SelfKey

The SelfKey Foundation

September 11th 2017

Contents

Problem: You do not own your own identity

As the Internet proliferates throughout the world, it becomes an intrinsic element of human daily life in almost every domain. The Internet is an inherently digital, international, exponential and technology network unbounded by traditional borders. The shift from paper to digital computing and Internet 1.0[i] and 2.0[ii] were some of the most fundamental changes of recent modern history. Today, almost everything is being disrupted by digitalization, computing, and the Internet. The development of blockchain is considered by many to enable an Internet 3.0.[iii]

However, despite advancement and disruption in other domains, the identity systems we rely upon today are currently paper-based, nationally-driven, government identity systems and do not leverage the power of Internet 3.0. Millions of people currently rely on — or are excluded from— identity systems due to a lack of any modern technology infrastructure.[iv]

Most identity systems are centrally planned and managed, do not integrate or link to other systems, and do not place the identity owner in a place of entitlement and power. These systems lead to inefficiencies, data leaks, threats, loss of privacy and identity theft[v] which have left billions without financial accounts of any kind.[vi]

Many centralized identity systems have very serious security issues.[vii] The recent Equifax data breach where the personal data of up to 143 million individuals may have been compromised highlights the vulnerability of centralized databases and calls into question the continued practice of collecting large centralized sets of highly sensitive data.[viii] In some instances, the citizens of entire countries (such as Sweden[ix]) have suffered potentially devastating personal data breaches. These breaches often do not occur as a result of hacking or other malicious efforts but, instead, because appropriate safeguards did not exist to prevent unauthorized access to the data.[x]

Current identity systems have largely failed to deliver any of the most basic requirements for a successful identity system: security, privacy, ownership, access, protection, interoperability, or linked data portability to identity owners.

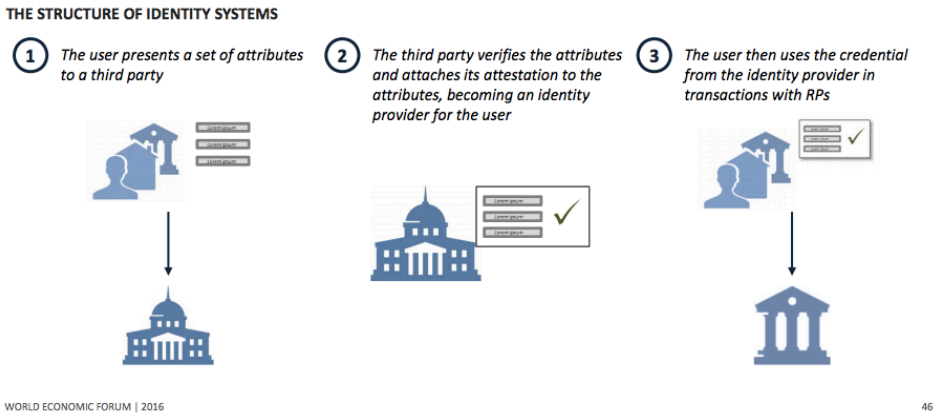
> "Current identity systems are limiting Fintech innovation as well as secure and efficient service delivery in Financial Services and society more broadly. Digital identity is widely recognised as the next step in identity systems." – WEF[xi]

The failings of traditional centralized identity systems are clear. To ensure that individuals retain ownership of their identity, the development of a sustainable digital identity model for our evolving global society is now essential.

Background

Parties in an Identity Transaction

There are typically three parties in an identity transaction; an identity owner (**IO**) (such as an individual or company), an identity claim issuer (**CI**) or 3rd party (such as a notary public or justice of the peace), and a relying party (**RP**) (such as a bank, brokerage or other financial institution). The IO has one or more identity claims (**IC**) (e.g. "My name is John H. Smith" or "I was born on 1 January 1975"). These claims are then attested to or verified by a third party and the IO is then able to share these verified claims with a relying party, to gain access to the relying party's products and services, such as opening a bank account.



By way of example, an individual (**IO**) wants to prove to a coin exchange (RP) that they are a US person (**claim**) and that they have a US passport (a **proof**) and that the electronic copy they are sending is a certified true copy of an original. This is an electronic identity claim which receives an **attestation** from

a notary and becomes a **verified claim.** Verified claims are the future of digital identity.

All of these parties struggle with the current paper driven and centralized identity systems, and would benefit from a digitized, decentralized identity system.

Limitations of a centrally managed identity system

Security and other risks

Most identity systems have large centralized databases containing millions (or billions) of identity records. Because of their sheer size, these centralized databases are high-value targets for hackers. The identity data they contain is relatively easy to steal and use.[xii] Because the reward for a successful breach increases exponentially with the number of identities held in that database, as a database grows larger, it becomes increasingly more vulnerable to attack. Furthermore, a single large database (as opposed to multiple, segmented, decentralized databases) often means a single point of failure.

Centralized identity systems are usually managed by a single party and that party then uses third-party processors to access the databases and process the data - often without sufficient safeguards and oversight – making the databases even more vulnerable to data breaches. Even if the operator is trustworthy, a centralized identity system is vulnerable through third-parties with authorized access. Individual identity documents are valuable commodities that are easily sold on the black market. Purchasers of stolen identity data can use this information to commit fraud and other crimes using the names of the innocent identity owners. Beyond the obvious damage identity theft wreaks on the identity owner, such breaches create significant liabilities for the operator of the central database.

Restricted access

To try and prevent unauthorized access to these centralized databases, access to the data is restricted by the operator. However, this often prevents identity owners from accessing their own data.[xiii] If operators do not allow the data to be accessed, that data cannot be linked to the benefit of the identity owner.

Linked data is a key component of digital identity[xiv], as linking data means that the identity owner can create linked relationships between data to their benefit.

Linking data is not a technically challenging task. In fact, these technologies are widely available today.

Key technologies that support linked data are URIs (a way to identify entities); HTTP (a simple but universal mechanism for retrieving resources); and RDF (a generic graph-based data model with which to structure and link data).[xv] These technologies have been around for years and yet individual identity owners cannot benefit from linked data.

In addition to the technical limitations and security risks introduced through using a centralized database, there are a number of business concerns of a single large database operator of identity data.

Monopolies

If there were a single, for-profit organization with a database containing the identity data of every person on the planet, it would operate as a monopoly and be able to charge high prices for access to that data. Furthermore, if the operator gained traction, the "network effect" would effectively lock users into the network. This, in turn, would create significant barriers to entry for new market participants. In the absence of competitive pressure, monopolistic pricing and reduced innovation would likely result.[xvi]

Data protection compliance

A large, globally centralized database for identity could also breach data privacy and data protection laws.

National and supranational data protection laws are designed to ensure data controllers put in place policies and procedures to keep personal data as secure as possible under threat of heavy monetary penalties and possible imprisonment if they fail to do so. However, these laws are different for each jurisdiction, and compliance standards vary enormously. Recent years have also seen an increasing trend towards jurisdictions adopting data exports controls. For instance, "the EU views the underlying US privacy laws as not meeting EU

adequacy requirements[xvii]". In response, only certain companies will be eligible to transfer data from the EU to the US if they can comply with the "privacy shield" framework. This is a barrier to entry for new startups who cannot meet these burdensome and potentially expensive compliance requirements. To compound the problem, the "privacy shield" framework is already under threat, less than 18 months after it replaced the "safe harbor" mechanism which was deemed inadequate by the European Court of Justice.

Central to most data protection laws is the concept of user consent. This is normally given by individuals at the time they provide their personal data through a tick-box or similar mechanism. However, as individuals are not at the epicenter of existing identity management process, they cannot easily grant (or revoke) consent or track the consent they give over time despite this being their inalienable right under those laws. Increasingly, data protection requires dynamic consent mechanisms to overcome these issues, but these are difficult to achieve with largely paper-based consent models.

Recent years have also seen a huge rise in international data-sharing regimes between regulatory authorities in a number of different jurisdictions with the introduction of FATCA, the Common Reporting Standards and other international data sharing agreements. Many of these sharing agreements are also exempted from data subject consent requirements under national data privacy laws, so individual identity owner consent is not required before their data is shared. One of the sectors where identity data routinely crosses borders is financial services and the data being shared between regulatory bodies routinely includes identity data obtained via the KYC process.

KYC regulatory requirements

KYC laws are national and international in scope, representing a huge and diverse group of relying parties including (without limitation) the following: coin exchanges, fintech startups, money transmitters, real estate companies and agents, precious metals dealers or storage facilities, fiduciaries, corporate services providers, lenders, banks, securities firms, lawyers, accountants, non-profit foundations, professional service providers, notaries, governments, insurers, re-insurers, financial institutions, and generally any legal entity or natural person dealing in money or finance.

KYC is not an option—itis mandatory, with civil or criminal sanctions imposed by both local and international bodies for failure to comply with KYC laws. Unfortunately, for many individuals and companies—from small startups to large corporations, as well as relying parties—KYC compliance is an expensive and painful reality.

For relying parties - KYC is expensive and time-consuming. The average annual, recurring cost of KYC compliance is USD 60 million for the average bank, but may be up to USD 500 million for others.[xviii] This cost is necessarily high because relying parties cannot quickly and easily access up to date identity data, validate the data or screen it to satisfy their regulatory requirements. Therefore, relying parties must send new requests to the identity owner and must treat every identity owner as a 'blank canvas' and force them through the a fully robust KYC process.

The time and effort expended by one relying party to perform KYC validation checks cannot be reused or recycled and is not leveraged in future requests. If the identity owner decides to change service providers, these same checks need to be completed by the new relying party. The identity data is not "ported" to the new service provider and so ends up being held by multiple providers, many of whom hold redundant, yet still highly sensitive identity data, for individuals who are no longer their clients or customers. The high cost involved in this procedure creates a barrier to exit when changing service providers, leading to an uncompetitive environment, to the detriment of identity owners, fintech startups, and innovation, generally and increases the risk of identity theft for the individuals.

Furthermore, those who lack identity documents issued by a national government are excluded from commerce completely because of their inability to comply with KYC regulations. Although certainly well-intentioned, KYC regulations can easily exclude legitimate market participants[xix] and slow down international commerce. This problem could be easily solved if there was a way for existing KYC data to be linked, re-used, and easily ported across borders in a compliant manner.

Solution: "SelfKey" Self-Sovereign Digital Identity Ecosystem

Our idea is simple: that users should be at the center of their identity management process, a concept known as **S**elf-**S**overeign **ID**entity (**SSID**). We can escape from the legacy systems of paper-based documents and move into a digital identity with privacy, security, transparency and individual rights with SelfKey, a SSID implementation built using blockchain technology, with the corresponding keys held in a digital identity wallet.

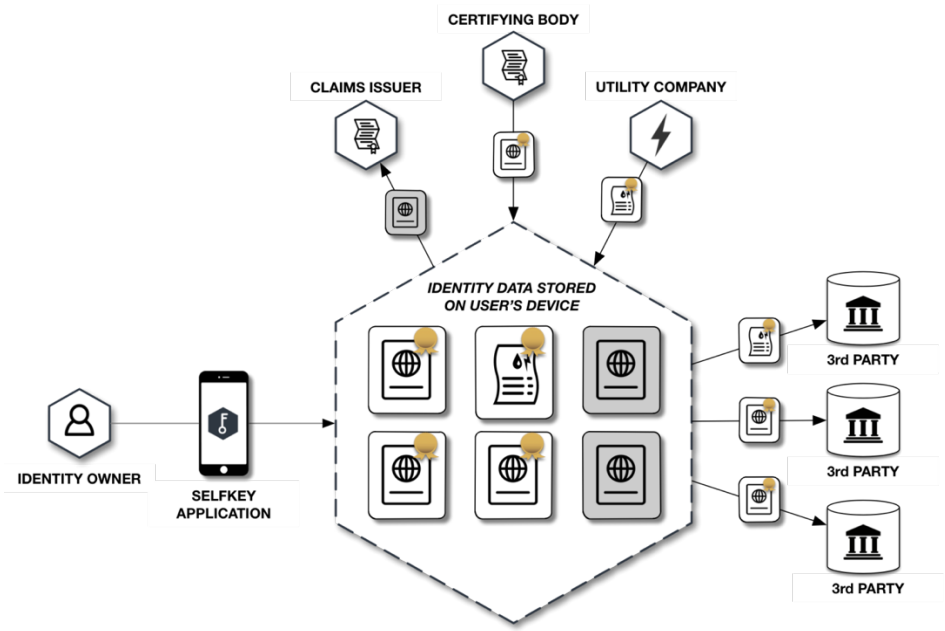
SelfKey is an identity system built on an open platform consisting of several key components including: **SelfKey Foundation, a non-profit foundation** whose charter and governance enshrines the principles of self-sovereign identity, a technology stack with a **free and open source identity wallet for the identity owner**, a marketplace with **real products and services** available at launch, a JSON-LD (machine readable) protocol, connection to 3rd party **identity micro services** which comply with **KYC laws and regulations**, and **a native token called "KEY"** which enables the SelfKey ecosystem to exchange value and information in an efficient, fully-digital, self-sovereign manner.

The products available at launch* include:

- Bitcoin and Digital Asset Exchange Signup
- Citizenship by Investment programs
- Citizenship through Investment in Real Estate Applications
- Company incorporation (including companies limited by shares, foundations, LLC's and Trusts)
- Bank account introduction and application
- Residence Permit Applications for more than 50 countries
- E-Wallets or Stored value facilities
- Gold and Precious Metals purchase and storage
- International insurance applications
- Money Remittance & Transfer services
- Token Sales

Whilst providing tangible utility for the KEY token for identity owners, relying parties and verifiers, through real world products and services, SelfKey overcomes the limitations of centralized identity systems, helps achieve compliance with the most comprehensive national data protection laws and KYC regulations, and returns ownership and control of identity data back to the individual – the identity owner.

SelfKey makes identity transactions more secure, private and efficient while complying with the myriad of laws and regulations that exist today. However, SelfKey is also building a bridge to a better world - one with digitally signed verified identity claims, data minimization, proof of individuality, proper governance, and a user-centric identity system. In this new world, the user can truly control, manage, and own their digital identity. SelfKey is designed to be censorship-proof, fair, inclusive, agile, and lean through a well-designed open source technology stack, and transparent legal & governance infrastructure through the SelfKey Foundation. SelfKey can match the current and future needs of evolving modern societies and the global Internet, ensuring human rights and fundamental freedoms of identity are met.



*Void where prohibited. These services are not offered by SelfKey foundation directly, but by partners who accept information/KYC sent by identity owners by using SelfKey.

Is blockchain the answer?

A blockchain is a distributed ledger whereby data is simultaneously replicated to all participants. Should our identity data be **stored on *and replicated across*** a blockchain that is managed by a number of participating entities (for instance big banks or governments)?

No. Blockchain (alone) is not the answer.

Replicating all identity data to all parties could potentially breach data protection laws for various reasons described above in the previous section, specifically the requirement to keep personal data "onshore" or within a specified jurisdiction. Furthermore, regulations and best practice requires that companies only store personal data that is relevant to their business—and even then, only with the customer's consent.

Cybersecurity risk is increased if identity data is replicated to all blockchain nodes. Central data stores are difficult to secure (as discussed above). Accordingly, simply using a blockchain to replicate this identity data to multiple parties will force each node on the chain to properly secure this data. As each organisation has their own cybersecurity practices (and gaps), this would make it easier for an attacker to steal the data. Even if the personal data is encrypted this still does not solve the problem of legal compliance, as encrypted data can still run afoul of personal data regulations.[xx] Anyone sufficiently motivated to seek to re-identify individuals from transaction records held on a decentralized ledger would likely have the wherewithal to re-identify individuals from other available databases. The fact of anonymity on the blockchain is not the whole story. In the "Big Data" era, powerful analytics technology can be applied to match databases that appear to be clear of personally-identifiable information to those which are not, and this will be a critical compliance test for blockchain solutions that record personal data.

What is the answer?

The concept of Self Sovereign Digital Identity is similar to the way we store and manage our non-digital identities today. Currently, most of us keep identity documents such as passports and birth certificates or utility bills at our homes – safely, securely, under our own control. We only share them with other entities

when necessary. Most of us don't store these important paper documents (or unnecessary personal information) with a third party—nor would we want to. Self-sovereign identity in SelfKey is the digital equivalent of what most of us already do with our physical identity documents.

How SelfKey works for the individual user

A new user would simply download the SelfKey Wallet application on a personal device. Identity data is stored locally, on the device. A user is able to back up this information onto another device or a personal backup solution.

When the user downloads the SelfKey wallet, it is empty. The first thing that a user needs to store in this container is a public/private key pair (also known as a SelfKey). This SelfKey will become the user's digital "pen" that can be used to apply an identity owner's unique digital signature to documents. Because the private key is known only to the identity owner, whenever this digital signature is applied, it serves to authenticate and validate the owner's identity to requesting parties confidentially and securely (without having to appear in person).

SelfKey has enormous benefits beyond a traditional username and password. Each SelfKey is unique to its owner. Where a username/password combination is stored in a third party's database, a SelfKey user would never share their private key - this would always remain a secret to the user.

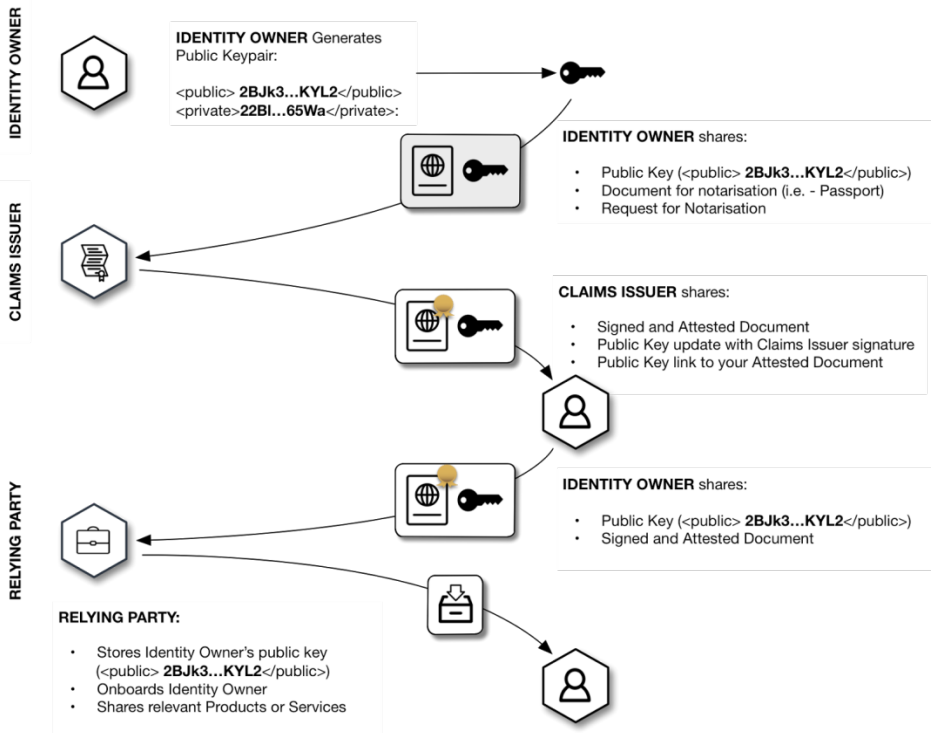
At this stage, no one–not even the SelfKey foundation–would know that this was the user's container, or that the SelfKey number even existed. No other entity issued it, and it was created solely by the user. This is exactly what it means to be self-sovereign. The user can now use SelfKey, along with identity proofs, to receive attestations from relevant verifiers such as notaries, government institutions, etc. After the user has attested identity claims stored in their digital wallet, they are eligible to purchase products and services in the SelfKey marketplace (covered in detail below).

In order for SelfKey users to take advantage of the products and services available in the SelfKey marketplace, they will first need to create identity claims. These identity claims are the user's attributes (e.g. nationality, date of birth, occupation, etc.) and are stored in text fields (JSON-LD blobs). To save

the time it would take to manually type the data into these text fields, photos or scans of documents can be saved and optical character recognition will automatically parse the information, making the process much easier. These identity proofs are needed only to comply with traditional KYC documentary requirements. In the future, SelfKey's digitally-signed attestations will eliminate identity documents as we know them today.

Once the identity claims have been created, the next step in the process is to receive attestations of these claims. Attestations can be stored in the SelfKey wallet too. These attestations are machine readable, digitally signed identity claims, which can also be valid within certain time windows.

The verifiers or relevant authorities such as utility companies, notaries, banks, passport agencies, hospitals, driving license authorities, immigration, can potentially sign the user's claims. These claims can be signed in a way whereby one could choose to disclose only a minimum of information. In other words, the identity owner can share what the requesting party needs to know, but nothing more.



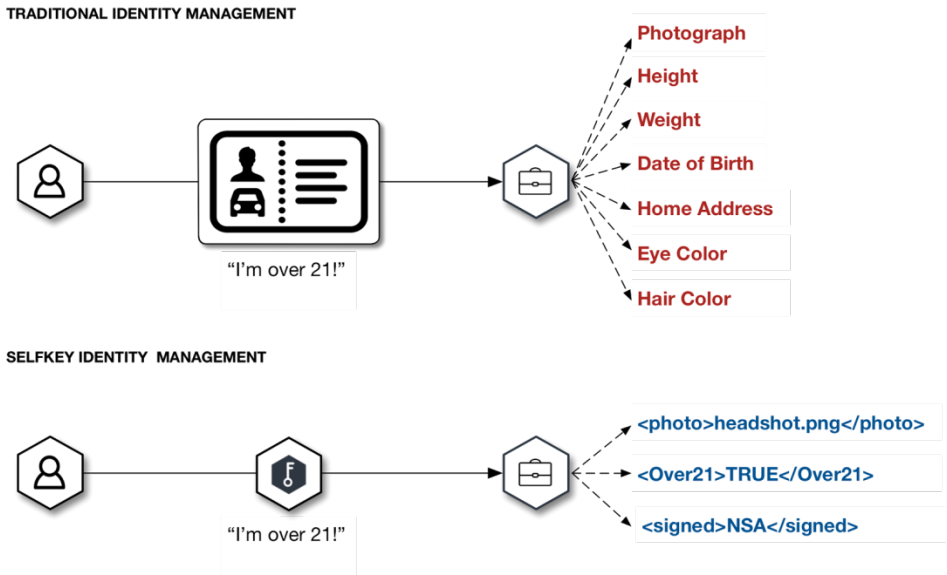
For instance, a user could easily prove they reside in a certain country. Or a person might be able to prove they are over 18" without revealing more than

this information. These identity attributes are boundless and could also include something such as "professional investor". The identity owner will be able to choose which piece of information to pass along to any relying party. The type of identity claims that can be attested is almost infinite.

Data is stored on a device (under the owner's control, the same as documents are currently stored at one's home or office today) and then when the owner wants to, they can approve a third party to collect specific data. One can do this by confirming a notification on said device. This experience feels similar to authentication via "linking" a Facebook account.

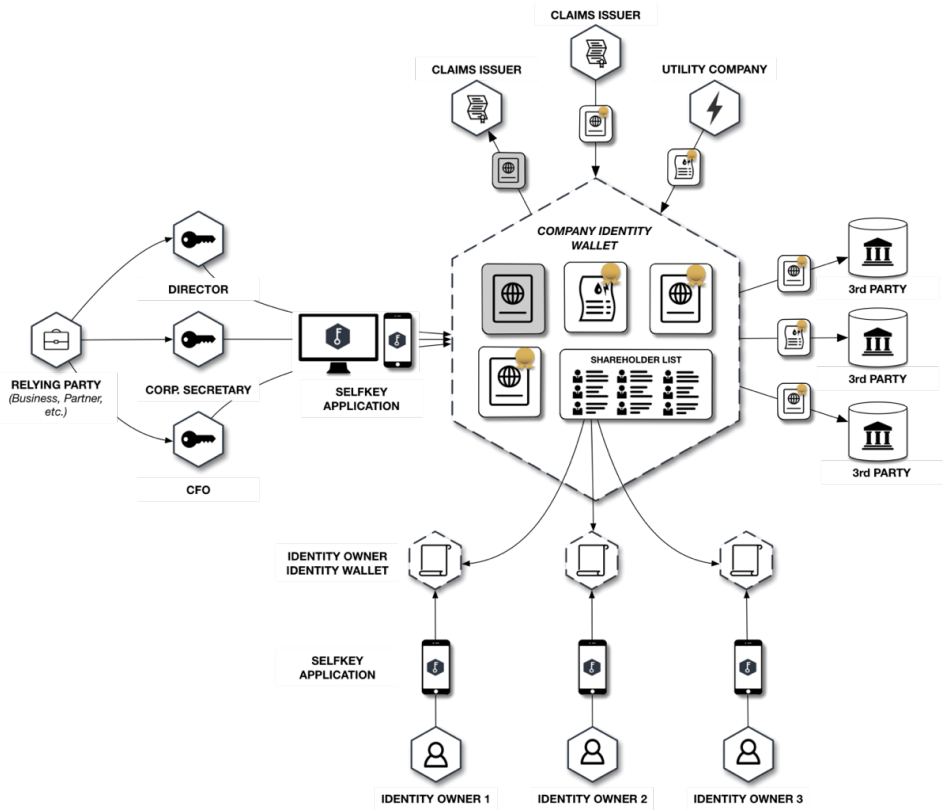
This analogy is only similar in experience-instead of going to Facebook's servers to collect personal data, a user will be granting requests from their personal data store, and will have granular control over what data is shared. Unlike certain Internet companies, the SelfKey foundation is nonprofit. There is no monetization by way of advertising or sale of user data.

Minimizing the amount of data which needs to be shared is safer both for the identity provider and the relying party. The identity owner does not share information which might be unnecessary or sensitive data – and the recipient doesn't need to store it. This helps with both security and compliance with jurisdictional privacy law requirements.



How SelfKey works for a company

As mentioned previously, identity claims and attested proofs are not limited to persons but can also apply to companies. A company could manage their startup documents from the identity wallet as well. SelfKey has basic cap table management, and can provide basic corporate governance which allows the startup to do things that are currently burdensome such as opening a bank account. When relying parties onboard a new company, KYC needs to be done not only on the specific company level but also for all significant shareholders at each ownership level above the entity until you reach the ultimate beneficial owners. This kind of level of documentation verification is extremely burdensome. Furthermore, for many businesses with multiple subsidiaries or affiliates in multiple countries, this is where the advantages of e-KYC are more compelling if linked identities can provide multilevel verification and is something a national, centralized system cannot solve.. With SelfKey, companies can easily demonstrate things that are traditionally time intensive and difficult for identity owners to prove and relying parties to validate (multiple ownership levels, complex structures, capitalization tables which can change on a daily basis).



How SelfKey works for a verifier

There are a number of companies and institutions globally who issue (or could issue) claims on behalf of identity owners for use by relying parties. Within the KYC space an obvious example of this would-be utility companies (who currently issue paper documents); banks (who give letters of attestation) and company registries (who issue paper documents). SelfKey can be used today to digitize and monetize these identity claims which relying parties are willing to pay for. This helps reinforce the crypto-economy in the SelfKey ecosystem. It may also be possible for verifiers to issue a fully digital certificate on the SelfKey platform. The owners of this company could instantly verify ownership by proving they hold the SelfKeys which were used to register the shares.[xxi]

The SelfKey network

The SelfKey Network is more than just an identity system for secure, encrypted P2P, structured data and file sharing over the Internet. The SelfKey network is designed with several innovative attributes to give it the best chance for long term adoption and success which are explored in the following paragraphs.

Foundation

First and foremost, as previously described in this paper, it is untenable for a single company to control or govern an identity system. Therefore, a foundation was formed, not for control over the network, but to preserve certain core Constitutional Principles (set out below). The foundation protects and preserves the founding principles of self-sovereign identity.

Non-Profit Status

The SelfKey Foundation makes its top priority the success of the network as a whole and the native token which runs the network (KEY). The foundation is non-profit and is set up in Mauritius which benefits from regulatory sandbox legislation that can be used by blockchain technology companies to develop and commercialize their applications The SelfKey Foundation does not sell or provide as advertising the identity data that flows in the system. All value in the network is designed to flow to and from the use of the native KEY tokens.

A critical element of the SelfKey network is the native ERC-20 Token called KEY, which stands for "Key to Encrypt Yourself". This token can be used to access products and services on the network. For instance, KEY is required to participate, used to incentivize participation, good behavior and use, and enable a self-reinforcing crypto-economy for identity which could appreciate in value as more individuals and company join the network, increasing demand for KEY. Certain actions on the network will require an exchange of KEY and others will involve placing KEY in a locked contract (to access the network, and prevent spam via an anti-Sybil mechanism) this research can provide a POI (proof of individuality mechanism) which can have vast implications to the Ethereum network.

Governance

SelfKey was founded by a for profit company, KYC-Chain Ltd (KYCC) who open sourced code and made the monetary contribution to setup the foundation. KYCC may continue to develop software for the Foundation, but for the SelfKey network to thrive it is necessary for KEY token holders to develop the open source platform as well. Members have no entitlement to receive a dividend or any distribution of profits from the SelfKey Foundation. There should be no expectation of profits resulting from the acquisition of KEY tokens although KEY holders may receive financial incentives derived through their own individual efforts in growing the network.

Legal

Remaining compliant with existing laws and regulations regarding data privacy, data security, and other important legal considerations is an important mission for any identity system when the goal is to achieve critical mass and adoption. To this end, the SelfKey architecture is designed in such a way as to be decentralized, to be globally accessible, and to be compliant with regulatory rules, in particular with data privacy laws. This is accomplished through a flexible, user driven approach which does not force a user to store their documents in any one particular storage system and which always requires the consent of an identity owner to trigger identity transactions.

At all times identity owners are in control of their identity, relying parties can more quickly access the validated identity claims and verifiers can receive

payment for their contributions and attestations. This flexible and user driven framework can help meet various country requirements for transfer of data overseas.

As the identity system may evolve and change due to legal and technology constraints-there should be a guiding ethos which is flexible in some regards (such as storage layer, or what - if anything, is hashed to the blockchain as a timestamp) but rigid in others, such as the preservation of individual rights and self-sovereign identity. To that end, the following are the principles of the constitution of the SelfKey Foundation.

The SelfKey Foundation

These constitutional principles are literally baked into the very governance and control mechanisms of the SelfKey Foundation. Violating these principles would be contrary to the constitution which makes these principles technically and legally binding.

Existence. Users will always have an independent existence. Any self-sovereign identity is derived from a proof of life. In order to further that the kernel of self that is upheld and supported, SelfKey endeavors to design our system to exist beyond any one national system, and instead of placing a priority on any one nation state-instead makes the most important participant in our system the individual natural living person.

Control. Users always maintain complete control of their identities. The user is the ultimate authority on their own identity. Users are able to reference their identity, update it, or even hide it or have it disappear. Users are able to choose publicity or privacy at their individual preference.

Access. Users have access to their own data. They can easily retrieve all the claims and other data. In other words, the network will not allow for hidden data about a user. This does not mean that a user can modify a claim solely at their own discretion - however, users will be aware of any claims about their identity.

Transparency. Systems and algorithms owned and operated by SelfKey are transparent and open source, in both how they function and in how they are

managed and updated. The foundation which manages the system is transparent.

Persistence. Identities are persistent and long-lived. Private keys may be lost, and might need to be rotated and data might need to be changed, but the identity should persist and remain.

Portability. All information will be transportable and not held by a single third-party entity, the identity owner remains ultimately in control of their identity.

Consent. Identity owners must consent to any transfer or use of their data.

Minimization. Disclosure of claims must be minimized. When data is disclosed, that disclosure should involve the minimum amount of data necessary to accomplish the task at hand. The minimum amount of user information is only exposed to the right entities under the right circumstances.

Protection. When a conflict occurs between the needs of the identity network and the rights of individual users, the SelfKey network will preserve the freedoms and rights of the individuals over the needs of the network. Identity authentication will occur through independent algorithms that are censorship-resistant and force-resilient and run in a decentralized manner.

Interoperability. SelfKey aims to be interoperable. The inherent persistence of censorship blockchain and autonomy of private keys and self-sovereign identity ensures wide and continuous availability, in a wide range of industries. Efforts are made to ensure interoperability with other identity systems.

These principles are part of the Foundations' constitution and members or the board elected by members can only pass a resolution or action which is in accordance to these principles.

SelfKey Technology Stack

Validating Nodes- At the core level of our system are validating Ethereum nodes. We have considered using the Ethereum "proof of authority" at this level, but have opted to use the normal consensus mechanism of Ethereum and

only change if there is any issue. In testing, we have used the EVM, Eris, Monax, and Tendermint consensus protocol, and alternative blockchains remains an option for SelfKey in the future should the Foundation board determine this as the best course of action. We found a public blockchain was the fairest, most inclusive, and well adopted blockchain currently existing.

Blockchain Layer – SelfKey key pairs are from the Ethereum Public network.

Storage - As there are challenges in compliance in an international system of identity, we have made the storage layer entirely up to the discretion of the identity owner. Documents will sit locally on the device of the user until when (at their consent and discretion) the identity owner moves the documents or data elsewhere. Later, storage drivers will be built for user controlled storage.

Key Management / Recovery

It is inevitable in a user managed identity system based on blockchain keys - that some users will misplace or lose their keys. In such a case, if there was not a way to recover the key - then all the attestations would be lost. Fortunately, we have developed a solution. SelfKey plans to use Uport, a convenient key recovery mechanism, whereby a user can delegate the responsibility of recovery to one or more accounts of their choosing. Uport will provide interoperability and build on standards which the Ethereum community already acknowledges and accepts.

The proxy contract Solidity code is very simple, and is presented here for reference:

```
contract Owned {
    address public owner;
    modifier onlyOwner(){ if (isOwner(msg.sender)) _ }
    modifier ifOwner(address sender) { if(isOwner(sender)) _ }

    function Owned(){
        owner = msg.sender;
    }

    function isOwner(address addr) public returns(bool) { return addr == owner;
}

    function transfer(address _owner) onlyOwner {
        owner = _owner;
    }
}

contract Proxy is Owned {
    event Forwarded (address indexed destination,uint value,bytes data);

    function forward(address destination, uint value, bytes data) onlyOwner {
        if (!destination.call.value(value)(data)) {throw;}
        Forwarded(destination, value, data);
    }
}
```

Protocols - In order to make the SelfKey network maximally interoperable, a number of standards and ongoing work will be dedicated to the protocol layer. This is how data will move in a structured format between one place and another (potentially one blockchain to another). Work is being done in this area with other leading identity systems to ensure interoperability; Sovrin, W3C, Uport, etc.

ID wallet - The SelfKey identity wallet is available upon launch and is the starting point for all identity transactions. The wallet can also store KEY.

Through the identity wallet the user can also access different apps in the application layer. Any company can build in this application layer. Any identity provider might also make interoperable their set of keys or certificates, for instance various x509 certificates which qualify under an arbitrary government electronic transaction ordinance.

ID Microservices – The microservices layer will largely allow for compliance with international laws and regulations, and will be used mostly by verifiers and relying parties. Any company might provide these microservices, but to support the initial application layer and several ICO's which will leverage the SelfKey System, KYCC has built and provided some initial microservices such as sanction list screening (the remediator), company registry lookup, and document collection and validation (the collector).

Application Layer – Any application can be built on the SelfKey platform as it has open API's, open source code, including the wallet which is completely open source.

Advantages of the SelfKey network over traditional identity systems

There are numerous benefits available to all parties of an identity ecosystem including identity owners, relying parties and verifiers, who each have different agendas. The chart below should demonstrate that a decentralized identity system can be beneficial for all parties.

Centralized Traditional Identity Systems	**Decentralized Identity System of SelfKey**
Identity Owners	
-do not own or control identity -need to repeatedly go through numerous onboarding processes to satisfy regulators -need to keep multiple authentication devices on hand for a login process -are unable to port information easily from one service to another (high switching costs) -must share identity documents, and cannot share only a minimum of information -only exist to relying parties under the permission and authority of a government -cannot re-use or recycle the output of an identity or KYC process -cannot easily manage company documents or gather signatures for important decisions	-have full consent and control of their identity -authenticate at multiple services through a single key pair stored in a wallet -can share a minimum of information -can recover a lost key -can access a marketplace of fintech products and identity services -can easily sign documents and reach consensus as a company
Verifiers	
-do not monetize identity claims (i.e. utility company). -are unable to revoke a claim -cannot quickly grant claims -identity claims are sometimes fraudulent	-can monetize identity claims through KEY -can revoke claims -can quickly grant claims -claims issued have more confidence
Relying Parties	
-must spend a lot time and effort onboarding clients to satisfy regulatory requirements -have annoying onboarding experiences where customers have an unsatisfactory experience -no way to import customer data -costs a lot of money to validate KYC -costly and challenging to be internationally compliant -processes are driven by paper based and manual effort by compliance teams	-can quickly onboard identity owners -can delight clients -can request additional client details easily -can benefit from economies of scale -can be internationally compliant -processes are driven by KEY and checked by RP's
Overall system features and benefits	
-Vast amounts of data sits in a large silo -reward for hackers is greater, thus bigger target -proprietary and secretive -creates monopolies of data -less likely to be interoperable with others -no value returned to the user -owned and controlled by a single party	-distributed network allows for multiple small storages -reward for penetration is lower -User centric and driven -Open Source -No single point of failure -No centralized management or control

-single point of failure -has traditionally led to massive data loss, instances of fraud, and is holding back the world from self-sovereign digital identity	-Better suited for an international context -More transparent

The KEY token

KEY will be critical to running the ecosystem as all products and services are available through some nominal payment in KEY, which will be used to power the 'identity ecosystem' through a variety of actions. For instance, KEY can be used, to do things such as pay for request attestations; receive identity claims (and give value back to user); pay for marketplace listings; and generally, to exchange value, incentivize use and adoption and allow access as a token.

As shown in the diagram below, each member of the ecosystem has a valuable role to play in encouraging system use, utilizing KEY, and providing identity proofs and attested claims. The below is not an exhaustive list of the uses of KEY – but it should be clear that there is abundant token utility from the launch of the network, and unlike many other tokens, KEY has intrinsic value.

Use of KEY Tokens

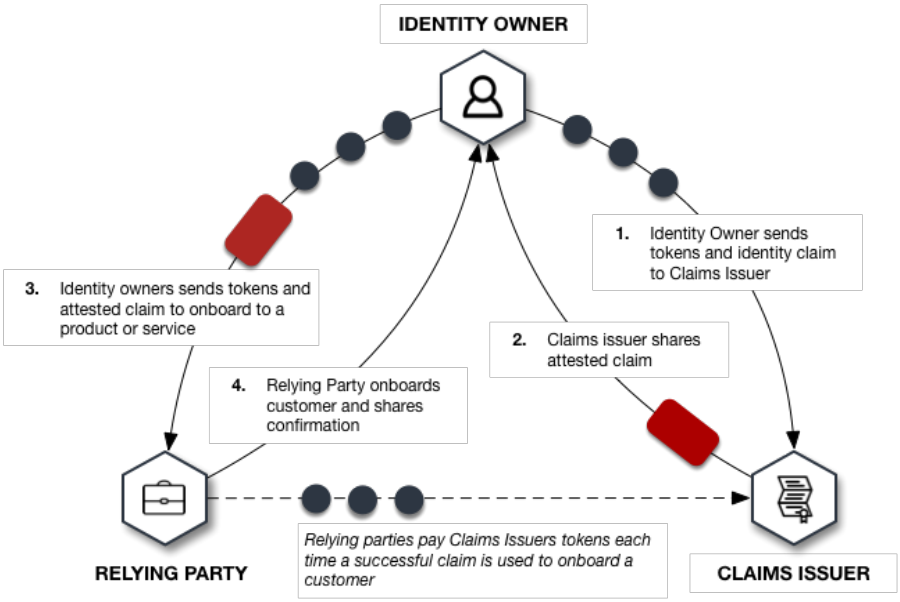
At the launch of the SelfKey network, the following services will be available:

- Bitcoin and Digital Asset Exchange Signup
- Citizenship by Investment programs
- Citizenship through Investment in Real Estate Applications
- Company incorporation (including companies limited by shares, foundations, LLC's and Trusts)
- Bank account introduction and application
- Residence Permit Applications for more than 50 countries
- E-Wallets or Stored value facilities
- Gold and Precious Metals purchase and storage
- International insurance applications
- Money Remittance & Transfer services
- Token Sales

Within this ecosystem, only three parties exchange value. Identity owners, relying parties and verifiers.

SelfKey will have a trust framework which will be signed by Relying Parties, Identity Owners and Verifiers. "Trust frameworks are not a new concept. They are commonly used both inside and outside of the world of digital identities. Mostly they are used to govern a variety of multi-party systems where participants desire the ability to engage in a common type of transaction with anyone of the other participants, and to do so in a consistent and predictable manner. In such cases, they are proven to work and scale." [xxii]

The SelfKey trust framework will include specific protocol level information but also information about KEY in order to properly incentivize good behavior. It is expected that Identity Owners, Verifiers and Relying parties will sign this trust framework which can help incentivize proper use of the network. These documents will be released approaching public launch of the network and with community feedback.



Looking to the future

Our working assumption is that it is very difficult to develop a system which will be compliant with all data privacy laws in every jurisdiction. Therefore, the identity owner is in charge of where their data is stored, and all actions are driven by the identity owner.

Importantly, personal data and identity data are kept out of the transaction ledgers altogether by replacing them with an encrypted reference to the data – a "hash". These hashes or 'fingerprints' help the identity owner prove that data did exist at a certain date, but without the identity owner sharing the actual identity claim - the data on the chain is completely anonymous and obfuscated. The use of hashes also helps address the fact that blockchain technology is structured to keep a permanent, immutable record of all transactions that have taken place, meaning that in theory there can be no "right to be forgotten" in the context of blockchain. Data protection laws the world over require that personal data only be kept for so long as there is a purpose to do so. We believe that encryption controls limiting the accessibility of personal data hashed in the blockchain is a viable solution for data protection compliance. It is true that encrypted personal data may still be classed as personal data in some jurisdictions as long as the holder possesses the encryption key. However, if it can be demonstrated that the keys will only be made available in circumstances dictated by the individual, then it is difficult to see the objection from a data protection perspective.

Data will flow from one place to another through Https, and work is being done on P2P messaging protocols, and pairwise encryption methodologies for data transfer. Essentially, the layperson can rest assured that: 1. Data only moves upon consent. 2. Data Privacy is paramount and data is never shared by the foundation with anyone 3. Each identity transaction uses encryption 4. Data does not move through the blockchain, per se - and happens mostly outside "off-chain" through various encrypted messaging and structured data protocols.

The blockchain will have hashed the data and is stored it in a way that it can be proven that the data has not changed. This timestamping mechanism is critical in certain situations to prove timeliness of documents. Care will be taken so that data is not correlated or causes a loss of privacy.

SelfKey Wallet

The Wallet (where the user will store and manage their ID attributes and claims) is available immediately and is open source, available on desktop for Mac, Linux and Windows. The SelfKey roadmap and immediate deliverables call for this wallet to be available on mobile.

SelfKey Ecosystem

The SelfKey Identity Ecosystem is another major component we will be working to improve. SelfKey includes 3 primary parties 1) the identity owners, 2) relying parties and 3) verifiers (or original claims issuers). SelfKey will engage on a tripartite marketing development push to get all of these parties on the network.

SelfKey Marketplace

The marketplace is a key component to the SelfKey ecosystem as it allows for identity owners to see which relying parties are using the SelfKey system. In the marketplace, identity owners can browse various financial offers and place an order for a particular product. Relying parties / service providers can list offers in the marketplace either free or for a fee. As the marketplace is two sided, KEY can be used as the main token or commodity to interchange value.

SelfKey Data minimization

One of the key aspects of the system is data minimization, or in other words - Identity Fragments. This will allows the identity owner to provide as little amount of information as possible to satisfy the relying party or verifier. While this can be done through advanced technology such as range proofs or zero knowledge proofs (ZKP's) it can also be done through specific protocols or identity fragments. A person could for instance, prove their residency was in Singapore - without revealing their exact address. This can be accomplished immediately through proper design and doesn't require a long development process of ZKP's. A portion of the funds received in the fundraiser will go towards data minimization.

SelfKey Proof of Individuality (Biometric Research)

As our first founding principle is existence, an important element of the SelfKey project is that a persons' identity does not *start* with a government issued identity document but rather with a human life. In order to do this, a certain amount of research will be done on Proof of Individuality (POI) so that anyone, anywhere is able to prove themselves to be alive at a given time, and gain certain access to the SelfKey network. A separate whitepaper has been written about this process and will be released when the POI validation and

testing begins in earnest. We believe that POI can be better solved with biometrics than what is currently being proposed in the Ethereum community – a series of video calls. Furthermore, the foundation will issue grants to try and do a purely biometric based key recovery mechanism, so that if you lost your keys, all one would need is not a complex brain password, but yourself.

The SelfKey team

The project team of SelfKey encompasses a group of highly experienced innovators who are passionate about identity and its future, as well as some of the industry's brightest legal and business minds. Full details at www.SelfKey.org

Conclusion

SelfKey proposes a self-sovereign identity system as the best model for our evolving global society. SelfKey is a distributed key management and recovery system, a privacy preserving protocol based on verified claims compatible with W3C in a JSON-LD compatible format, powered by a fully decentralized blockchain, and developed by a non-profit foundation with distributed governance. Inscribed in the forecourt of the Temple of Apollo at Delphi, around 3000 years ago: γνῶθι σεαυτόν, or when translated into English; know thyself. It is as clear now as it was then, you are the person best suited to manage your identity. As we enter into a world that is increasingly digital, our lives will move in unimagined ways onto public Internet infrastructure. Our digital identity is at risk and not currently owned by identity owners.

Self-Sovereign identity on blockchain keys is only a partial solution, but in this paper the SelfKey Foundation has proposed a distributed technology, legal and governance ecosystem for you to truly own your own identity.

[i] "What is web 1.0?" *Techopedia*. Accessed August 3, 2017, https://www.technopedia.com/definition/27960/web-10.

ii "Instead of merely reading a Web 2.0 site, a user is invited to contribute to the site's content by commenting on published articles or creating a user account or profile on the site…The unique aspect of this migration… is that customers are building… business(es) for [corporations]," Quotation from article entitled "Web 2.0," *Wikipedia,* Accessed August 3, 2017, https://en.wikipedia.org/wiki/web_2.0.

iii Rob Marvin, "Blockchain: The Invisible Technology That's Changing the World," *PCMag*, published august 2, 2017,https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor.

See Also:

Adam tinworth, "Next16: Blockchain Will Build Web 3.0, Says Jamie Burke," *Next Conference*, Published September 23, 2016, https://nextconf.eu/2016/09/next16-blockchain-will-build-web-3-0-says-jamie-burke/.

Sirikiat Bunworaset, "Web 3.0: Ethereum Will Change Everything," *Bangkok Post*, Published June 20, 2017, http://www.bangkokpost.com/business/news/1272219/web-3-0-ethereum-will-change-everything.

Los Silva, "Web 3.0: How Decentralized Applications Are Changing Online Censorship," *Ethnews*, Published February 5, 2017, https://www.ethnews.com/web-30-how-decentralized-applications-are-changing-online-censorship.

Tristan Winters, "Web 3.0 – A Chat With Ethereum's Gavin Wood," *Bitcoin magazine,* Published April 25, 2014, https://bitcoinmagazine.com/articles/web-3-0-chat-ethereums-gavin-wood-1398455401/.

"The Blockchain the New Web 3.0," Accessed August 3, 2017, https://www.moneyoip.com/new-web-3-0.

iv "The right to an identity – the global situation," *Humanium,* Accessed August 3, 2017, http://www.humanium.org/en/world/right-to-identity/.

v Jean Camp, "Identity in Digital Government: A report of the 2003 Civic Scenario Workshop," (An Event of the Kennedy School of Government, Harvard University, Cambridge, MA, 02138, April 28, 2002) http://www.ljean.com/files/identity.pdf.

vi Ben Schiller, "2 Billion People Are Still Left Out Of The Modern Financial System: How Quickly Can We Change That?," *Fast Company,* Published November 3, 2015, https://www.fastcompany.com/3051846/2-billion-people-are-still-left-out-of-the-modern-financial-system-how-quickly-can-we-change.

vii Ravi Raja Konathala, "What are the privacy issues with Aadhaar?", *Quora* (question-and-answer forum), April 5, 2017, https://www.quora.com/what-are-the-privacy-issues-with-aadhaar.

viii Equifax shares drop as questions mount over data breach https://www.ft.com/content/f503ef3c-94b2-11e7-a9e6-11d2f0ebb7f0

ix Tech2 News Staff, "Massive Swedish data breach reveals Swedish military secrets and the identity of almost all its citizens," *Tech2*, Published July 26, 2017, http://www.firstpost.com/tech/news-analysis/massive-swedish-data-breach-leaks-swedish-military-secrets-and-the-identity-of-almost-all-its-citizens-3855113.html

xi "A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity," *World Economic Forum*, Published in August 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

xii "Data Breach Tracker: All the Major Companies That Have Been Hacked," *Time*, Published October 30, 2014, http://time.com/money/3528487/data-breach-identity-theft-jp-morgan-kmart-staples/.

xiii Ambrose McNevin, "The five biggest issues in identity management and what's behind them," *Computers Business Review*, Published May 20, 2016, http://www.cbronline.com/news/cloud/the-top-five-issues-in-identity-management-4899761/.

xiv see subheading "KYC-Chain" under heading "Use cases:", *Un-Blockchain,* https://un-blockchain.org/use-cases/identity-under-construction/.

xv Wikipedia contributors, "Semantic Web," Wikipedia, The Free Encyclopedia, Accessed August 3, 2017, https://en.wikipedia.org/w/index.php?title=Semantic_Web&oldid=793179594.

xvi Nitasha Tiku, "Digital Privacy Is Making Antitrust Exciting Again," *Wired*, Published June 4, 2017, https://www.wired.com/2017/06/ntitrust-watchdogs-eye-big-techs-monopoly-data/.

xvii "Blockchains and Laws. Are They compatible?", *Baker McKenzie* in collaboration with *R3*, Accessed August 3, 2017, http://www.bakermckenzie.com/en/-/media/files/expertise/fig/br_fig_blockchainsandlaws_jul17.pdf.

19 "Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity," Press Release, *Thomson Reuters,* Published May 09, 2016, https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html.

xix Gabriella Jóźwiak "KYC leads to Financial Exclusion", *The Guardian*, Published February 2015.

xx Nigel Cory, "Cross Border data flows where are the barriers and what do they cost?", *Itif*, Published May 7, 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost May 1, 2017.

xxi "RegTech for Know-Your-Customer Procedures: Enabling & Operating on Blockchain Technology," Published 2016, http://www.sec.or.th/fintech/Documents/KYC.pdf.

xxii http://www.openidentityexchange.org/blog/2017/06/22/trust-frameworks-for-identity-systems-2/