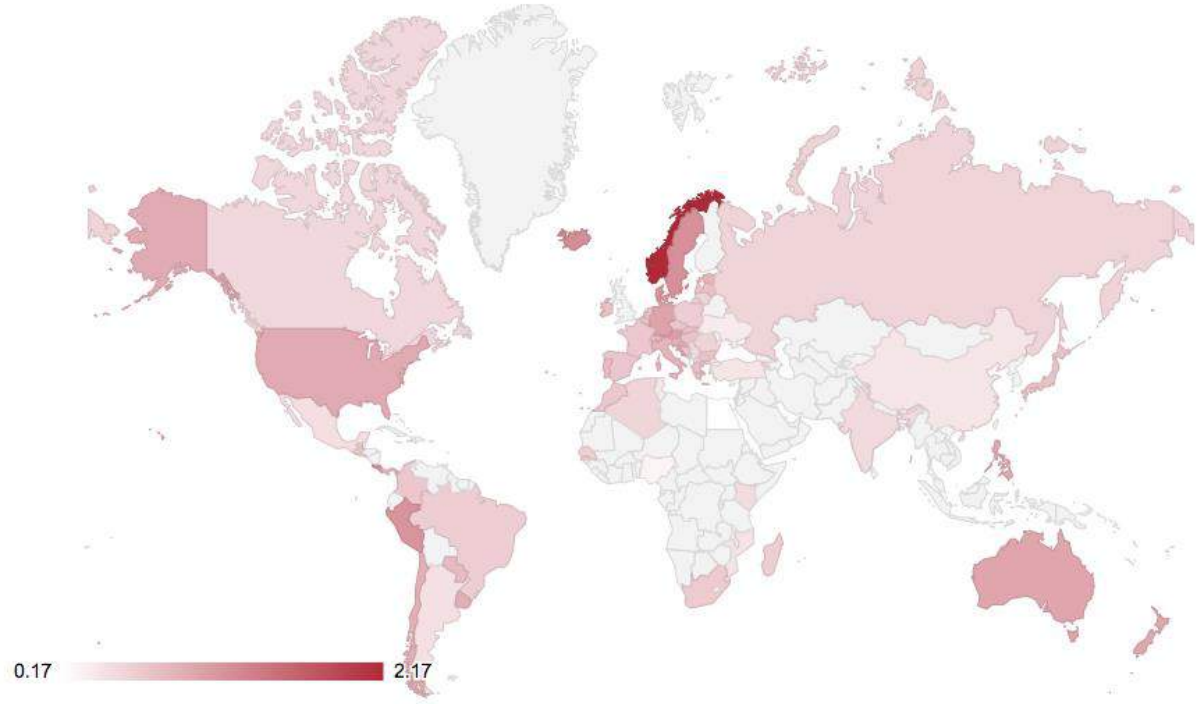


Figure 14: Purchasing power parity per capita [60]

Smart Contract Execution and Creation

The value of the network to its participants is driven by the density of utility in real world applications. The adoption by Service Providers will be fuelled by the use of Meeco's distributed ledger reducing the cost of existing business practises. Having a volatile fiat (fiduciary money) price of execution reduces the utility for existing business practises by introducing uncertainty in the cost of the utility. This makes it appealing to fix the cost of a smart contracts execution to a fiat value.

To allow Service Providers to budget for the use of the Meeco blockchain without having to continuously purchase tokens, **Service Providers can pre-pay for the utility of their smart contract.** This allows Service Providers to bulk-purchase the tokens required for their budget cycle in fiat. This helps to reduce the timing risk associated with trading crypto currencies, this is discussed below.

The fiat cost to execute the functionality is priced to the cost of the utility in poorer countries. The functionality in the KYC performed by banks in Australia is around $150 whereas in India it is closer to $3 [58]. To create an economic incentive for Service Providers to adopt Meeco's Distributed Ledger in its target countries, the utility will be priced to be 15x cheaper than the cost in Australia.

RISK Vector – Price Volatility

To discuss the risks and attack vectors we will assume there is a Meeco Token, e.g. XME.

A Service Provider wishing to purchase $10,000 USD worth of functionality 2,000 XME at a hypothetical $5 USD (0.01 ETH) a token, would first have to transfer fiat onto an exchange and convert it into ETH. If ETH is $500 USD, the Service Provider will now have 20 ETH.

For simplicity, assume there is no ETH transaction fee or USD to ETH conversion fee. The Service Provider would then need to transfer the ETH to an exchange that has a ETH/MXE pair. If by the time the transaction arrives on the exchange the cost of a XME token is now $10 USD (0.02 ETH) the Service Provider can now only afford 1,000 MXE this exceeds the Service Provider's budget.

This is mitigated by:

- The Meeco treasury offering a service for Service Providers to directly pre-pay the tokens for a spot price in fiat. This will be subject to Meeco attaining the appropriate licenses to be compliant with money transmitter laws.

Attack Vector – Price Manipulation

Having a fixed price in fiat creates an economic incentive for providers to batch their transactions, and to manipulate the price of the network up before executing them to reduce the amount of XME that the transaction costs. For example, if a bank introduces the use of Meeco's Distributed Ledger into their loan applications and the cost of execution is pegged at a hypothetical USD$5 for one application, and one XME token costs $2, the bank has 1,000 applications to process which will cost them $5,000 or 2,500 XME. The bank schedules all of their transactions to take place at 9am. At 8:58 am, the bank manipulates the value of XME to $100 so that the transaction will now only cost 50 XME then dumping the tokens they purchased to return to the original $2. This type of attack is costly to implement as the depth of the market on exchanges increases.

This is mitigated by:

- Allowing providers to pre-pay the utility in their smart contract, so if a bank expects to do 1,000 KYC checks that month they can buy the tokens in fiat and load the utility into the smart contract. This allows the Service Providers to control their costs in fiat.

4.4 Token engineering analysis

It should be noted that **this section is not a forecast**. It is an exploration of the different variables that will affect the demand for tokens and how they relate to the overall token supply.

The countries used in the analysis and why they were chosen, is outlined in Section 6. Distribution and bootstrapping the network.

To model the transactions for the network, the KYC use case is examined due to its high costs. KYC events also occur when changing telcos and utility providers. This could be applied to on boarding for sharing economy services like Airbnb or on demand services like Uber and TaskRabbit.

Outside of KYC there are other applications listed in section 1.3 User stories that are not considered in modelling out the utility value of the network. The KYC for banks has been chosen for modelling as it has a clear cost basis to model the utility value of the network.

Assumptions

The average customer undergoes approximately three KYC events with a bank between the ages 26 – 42. To reduce the variables in the model and to take a conservative approach, only these KYC events with the bank are examined.

Many people have accounts with multiple banks so the average number of customers for big banks, banks and credit unions are modelled separated in Table 16.

				Entities			Customers			KYC Events per entity		
Country	KYC Cost (USD)	Population	Target Age	Big Banks	Banks	Credit Unions	Big Banks	Banks	Credit Unions	Big Banks	Banks	Credit Unions
Australia	$ 112.50	24,130,000	25%	4	35	74	10,000,000	500,000	54,000	441,176	22,059	2,382
Estonia	$ 77.50 [61]	1,300,000	25%	0	15 [62]	22 [63]	-	80,000	308	-	3,529	14
UK	$ 70.00 [64]	65,640,000	25%	5 [65]	155 [66]	390 [67]	24,000,000	1,360,133	2,667	1,058,824	60,006	118
France	$ 75.00	66,900,000	25%	12	98	206	27,724,824 [68]	1,386,242	149,715	1,223,154	61,158	6,605
Belgium	$ 75.00	11,350,000	25%	2	17	35	4,703,689	235,185	25,400	207,516	10,376	1,121
Netherlands	$ 75.00	17,020,000	25%	3	25	53	7,053,461	352,674	38,089	311,182	15,559	1,680
Luxembourg	$ 75.00	582,000	25%	1	1	2	241,194	12,060	1,303	10,641	532	57
Germany	$ 75.00	82,670,000	25%	14	120	254	34,260,257	1,713,013	185,006	1,511,482	75,574	8,162
Spain	$ 75.00	46,560,000	25%	8	68	143	19,295,483	964,775	104,196	851,271	42,564	4,597
Canada	$ 75.00	36,290,000	25%	7	53	112	15,039,371	751,969	81,213	663,502	33,175	3,583

Table 16: Modelling assumptions for banking. [65, 67, 62, 66, 64, 68]

The number of transactions in the network can be determined by applying different scenarios for the uptake of each type of entity in each jurisdiction. While the uptake will be different to what is shown in Table 17, each column serves as a different scenario of adoption which shows the impact on the supply of tokens, benefit to the network and value of the overall network's utility.

Adoption is assumed to be slower in the first two years because of the longer lead time of enterprise sales. It is anticipated that the adoption rate will increase as the benefits of the utility of the network are able to be demonstrated though early use-cases. It is also worth noting that countries like Australia are facing regulatory change by July 2019, that will enable customers access rights to their data, therefore there are market forces that will be driving the need for solutions.

Year		1	2	3	4	5	6	7
Australia	Big Banks	0	0	1	1	2	2	4
	Banks	1	5	10	15	20	25	35
	Credit Union	1	11	21	32	42	53	74
Estonia	Big Banks	0	0	0	0	0	0	0
	Banks	1	2	4	6	8	10	15
	Credit Union	1	3	6	9	12	15	22
UK	Big Banks	0	1	2	3	3	4	5
	Banks	0	2	10	45	89	111	155
	Credit Union	0	10	50	168	223	279	390
France	Big Banks	1	2	4	5	7	8	12
	Banks	0	4	10	20	56	70	98
	Credit Union	0	3	20	60	100	148	206
Belgium	Big Banks	0	1	1	1	2	2	2
	Banks	0	3	5	8	10	13	17
	Credit Union	1	5	10	15	20	25	35
Netherlands	Big Banks	0	1	1	2	2	3	3
	Banks	0	2	4	11	15	18	25
	Credit Union	0	3	8	20	31	38	53
Luxembourg	Big Banks	0	0	1	1	1	1	1
	Banks	0	0	1	1	1	1	1
	Credit Union	0	0	1	1	2	2	2
Germany	Big Banks	0	0	1	3	5	10	14
	Banks	0	0	3	15	45	86	120
	Credit Union	0	0	14	25	60	120	254
Spain	Big Banks	0	1	2	3	5	6	8
	Banks	0	2	6	18	39	49	68
	Credit Union	0	3	16	36	72	103	143
Canada	Big Banks	0	0	1	2	3	5	7
	Banks	0	0	1	6	16	38	53
	Credit Union	0	0	3	12	30	70	112
Total		**6**	**64**	**217**	**544**	**921**	**1,315**	**1,934**

Table 17: Example uptake

With an example uptake and transaction volume for each type of entity in each jurisdiction, estimates for the transaction load on the network can be modelled.

Year		1	2	3	4	5	6	7
Australia	Big Banks	-	-	441,176	441,176	882,353	882,353	1,764,706
	Banks	22,059	110,294	220,588	330,882	441,176	551,471	772,059
	Credit Union	2,382	26,206	50,029	76,235	100,059	126,265	176,294
Estonia	Big Banks	-	-	-	-	-	-	-
	Banks	3,529	7,059	14,118	21,176	28,235	35,294	52,941
	Credit Union	14	41	81	122	163	204	299
UK	Big Banks	-	1,058,824	2,117,647	3,176,471	3,176,471	4,235,294	5,294,118
	Banks	-	120,012	600,059	2,700,264	5,340,522	6,660,651	9,300,909
	Credit Union	-	1,176	5,882	19,765	26,235	32,824	45,882
France	Big Banks	-	2,446,308	4,892,616	6,115,770	8,562,078	9,785,232	14,677,848
	Banks	-	244,631	611,577	1,223,155	3,424,833	4,281,041	5,993,458
	Credit Union	-	19,815	132,101	396,304	660,507	977,551	1,360,645
Belgium	Big Banks	-	207,516	207,516	207,516	415,031	415,031	415,031
	Banks	-	31,127	51,879	83,006	103,758	134,886	176,389
	Credit Union	-	5,603	11,206	16,809	22,412	28,015	39,221
Netherlands	Big Banks	-	311,182	311,182	622,364	622,364	933,546	933,546
	Banks	-	31,118	62,237	171,151	233,387	280,065	388,979
	Credit Union	-	5,041	13,443	33,608	52,092	63,855	89,061
Luxembourg	Big Banks	-	-	10,641	10,641	10,641	10,641	10,641
	Banks	-	-	532	532	532	532	532
	Credit Union	-	-	57	57	115	115	115
Germany	Big Banks	-	-	1,511,482	4,534,446	7,557,410	15,114,819	21,160,747
	Banks	-	-	226,722	1,133,612	3,400,835	6,499,373	9,068,892
	Credit Union	-	-	114,268	204,051	489,722	979,444	2,073,155
Spain	Big Banks	-	851,271	1,702,543	2,553,814	4,256,357	5,107,628	6,810,170
	Banks	-	85,127	255,382	766,145	1,659,981	2,085,617	2,894,325
	Credit Union	-	13,791	73,550	165,488	330,976	473,479	657,354
Canada	Big Banks	-	-	663,502	1,327,003	1,990,505	3,317,508	4,644,512
	Banks	-	-	33,175	199,051	530,802	1,260,654	1,758,280
	Credit Union	-	-	10,749	42,995	107,488	250,805	401,288
Total		**27,984**	**5,576,142**	**14,345,942**	**26,573,609**	**44,427,039**	**64,524,191**	**90,961,398**

Table 18: Transactions based on Table 17 and Table 16

Based on the cost of KYC in each jurisdiction, the value in the utility of the network can be modelled as shown in Table 19. This can be sanity checked against the average cost for a financial firm to meet their KYC obligations as being $60 million [69], using the number of big bank and banks that gives an approximate KYC cost around $35B. This is in the right ballpark for the network's estimated utility value shown at year 10 in Table 19.

Year		1	2	3	4	5	6	7
Australia	Big Banks	$ -	$ -	$ 49,632,353	$ 49,632,353	$ 99,264,706	$ 99,264,706	$ 198,529,412
	Banks	$ 2,481,618	$ 12,408,088	$ 24,816,176	$ 37,224,265	$ 49,632,353	$ 62,040,441	$ 86,856,618
	Credit Union	$ 268,015	$ 2,948,162	$ 5,628,309	$ 8,576,471	$ 11,256,618	$ 14,204,779	$ 19,833,088
Estonia	Big Banks	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Banks	$ 273,529	$ 547,059	$ 1,094,118	$ 1,641,176	$ 2,188,235	$ 2,735,294	$ 4,102,941
	Credit Union	$ 1,052	$ 3,156	$ 6,313	$ 9,469	$ 12,626	$ 15,782	$ 23,147
UK	Big Banks	$ -	$ 74,117,647	$ 148,235,294	$ 222,352,941	$ 222,352,941	$ 296,470,588	$ 370,588,235
	Banks	$ -	$ 8,400,821	$ 42,004,107	$ 189,018,483	$ 373,836,555	$ 466,245,592	$ 651,063,664
	Credit Union	$ -	$ 82,353	$ 411,765	$ 1,383,529	$ 1,836,471	$ 2,297,647	$ 3,211,765
France	Big Banks	$ -	$ 183,473,100	$ 366,946,200	$ 458,682,750	$ 642,155,850	$ 733,892,400	$ 1,100,838,600
	Banks	$ -	$ 18,347,321	$ 45,868,301	$ 91,736,603	$ 256,862,488	$ 321,078,110	$ 449,509,354
	Credit Union	$ -	$ 1,486,142	$ 9,907,610	$ 29,722,831	$ 49,538,051	$ 73,316,316	$ 102,048,386
Belgium	Big Banks	$ -	$ 15,563,677	$ 15,563,677	$ 15,563,677	$ 31,127,354	$ 31,127,354	$ 31,127,354
	Banks	$ -	$ 2,334,557	$ 3,890,928	$ 6,225,485	$ 7,781,857	$ 10,116,414	$ 13,229,156
	Credit Union	$ -	$ 420,221	$ 840,441	$ 1,260,662	$ 1,680,882	$ 2,101,103	$ 2,941,544
Netherlands	Big Banks	$ -	$ 23,338,658	$ 23,338,658	$ 46,677,315	$ 46,677,315	$ 70,015,973	$ 70,015,973
	Banks	$ -	$ 2,333,872	$ 4,667,744	$ 12,836,296	$ 17,504,040	$ 21,004,849	$ 29,173,401
	Credit Union	$ -	$ 378,089	$ 1,008,238	$ 2,520,596	$ 3,906,923	$ 4,789,132	$ 6,679,578
Luxembourg	Big Banks	$ -	$ -	$ 798,068	$ 798,068	$ 798,068	$ 798,068	$ 798,068
	Banks	$ -	$ -	$ 39,904	$ 39,904	$ 39,904	$ 39,904	$ 39,904
	Credit Union	$ -	$ -	$ 4,311	$ 4,311	$ 8,623	$ 8,623	$ 8,623

Germany	Big Banks	$ -	$ -	$ 113,361,144	$ 340,083,433	$ 566,805,722	$ 1,133,611,445	$ 1,587,056,023
	Banks	$ -	$ -	$ 17,004,173	$ 85,020,866	$ 255,062,597	$ 487,452,964	$ 680,166,926
	Credit Union	$ -	$ -	$ 8,570,131	$ 15,303,805	$ 36,729,132	$ 73,458,265	$ 155,486,660
Spain	Big Banks	$ -	$ 63,845,348	$ 127,690,696	$ 191,536,044	$ 319,226,741	$ 383,072,089	$ 510,762,785
	Banks	$ -	$ 6,384,540	$ 19,153,621	$ 57,460,864	$ 124,498,539	$ 156,421,241	$ 217,074,375
	Credit Union	$ -	$ 1,034,299	$ 5,516,259	$ 12,411,582	$ 24,823,165	$ 35,510,916	$ 49,301,563
Canada	Big Banks	$ -	$ -	$ 49,762,625	$ 99,525,249	$ 149,287,874	$ 248,813,123	$ 348,338,372
	Banks	$ -	$ -	$ 2,488,133	$ 14,928,796	$ 39,810,124	$ 94,549,043	$ 131,871,034
	Credit Union	$ -	$ -	$ 806,158	$ 3,224,634	$ 8,061,585	$ 18,810,364	$ 30,096,582
Total		$ 3,024,214	$ 417,447,110	$ 1,089,055,458	$ 1,995,402,462	$ 3,342,767,340	$ 4,843,262,525	$ 6,850,773,135

Table 19: Estimated value of the network utility based on Table 18 and Table 16

With a valuation for the network's utility and the circulating token supply, an approximate token price can be estimated (Table 20). This gives an approximate model for how the utility value of the network translates to different market caps.

Year	1	2	3	4	5	6	7
Circulating Supply	30,760,366	39,161,566	44,049,018	49,135,639	54,397,732	57,218,464	60,185,079
Transactions	27,984	5,576,142	14,345,942	26,573,609	44,427,039	64,524,191	90,961,398
Utility Value	$ 8.11	$ 5.61	$ 5.69	$ 5.63	$ 5.64	$ 5.63	$ 5.65
Money Supply	15,010,366	18,161,566	17,799,018	17,635,639	17,647,732	15,218,464	7,685,079
Tokens / Transaction	536.388	3.257	1.241	0.664	0.397	0.236	0.084
Token Value	$ 0.02	$ 1.72	$ 4.59	$ 8.49	$ 14.21	$ 23.87	$ 66.86

Table 20: Price extrapolation

With an approximate token value, it is possible to get an indication of the Master Node returns and staking costs (Table 21). The primary source of income from staking a Master Node is from the transaction fees. This creates the right economic incentive for Master Node backers to champion the adoption of Meeco in their jurisdiction.

Year	1	2	3	4	5	6	7
Public Master Nodes	60	80	100	120	140	160	200
Jurisdictions	3	4	6	8	10	12	14
Master Nodes / Jurisdiction	20	20	16.7	15	14	13.3	14.3
Average Backers / Master Node	7	7	7	7	7	7	7
Total Backers	420	560	700	840	980	1,120	1,400
Staked Tokens	15,750,000	21,000,000	26,250,000	31,500,000	36,750,000	42,000,000	52,500,000
Staked Token Supply	51%	54%	60%	64%	68%	73%	87%
Backing Cost	$ 567	$ 64,646	$ 172,086	$ 318,223	$ 532,733	$ 895,076	$ 2,507,170
Master Node Block Reward	$ 33	$ 3,236	$ 8,440	$ 15,018	$ 24,094	$ 38,802	$ 93,917
Master Node and Backer	$ 378	$ 39,136	$ 81,679	$ 124,713	$ 179,077	$ 227,028	$ 256,904
Market Cap	$ 464,808	$ 67,510,213	$ 202,139,623	$ 416,962,670	$ 772,786,105	$ 1,365,729,368	$ 4,023,845,935

Table 21: Master Node extrapolations

4.5 Treasury

The treasury proposal submission and voting process is modelled on Dash [42], where a proposal is first discussed in a community forum and then a formal application is submitted for approval by the Master Nodes and their backers.

Submission Limits	Fee	Funding Limit
Individual	$250	$10,000
Group	$1,500	$30,000
Corporation	$10,000	$200,000
Government	$50,000	$1,000,000

Table 22: Treasury fees and proposal funding limits

Year	1	2	3	4	5	6	7
Master Nodes Block Reward	$ 13,756	$ 1,812,153	$ 5,908,078	$ 12,615,397	$ 23,612,059	$ 43,458,470	$ 131,483,690
Master Nodes and Backer	$ 181,453	$ 25,046,827	$ 65,343,327	$ 119,724,148	$ 200,566,040	$ 290,595,752	$ 411,046,388
Insurer	$ 11,341	$ 1,565,427	$ 4,083,958	$ 7,482,759	$ 12,535,378	$ 18,162,234	$ 25,690,399
Treasury	$ 20,413	$ 2,817,768	$ 7,351,124	$ 13,468,967	$ 22,563,680	$ 32,692,022	$ 46,242,719
Bounty	$ 2,268	$ 313,085	$ 816,792	$ 1,496,552	$ 2,507,076	$ 3,632,447	$ 5,138,080
Data Owner	$ 11,341	$ 1,565,427	$ 4,083,958	$ 7,482,759	$ 12,535,378	$ 18,162,234	$ 25,690,399

Table 23: Transaction fees

If the application is for funding to cover the staking costs for Service Provider or Identity Provider in a new jurisdiction the funding can be staked such that if the provider stops running the Master Node the funds will be automatically returned to the treasury. The submission costs are shown in Table 22 and are fixed in flat to ensure that the process of making a submission remains accessible if the tokens significantly increase in value.

A framework for preparing the information required for submissions will be put forward so that the community has clear set of guidelines when applying.

4.5.1 Identity providers

Ultimately, the Identity Providers accept liability in making use of identity through the blockchain with a Service Provider. As such the Identity Providers should participate the economic rewards

4.5.2 Law enforcement

In the current banking system, banks accept the liability for funds being stolen by reimbursing users and then pursuing the hackers. This creates security for customers to bank online and take part in online shopping.

A similar mechanism is required to act as an enforcer for digital identity. The person doing the money laundering from the MtGox theft was caught by a group of volunteers [70]. The Treasury will create bounties to fund this type of activity.

Bounties will be paid for collaboration with law enforcement agencies in assistance with tracking identity hackers. The release of funds will be voted on by Master Node operators for the local jurisdiction in which the prosecution occurs.

It is important to note that a distributed honeypot of data is still a honeypot. It just means that botnets are required to search for and extract the data. Whitelisting providers as outlined in section 2.4 Token curated registry and governance helps to mitigate this risk.

5. Governance

There are four types of governance in the Meeco ecosystem.

1. **Provider Level** – approving the addition of new providers into the network, approving requests to transfer the ownership of proxies to providers

2. **Meeco Technology** (Funds Governance) – data standards and blockchain protocol decisions including funding allocation

3. **Meeco Treasury** – For example, funds management from a possible Initial Coin Offering and approving the proposals for allocating funds in the Meeco Treasury

4. **Meeco Commercial Entity** - business model.

Service Providers and Identity Providers have the option to stake a node with voting rights. A set of guiding principles for the economic actors who have voting rights for the approval and rejection of proposals will be outlined (similar to Sovrin's founding steward agreement [71]).

Guiding principles will be specified for treasury funds and actions relating to the utility of the network. All proposal votes will be publically auditable to ensure that appropriate checks and balances are in place to ensure that those empowered with governance responsibilities can be audited by anyone.

Transparency ensures that people using Meeco can hold voters accountable. To create a financial disincentive for bad actors, people using Meeco are able to down vote actions taken by those with voting rights. A Meeco user can slash a portion of the voter's stake at a cost to themselves. This creates an economic disincentive for the Meeco user to down vote without cause.

5.1 Provider governance

Each jurisdiction can run its own chain and govern which Service Providers are allowed into the Meeco regional network. This ensures that the governance for Service Providers selection is deemed appropriate for a region and is not controlled by overseas interests.

Therefore, each region can make culturally appropriate choices. For example, in the US, online gambling is not allowed [72]. The US region nodes would vote 'no' on allowing sportsbet.com into the network. Conversely, in Australia, online gambling is allowed [73], so the Australian regional nodes would vote 'yes' to allowing sportsbet.com into the network.

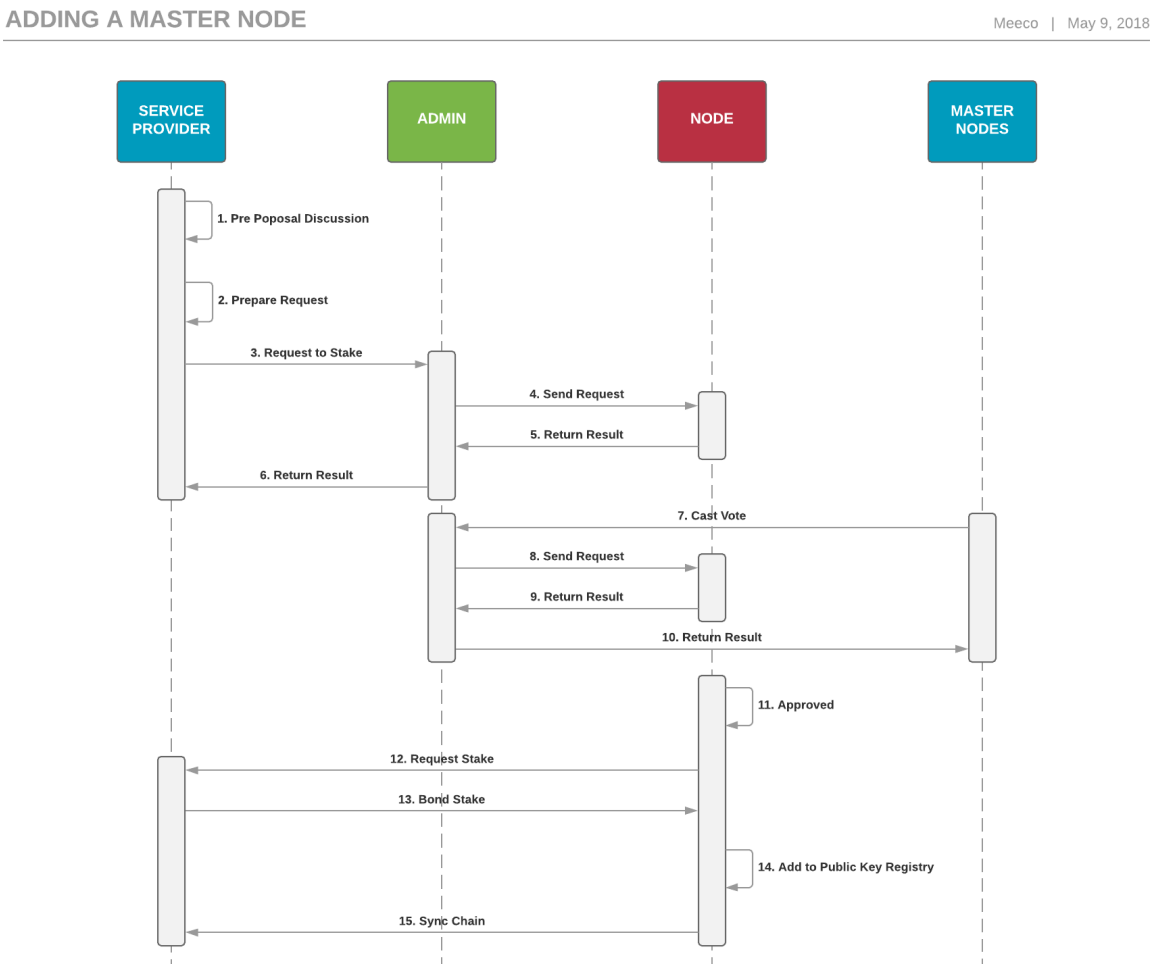
As each region runs the same blockchain it makes it easy to build a cross chain bridge for interoperability between regions. Charlotte can use her Australia verified attributes with the Estonian Meeco chain if the two regions have an agreement in place.

5.1.1 Adding a master node

A proposal would be submitted with an application fee. The proposal would then be available for discussion for a period through the admin interface, during which the node operators would vote to approve, deny or abstain on the application.

If successful, then the proposal operators would make a section transaction to stake their node. A challenge protocol is used to randomly check if the nodes are behaving correctly. In the case where a node misbehaves, their stake is progressively slashed, eventually resulting in the node automatically being removed from the network.

A similar process takes place for integrating with Service Providers and Identity Providers. The regional chain votes to approve or deny their addition to the network. To remove a Service Provider from the network would require either the entity to voluntarily opt to be removed, or legal proceedings in the jurisdiction to show a violation of the TOS.



1. A pre-proposal discussion occurs in a public forum.
2. The Service Provider prepares the request to become a Master Node.
3. The request is sent to through an admin interface.
4. The request to become a Master Node is submitted to a smart contract.
5. The transaction id is returned to the admin interface.
6. The Service Provider is notified about the state of their application.
7. Master Nodes then vote on the Service Provider's application.
8. The vote is written to the distributed ledger with the Master Nodes identity.
9. The result receipt from the vote being written is returned to the admin interface.
10. The Master Node's is then notified that their vote was successfully recorded.
11. Service Provider's application reaches enough votes to be approved.
12. A request for the Master Node stake is sent to the Service Provider.
13. The Service Provider transfers the stake.
14. The public key for the new Node is added into the Public Key Registry. A wallet is created for the Service Provider and the public key for that wallet is registered against the Service Provider.
15. The Service Provider Master Node syncs from the network.

Initially, to bootstrap the network, Meeco will be running the Master Nodes and voting on which Service Providers to add.

Attack Vector – Protectionism

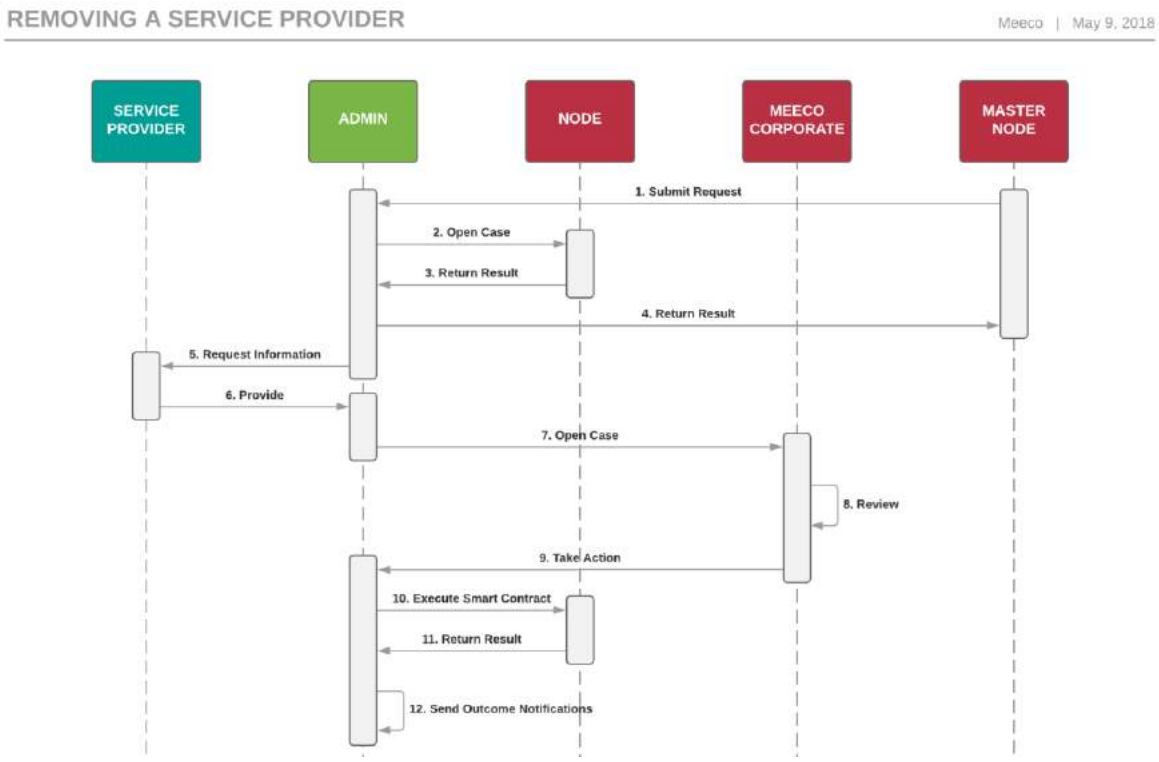
Existing Master Nodes may choose to vote against the best interests of the network by voting to exclude their competitors. This is mitigated by:

- Giving Meeco users a way to financially hold Master Nodes accountable
- Having public discussion before the proposal is submitted.

5.1.2 Removing a service provider

Removing a Service Provider from the network does not necessarily mean removing the node from the network. This action requires either the Service Provider to execute a smart contract to voluntarily remove themselves from the network, or a legal ruling. The Legal ruling is required to prevent large entities, like banks, from forcing out smaller entities, like credit unions. In the case of a law changing to preclude a Service Provider from operating in the network, the liability for the legal bill would fall to the local level of government. Should a Service Provider breach the terms of service, liability would then fall on the network.

A regional Master Node can submit to a governance contract (with the supporting information) to remove a Service Provider. The Meeco commercial entity will then countersign the claim on the contract to approve its execution to ensure compliance with local laws.



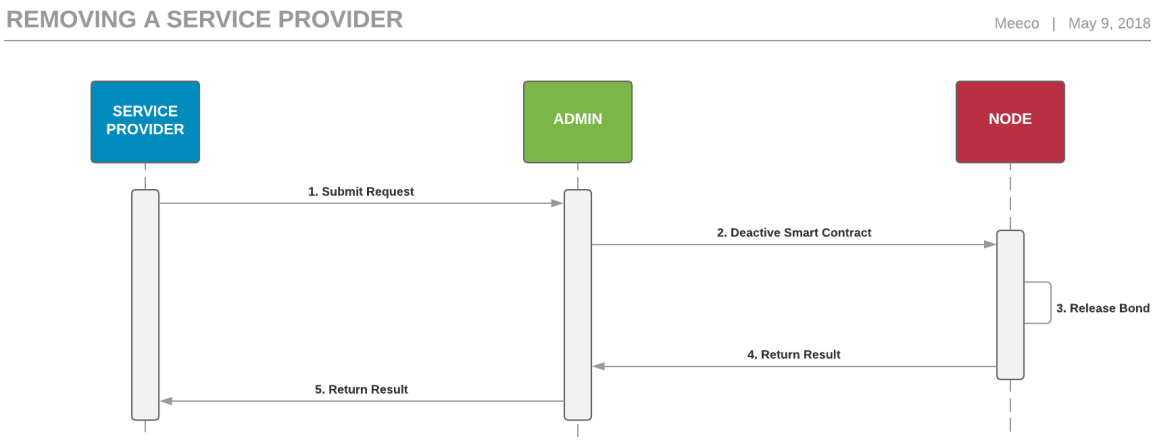
This should be an infrequent and high friction event.

1. A Master Node submits a request through the admin interface to remove a Service Provider with the supporting legal ruling that the Service Provider is no longer able to operate in a jurisdiction.
2. A governance contract is called with the supporting information.
3. The result of executing the smart contract made accessible through the admin interface for all Master Nodes.

4. The result of executing the smart contract is returned to the Master Node that submitted the claim.
5. A request for any additional information is sent to the Service Provider.
6. The Service Provider has a window of time to provide any supporting information.
7. After the Service Provider has supplied additional information, or the time window has elapsed, the case is opened for Meeco the corporate entity to review.
8. Meeco reviews the information that has been supplied and either countersigns the claim that was opened by the Master Node to remove the Service Provider or rejects the claim.
9. The result of the investigation is submitted through the admin interface.
10. The result is sent to the governance contract.
11. The result of executing the governance contract is returned to the admin interface.
12. All of the Master Nodes and the Service Provider are notified of the outcome.

If a Provider no longer wishes to run a Master Node, they can remove themselves from the network by simply removing their staked tokens from the bonded wallet address after their lock up period has passed.

A Service Provider can remove themselves from the network through the admin interface.



1. The Service Provider submits a request to deactivate their integration.
2. A deactivation call is made to their smart contract, the transaction is made from the Service Provider's wallet.
3. The Service Provider's bond is released.
4. The result is returned to the admin interface and is visible to all of the Master Node operators, backers, Identity Providers and other Service Providers in the network.

The Service Provider is notified once the process is complete.

5.2 Technology development funds allocation

Many projects have set up an independent foundation to manage the proceeds of funding. This approach was popularised by Ethereum. This model can run into issues if the independent board members of the foundation have a different vision to the project team.

The Tezos class action law suits are an example of this. If the board members of the foundation overlap with the board members of the commercial entity doing the work, then there is the potential for undue influence from the commercial entity on the foundation.

The funds for development of the core technology would be administered by a Meeco entity with appropriate fiscal and legal governance and oversight.

5.3 Treasury funds

The Treasury governance is modelled on the Dash distributed autonomous organisation model. The distribution of Master Nodes and backers on a jurisdictional basis helps to prevent a concentration of influence. The weighting of votes is a function of the stake of the voter and the amount of transactions the voter's smart contracts have processed. This means that the voters who are driving more utility into the network have a higher say in how the treasury funds are spent.

There is a pledge from the Meeco commercial entity to vote for a portion of the treasury funds to be accessible to fund open source development related to distributed ledger technology. This might also include helping to fund developers and eco-system partners who wish to devote a percentage of their time to advance the common good of the network.

5.4 Commercial operation and future funding

Meeco Group Pty Ltd was registered as a company in Australia in August 2012. Through its parent entity, Meeco Planet Pty Ltd, to date it has raised AUD$4.7M with a mandate to develop a range of technologies to enable everyone on the planet to get equity and value for the information they share.

The company has offices in Australia and the UK (Meeco Group Ltd). Meeco is currently governed by a board of three directors.

Katryna Dow - Founder & CEO
Appointed Director: 24 August 2012 at the inception of Meeco

Katryna devised the concept for Meeco in late 2011. In early 2012 she wrote the Meeco Manifesto, and later that year formed the company Meeco Group Pty Ltd. She bootstrapped the company through 2012 and 2013, including self-funding a small development team. At the beginning of 2014 Meeco raised external equity, a pledge of AUD$1.8M towards the development of the Meeco platform. The funds were advanced over a period of two years based on meeting specific objectives and milestones.

Robert Collins
Appointed Director: 19 January 2016

Robert is a non-executive director and Meeco investor. He successfully led the second round of seed investment AUD$1.4M in October 2015 and subsequently secured a seat on the Meeco Board.

Glenn Smith
Appointed Director: 11 January 2018

Glenn Smith is a non-executive director. He successfully led the third round of seed investment of AUD$1.5M in March 2017 and was invited to subsequently join the Board.

The Meeco Planet Pty Ltd Board directs commercial activities for the Meeco group of companies, including the commercialisation of Meeco's existing technology; API-of-Me platform, web and mobile applications, data wallet, data vault, Consent Engine, and personal event ledger.

Additionally, Meeco has pioneered its technology through research and development, formalised trials, proof-of-concepts and learning labs. All eligible Research and Development rebates from the Australian Government have been re-invested into ongoing R&D.

Meeco has proven to be strong on internal governance, fiscally responsible, enterprising and resilient, carving out an entirely new market with sustained focus over the past four years since launch. Katryna's vision and focus has steered the company into a global market where she is recognised as a thought leader and champion of digital rights. She devised the progressive disclosure consumption based (tokenised) business model in 2013, which was the basis for achieving the first round of funding. Together with her early backers she was clear that a tokenised economy would enable the fair access and exchange of personal data.

Based on the community engagement of this Whitepaper, the Board will consider a recommendation on funding options, which may include direct investment, service provider partnerships and/or an Initial Coin Offering (ICO), including the appropriate jurisdiction.

5.5 Law enforcement

In a representative democracy, liability for the safety of citizens is assumed by the nation state. The justice system is selected based on where the crime occurs. Self-Sovereign Identity requires protection. When society functioned as tribes, the laws were set and upheld by the tribe. The centralisation to cities and empires resulted in local laws. Further centralisation to nation states brought about the emergence of local, state and federal laws.

Whilst it can be argued that a move towards distributed autonomous organisations (DAO) may be the future, it is clear that without the right governance, ethics and societal incentives, the risks of liability, recourse and injustice is too high.

It is for this reason that Meeco would advocate that a Treasury dedicate a pool to fund the bounty program outlined in section 4.5.1. Ultimately, the Identity Providers accept liability in making use of identity through the blockchain with a Service Provider. As such the Identity Providers should participate the economic rewards to assist in the protection of the Self-Sovereign Identity ecosystem. The governance of release of funds will be administered by the jurisdiction(s) where the prosecutions take place.

6. Distribution and bootstrapping the network

Initially the system will be bootstrapped by Meeco, creating Identity Provider proxy servers. These will be slim APIs that are a custom integration between how Meeco sends data around the network, and the API design of the Identity Providers systems, such as:

- Australia – myGov, GovPass
- Belgium – eID & eIDAS
- Dutch – EHerrkenning
- Estonia – e-Identity & eIDAS
- EU – European Union's Electronic Identification and Trust Services (eIDAS)
- France - eIDAS
- Germany – national eID & eIDAS
- Norway – Difi, Norwegian public authorities: MinID, BankID, BankID, Buypass or Commfides.
- UK Government – Verify & eIDAS.

The countries chosen as the initial target market were selected based on the relationship developed with the Meeco team, and the existing Identity Provider infrastructure (as shown in Figure 15).

The US has been excluded for now because of the complexity of the market in terms of state and federal laws, together with the lack of privacy protections and or data rights for USA residents and citizens.

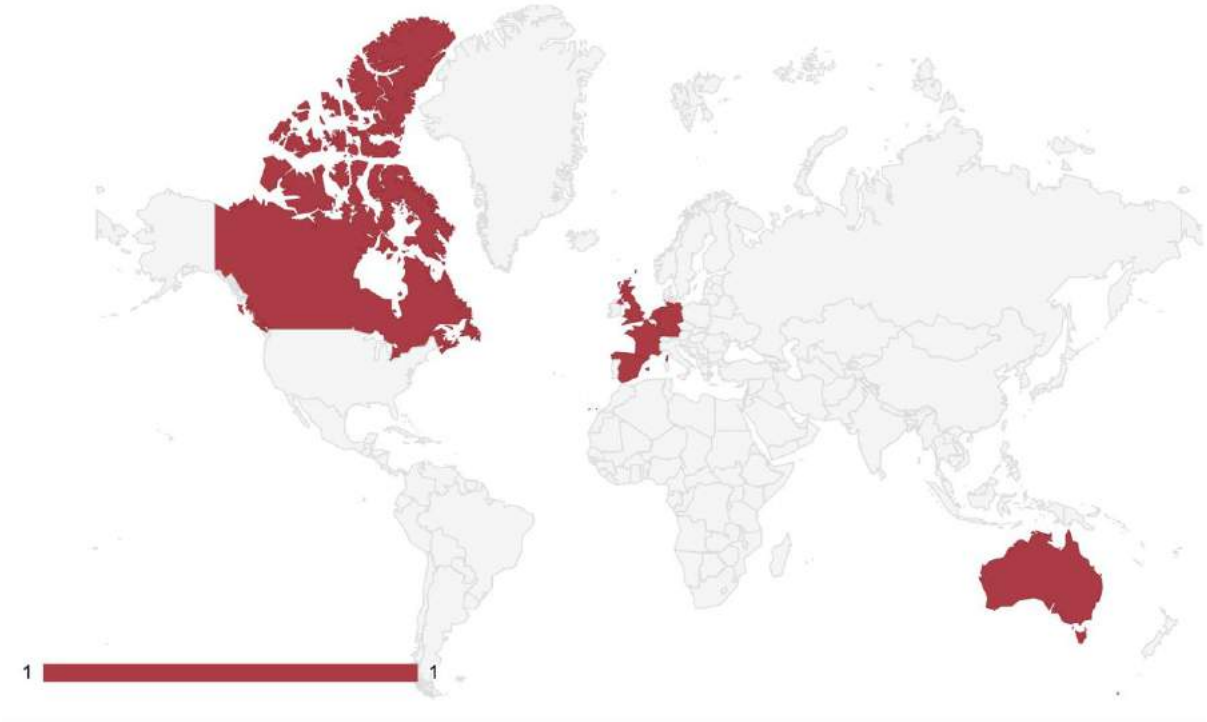


Figure 15: Target markets - Australia, UK, Estonia, France, Belgium, Netherlands, Luxemburg, Germany, Spain and Canada

Meeco will create an economic incentive for state sponsored support of on-boarding Service Providers.

Meeco will allow the first country that integrates a minimum viable utility, made of up of banks, telco and government identity providers to stake or back a Master Node in every jurisdiction.

The minimum viable utility will be determined based on population and geography served.

Conclusion

Through the leadership and drive of our founder, Katryna Dow, Meeco has been pioneering personal data since 2012. Our vision for everyone on the planet to get equity and value for the information they share is an idea whose time has come.

Meeco has a track record of development and delivery with the skills and experience to extend distributed ledger technology to power the API-of-Me.

Meeco has proven to be a worthy steward of investment, achieving a global presence, five international awards and recognition across Fintech, Identity, RegTech, Innovation and Personal Data.

Regulatory forces in Europe and Australia are now driving change around the access and processing of personal data. Audit and the transparency of smart contracts enable new business rules and models. Economic incentives for a trusted data eco-system are now ready and able to emerge.

This whitepaper provides the community an opportunity to help Meeco shape a new trust-based ecosystem so people access, control, delegate and consent to use their data to create value.

We are on the cusp of a personal data revolution, join us!

DISCLAIMER

This Whitepaper, or versions thereof does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any territory.

IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL OR OTHER PROFESSIONAL ADVISOR(S).

This paper outlines the credentials of Meeco. For more information about our history and the team visit https://meeco.me/whitepaper

Works cited

[1] G. Samman and K. Dow, “Immutable Me,” GitHub, 5 May 2016. [Online]. Available: https://github.com/ymmah/ID2020/blob/50badc19f41fcb478edb7756add9fe9f000882c2/topics-and-advance-readings/immutable-me.pdf. [Accessed 13 May 2018].

[2] Ponemon Institute, “2017 Ponemon Cost of Data Breach Study Global Overview,” IBM, 2017.

[3] Statista, “Number of compromised data records in selected data breaches as of March 2018 (in millions),” 2018. [Online]. Available: https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/. [Accessed 13 May 2018].

[4] Equifax, “Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation Of Cybersecurity Incident,” Equifax, 2 October 2017. [Online]. Available: https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821. [Accessed 29 April 2018].

[5] Consumer Financial Protection Bureau, “Consumer Financial Protection Bureau Fines Wells Fargo $100 Million for Widespread Illegal Practice of Secretly Opening Unauthorized Accounts,” 8 September 2016. [Online]. Available: https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-fines-wells-fargo-100-million-widespread-illegal-practice-secretly-opening-unauthorized-accounts/. [Accessed 29 April 2018].

[6] Z. Whittaker, “AdultFriendFinder Network Hack Exposes 412 Million Accounts,” ZDNet, 13 November 2016. [Online]. Available: https://www.zdnet.com/article/adultfriendfinder-network-hack-exposes-secrets-of-412-million-users/. [Accessed 29 April 2018].

[7] N. Confessore, “Cambridge Analytica and Facebook: The Scandal and the Fallout So Far,” The New York Times, 4 April 2018. [Online]. Available: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. [Accessed 13 May 2018].

[8] U. Maurer, “Unifying Zero-Knowledge Proofs of Knowledge,” in *International Conference on Cryptology in Africa*, 2009.

[9] T. Bouma, “I Need a Triple A Identity from You.,” Medium, 18 February 2018. [Online]. Available: https://medium.com/@trbouma/i-need-a-triple-a-identity-from-you-c6a09f32eec1. [Accessed 29 March 2018].

[10] T. Bouma, “Self Sovereign Identity—An Unofficial Generic Icon,” Medium, 26 February 2018. [Online]. Available: https://medium.com/@trbouma/self-sovereign-identity-an-unofficial-generic-icon-a5a6ab332cd7. [Accessed 10 April 2018].

[11] C. Allen, “Self-Sovereign Identity Principles 1.0,” GitHub, 23 October 2016. [Online]. Available: https://github.com/ChristopherA/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md. [Accessed 13 May 2018].

[12] “Regulation (EU) 2016/679 of the European Parliament and of the Council,” The European Parliament and the Council of the European Union, 27 April 2016. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC. [Accessed 10 March 2018].

[13] “GDPR Key Changes,” EU GDPR Portal: Powered by Trunomi, [Online]. Available: https://www.eugdpr.org/key-changes.html. [Accessed 10 March 2018].

[14] European Commission, “Information about Directive (EU) 2015/2366 on payment services including date of entry into force and a link to the summary.,” 12 January 2016. [Online]. Available: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366/law-details_en. [Accessed 10 March 2018].

[15] Payment Systems Regulator, “The Payment Services Regulations 2017 – the PSR’s draft approach to monitoring and enforcement,” 13 April 2017. [Online]. Available: https://www.psr.org.uk/psr-publications/consultations/Payment-Services-Regs-2017-draft-approach. [Accessed 10 May 2018].

[16] “UBS: Australian banks have hugely inflated borrower incomes,” Macro Business, 6 February 2018. [Online]. Available: https://www.macrobusiness.com.au/2018/02/ubs-australian-banks-hugely-inflated-borrower-incomes/. [Accessed 7 March 2018].

[17] Bitcoin, “Merkle Tree,” [Online]. Available: https://bitcoin.org/en/glossary/merkle-tree. [Accessed 13 May 2018].

[18] NuCypher, “Upgradeable contracts,” 27 March 2018. [Online]. Available: https://github.com/nucypher/nucypher-kms-ethereum/tree/master/nkms_eth/project/contracts/proxy. [Accessed 1 May 2018].

[19] M. Egorov, D. Nunez and M. Wilkison, “NuCypher KMS: Decentralized key management system,” 27 April 2018. [Online]. Available: https://www.nucypher.com/whitepapers/english.pdf. [Accessed 27 April 2018].

[20] Onecryptor, “Proxy Re-Encryption, Frictionless end-to-end encryption integrated into your workflow,” [Online]. Available: https://besafe.io/proxy-re-encryption/. [Accessed 28 April 2018].

[21] R. Shea, Twitter, 11 April 2018. [Online]. Available: https://twitter.com/ryaneshea/status/983855146022170625. [Accessed 11 April 2018].

[22] M. Goldin, “Token-Curated Registries 1.0,” ConsenSys, 15 September 2017. [Online]. Available: https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7. [Accessed 20 April 2018].

[23] Google , “Find, lock, or erase a lost Android device,” Google, [Online]. Available: https://support.google.com/accounts/answer/6160491?hl=en. [Accessed 28 3 2018].

[24] Apple Inc, “If your Mac is lost or stolen,” Apple Inc, 4 December 2017. [Online]. Available: https://support.apple.com/en-au/HT204756. [Accessed 28 March 2018].

[25] D. Reed, J. Law, D. Hardman and M. Lodder, “DKMS (Decentralized Key Management System) Design and Architecture V3,” Hyperledger, 2 April 2018. [Online]. Available: https://github.com/hyperledger/indy-sdk/blob/master/doc/dkms/DKMS%20Design%20and%20Architecture%20V3.md. [Accessed 2 April 2018].

[26] M. Luongo and C. Pon, “The Keep Network: A Privacy Layer for Public Blockchains,” Keep Network, 2017.

[27] G. Zyskind, O. Nathan and A. S. Pentland, “Enigma: Decentralized Computation Platform with Guaranteed Privacy,” Enigma, 2017.

[28] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[29] P. Evans-Greenwood, R. Hillard, I. Harper and P. Williams, “Bitcoin, Blockchain & distributed ledgers Caught between promise and reality,” Deloitte, 2016.

[30] T. McConaghy, “Can Blockchains Go Rogue? AI Whack-A-Mole, Incentive Machines, and Life. TE Series Part I.,” OceanProtocol, 28 February 2018. [Online]. Available: https://blog.oceanprotocol.com/can-blockchains-go-rogue-5134300ce790. [Accessed 26 April 2018].

[31] K. Samani, “Understanding Token Velocity,” 8 December 2017. [Online]. Available: https://multicoin.capital/2017/12/08/understanding-token-velocity/. [Accessed 19 April 2018].

[32] Anon., “Masternode coins,” 21 April 2018. [Online]. Available: https://docs.google.com/spreadsheets/d/1D-VhuSSt7fMrSP22WdREqOuJIDu4iZV7vrx41jBNnqQ/edit#gid=708288622. [Accessed 21 April 2018].

[33] CryptoID, “Stratis Explorer,” CryptoID, 21 April 2018. [Online]. Available: https://chainz.cryptoid.info/strat/#. [Accessed 21 April 2018].

[34] Saul, “NEM Supernode Reqards Program,” 26 January 2016. [Online]. Available: https://forum.nem.io/t/nem-supernode-rewards-program/1735. [Accessed 19 April 2018].

[35] R. Yap, “Znodes Specifications Release and Founders’ Rewards Reduction,” 14 November 2017. [Online]. Available: https://zcoin.io/znodes-specifications-release-founders-rewards-reduction/. [Accessed 20 April 2018].

[36] Tendermint, “Byzantine Consensus Algorithm,” [Online]. Available: https://tendermint.readthedocs.io/en/master/specification/byzantine-consensus-algorithm.html. [Accessed 20 4 2018].

[37] C. Kulman, “Smallest number of nodes for an Ethereum private blockchain,” Ethereum Stack Exchange, 7 March 2016. [Online]. Available: https://ethereum.stackexchange.com/questions/1468/smallest-number-of-nodes-for-an-ethereum-private-blockchain. [Accessed 21 April 2018].

[38] CryptoID, “Stratis Explorer,” CryptoID, 21 April 2018. [Online]. Available: https://chainz.cryptoid.info/strat/#!network. [Accessed 21 April 2018].

[39] CryptoID, “Dash Master Nodes,” CryptoID, 21 April 2018. [Online]. Available: https://chainz.cryptoid.info/dash/masternodes.dws. [Accessed 21 April 2018].

[40] Nem Nodes, “NEM node list,” 21 April 2018. [Online]. Available: https://nemnodes.org/nodes/. [Accessed 21 April 2018].

[41] NEM team, “Community Fund DAO, Submission Requirements Guidelines,” [Online]. Available: https://nem.io/wp-content/themes/nem/files/CommunityFundDao.pdf. [Accessed 20 April 2018].

[42] The Dash Network, “Decentralized Governance System,” [Online]. Available: https://www.dash.org/governance/. [Accessed 21 April 2018].

[43] PIVX Community, “Coin Specs,” [Online]. Available: https://pivx.org/coin-specs/. [Accessed 20 4 2018].

[44] Pivx Wiki, “Metrics PIVX,” [Online]. Available: http://pivx.wiki/metrics/. [Accessed 20 4 2018].

[45] PIVX Forum, “PIVX How to Create a Proposal,” [Online]. Available: https://forum.pivx.org/t/howto-create-a-proposal/959. [Accessed 20 April 2018].

[46] R. Yap, “What is the Total Supply and Distribution for Zcoin,” 1 November 2016. [Online]. Available: https://zcoin.io/ufaqs/what-is-the-distribution-for-zcoin/. [Accessed 20 April 2018].

[47] Hanniabu, “Blocknet Proposal Introduction & Guide,” 2 November 2017. [Online]. Available: http://blocknetdx.forumotion.com/t6-blocknet-proposal-introduction-guide. [Accessed 20 April 2018].

[48] Ionomy, “Developmnent & Incentive Coin Addresses,” 2018. [Online]. Available: https://ionomy.com/bounty-info. [Accessed 20 April 2018].

[49] TECH, Crown, “Building a Fairly Governed Economy,” [Online]. Available: https://crown.tech/governance/. [Accessed 19 April 2018].

[50] M. Brusov, Y. Lobyntsev, K. Kurbanova and N. Kolmakhidze, 4 October 2017. [Online]. Available: https://cindicator.com/Cindicator_WhitePaper_en.pdf. [Accessed 12 November 2017].

[51] V. Buterin, “On Medium-of-Exchange Token Valuations,” 17 October 2017. [Online]. Available: https://vitalik.ca/general/2017/10/17/moe.html. [Accessed 4 March 2018].

[52] W. Mougayar, “Tokenomics—A Business Guide to Token Usage, Utility and Value,” Medium, 11 June 2017. [Online]. Available: https://medium.com/@wmougayar/tokenomics-a-business-guide-to-token-usage-utility-and-value-b19242053416. [Accessed 7 April 2018].

[53] M. Sall, “Valuing Cryptoassets from the Ground Up,” Medium, 24 April 2018. [Online]. Available: https://medium.com/@sall/valuing-cryptoassets-from-the-ground-up-441ad5a9ff03. [Accessed 25 April 2018].

[54] F. Krueger, “How to Think About Tokenomics,” Medium, 12 February 2018. [Online]. Available: https://medium.com/workcoin/how-to-think-about-tokenomics-b3da509444e5. [Accessed 18 April 2018].

[55] T. McConaghy, “Towards a Practice of Token Engineering,” Ocean Protocol, 1 March 2018. [Online]. Available: https://blog.oceanprotocol.com/towards-a-practice-of-token-engineering-b02feeeff7ca. [Accessed 25 April 2018].

[56] J. Horne, “The Emergence of Cryptoeconomic Primitives,” Medium, 5 March 2018. [Online]. Available: https://medium.com/@jacobscott/the-emergence-of-cryptoeconomic-primitives-14ef3300cc10. [Accessed 26 April 2018].

[57] M. Goldin, “Token Curated Registries 1.0,” Consensus, 15 September 2017. [Online]. Available: https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7. [Accessed 26 April 2018].

[58] P. Bhakta, “KYC Norms Could Burn a Hole in e-wallet Companies Pockets,” 11 October 2017. [Online]. Available: https://economictimes.indiatimes.com/small-biz/money/kyc-norms-could-

burn-a-hole-in-e-wallet-companies-pockets/articleshow/61030204.cms. [Accessed 19 April 2018].

[59] Global Brand Prices, “The price of Coca-Cola around the world,” December 2015. [Online]. Available: http://www.globalbrandprices.com/rankings/Coca_cola/. [Accessed 6 May 2018].

[60] CIA World Factbooks, “Countries Compared by Economy > GDP > Purchasing power parity per capita. International Statistics at NationMaster.com,” 28 March 2011. [Online]. Available: http://www.nationmaster.com/country-info/stats/Economy/GDP/Purchasing-power-parity-per-capita. [Accessed 20 April 2018].

[61] Company in Estonia, “BlueOrange Bank KYC requirements for a new company,” [Online]. Available: https://www.estoniancompanyregistration.com/blueorange-bank-kyc/. [Accessed 11 May 2018].

[62] TheBanks.eu, “List of Banks in Estonia,” [Online]. Available: https://thebanks.eu/banks-by-country/Estonia. [Accessed 13 May 2018].

[63] A. Roos and J. Oun, “Credit Unions in Estonia,” *Karafolas S. (eds) Credit Cooperative Institutions in European Countries. Contributions to Economics.,* pp. 283-290, 10 May 2016.

[64] V. Goncalves, “Typical UK bank will spend £10m annually on inefficient KYC: Research,” Private Banker International, 27 June 2017. [Online]. Available: https://www.verdict.co.uk/private-banker-international/news/typical-uk-bank-will-spend-10m-annually-inefficient-kyc-research/. [Accessed 11 May 2018].

[65] Barclays UK, “Barclays PLC Annual Report 2016,” 2016. [Online]. Available: https://www.home.barclays/content/dam/barclayspublic/docs/InvestorRelations/AnnualReports/AR2016/4%20Barclays%20UK%20Performance.pdf. [Accessed 11 May 2018].

[66] TheBanks.eu, “List of Banks in the United Kingdom,” [Online]. Available: https://thebanks.eu/banks-by-country/United-Kingdom. [Accessed 13 May 2018].

[67] “Credit Unions in the UK,” [Online]. Available: http://www.creditunions.co.uk/. [Accessed 13 May 2018].

[68] Statista, “Number of customers per bank employee in France from 2008 to 2015,” [Online]. Available: https://www.statista.com/statistics/749118/number-customers-per-employee-bank-france/. [Accessed 11 May 2018].

[69] B. Mairs, “Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity,” Thomson Reuters, 9 May 2016. [Online]. Available:

https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html. [Accessed 25 April 2018].

[70] K. Nilsson, “Breaking open the MtGox case, part 1,” 27 July 2017. [Online]. Available: https://blog.wizsec.jp/2017/07/breaking-open-mtgox-1.html. [Accessed 10 April 2018].

[71] Sovrin Board of Trustees, “Sovrin Founding Steward Agreement,” 28 June 2017. [Online]. Available: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Founding-Steward-Agreement-2017-06-28.pdf. [Accessed 1 April 2018].

[72] The Federal Bureau of Investigations, “Online Gambling, Don't Roll the Dice,” 6 June 2007. [Online]. Available: https://archives.fbi.gov/archives/news/stories/2007/june/gambling_060607. [Accessed 11 May 2018].

[73] Australian Government Federal Register of Leglislation Year: 2016 Month: March Day: 10 Year acces, “Interactive Gambling Act 2001, No. 84, Compilation No. 14,” 10 March 2016. [Online]. Available: https://www.legislation.gov.au/Details/C2016C00607. [Accessed 11 May 2018].

