“SelfKey” : Self-Sovereign Digital Identity Ecosystem

Sravya Jarugu

Akshay Mukkavilli

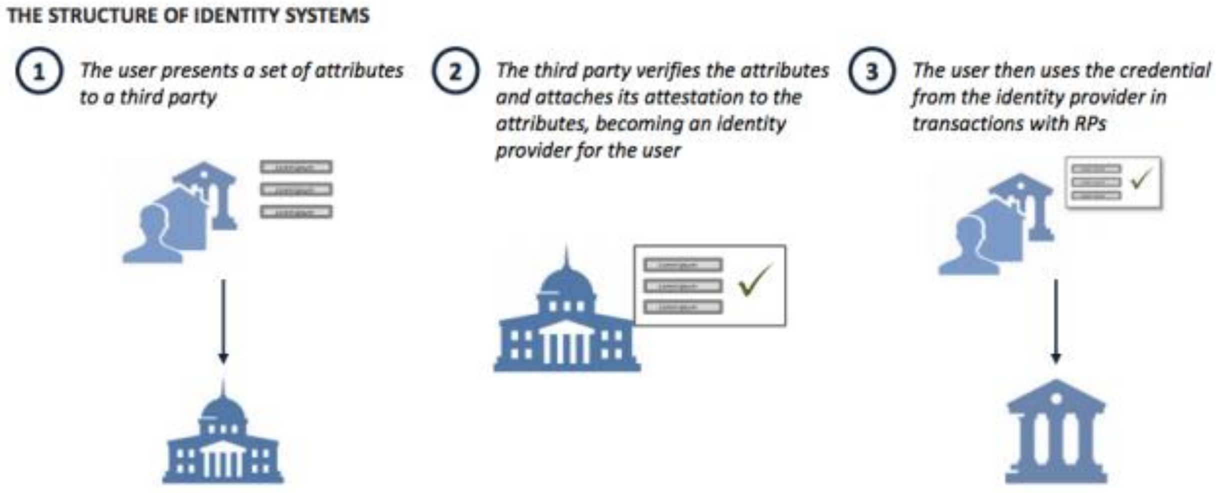
Mounika Mekapothula

Sai Kiran Reddy Gade

Problem: You do not own your own identity:

The shift from paper to digital computing and Internet are some of the most fundamental changes of recent modern history. Despite the advancements, the identity systems we rely upon today are currently paper-based, nationally-driven, government identity systems and do not leverage the power of Internet. 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. Many centralized identity systems have very serious security issues. 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.

Parties in an Identity Transaction:


THE STRUCTURE OF IDENTITY SYSTEMS
1 The user presents a set of attributes to a third party
2 The third party verifies the attributes and attaches its attestation to the attributes, becoming an identity provider for the user
3 The user then uses the credential from the identity provider in transactions with RPs

1. Identity Owner
2. Identity Claim Issuer
3. Relying Party

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.

Limitations of a centrally managed identity system: KYC Laws and Regulations

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, nonprofit foundations, professional service providers, notaries, governments, insurers, re-insurers, financial institutions, and generally any legal entity or natural person dealing in money or finance.

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. 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:

idea is simple: that users should be at the center of their identity management process, a concept known as Self-Sovereign IDentity (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.

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.

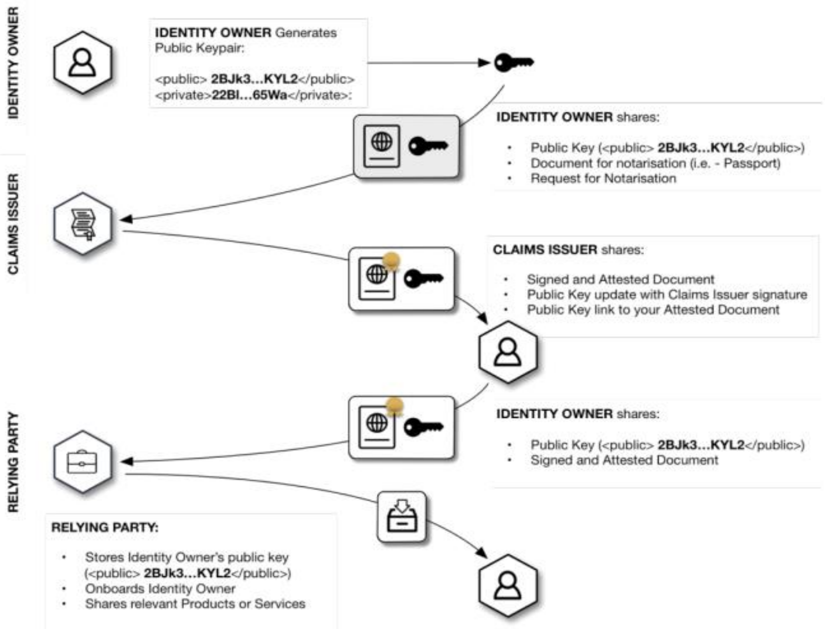
How SelfKey works for the individual user:

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.

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.

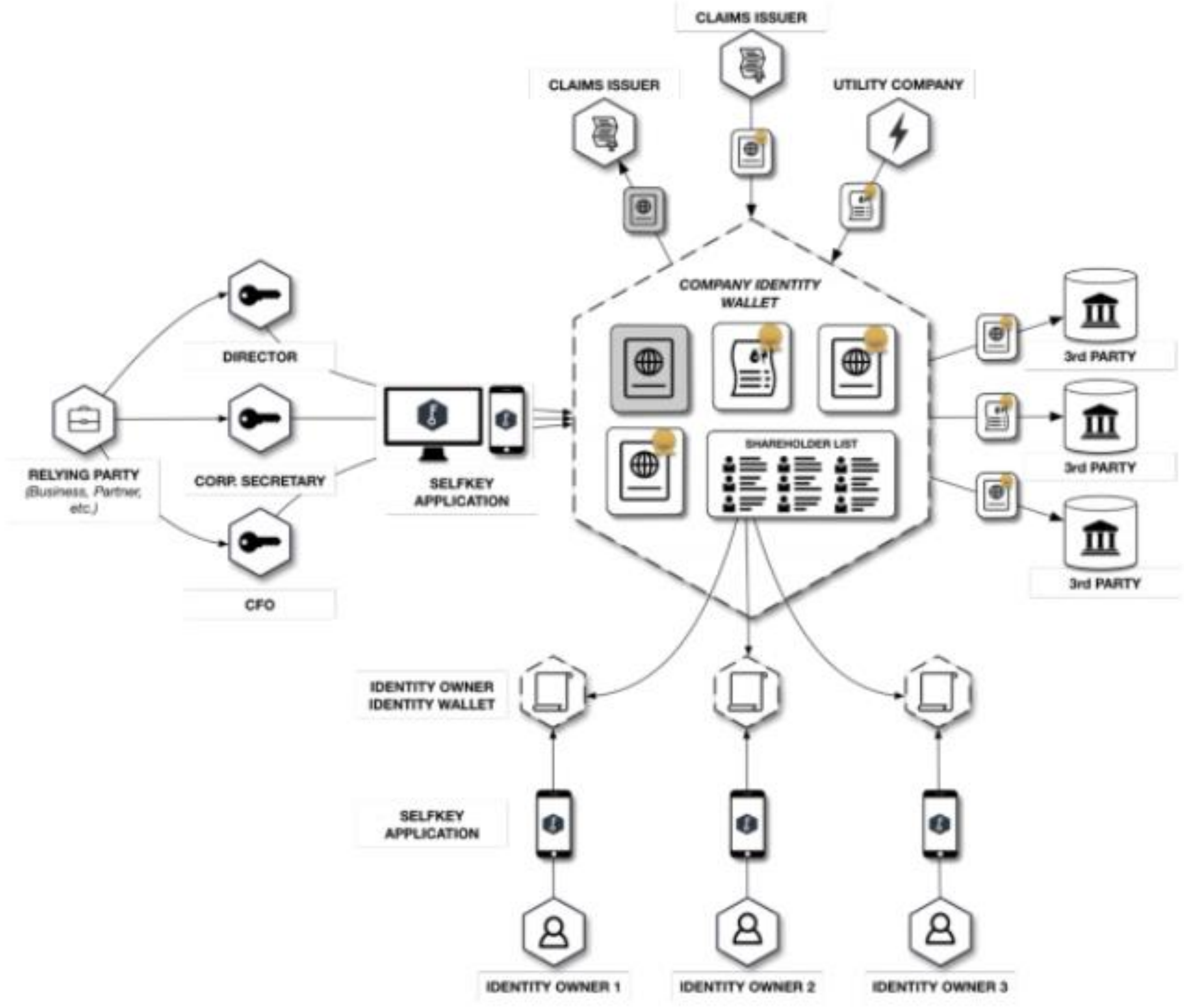
Once the identity claims have been created, the next step in the process is to receive attestations of these claims. Attestations can be stored in the SelfKey wallet too. These attestations are machine readable, digitally signed identity claims, which can also be valid within certain time windows. The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


IDENTITY OWNER
IDENTITY OWNER Generates Public Keypair:
<public> 2BJk3...KYL2</public>
<private>22Bl...65Wa</private>:
IDENTITY OWNER shares:
• Public Key (<public> 2BJk3...KYL2</public>)
• Document for notarisation (i.e. - Passport)
• Request for Notarisation
CLAIMS ISSUER
CLAIMS ISSUER shares:
• Signed and Attested Document
• Public Key update with Claims Issuer signature
• Public Key link to your Attested Document
IDENTITY OWNER shares:
• Public Key (<public> 2BJk3...KYL2</public>)
• Signed and Attested Document
RELYING PARTY
RELYING PARTY:
• Stores Identity Owner's public key (<public> 2BJk3...KYL2</public>)
• Onboards Identity Owner
• Shares relevant Products or Services

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.

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)



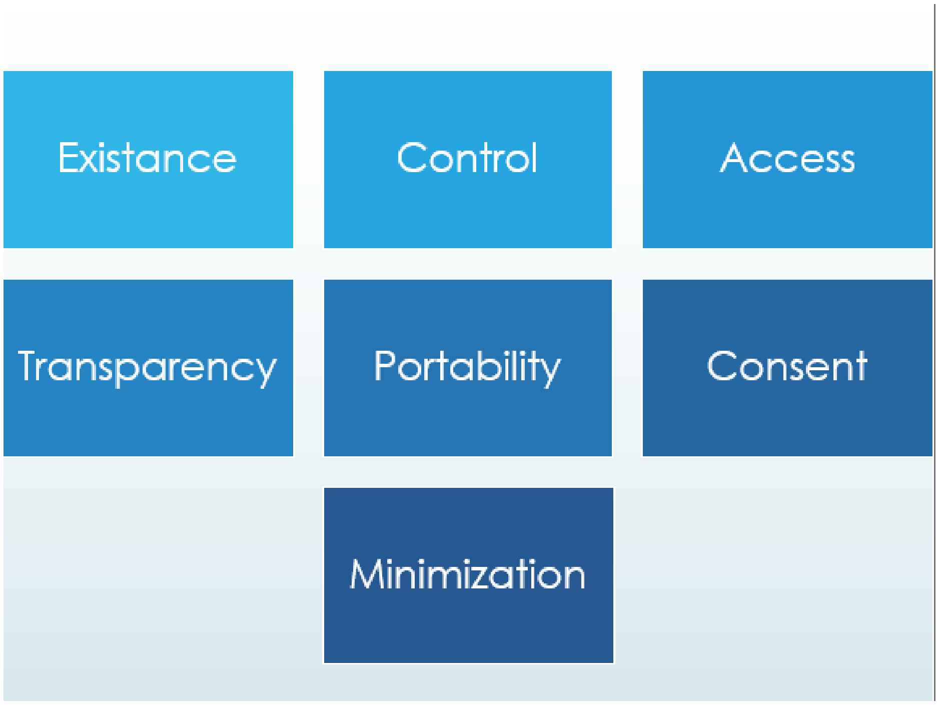
How SelfKey works for a verifier

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.

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.



Existance

Control

Access

Transparency

Portability

Consent

Minimization

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 disappeared. 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.

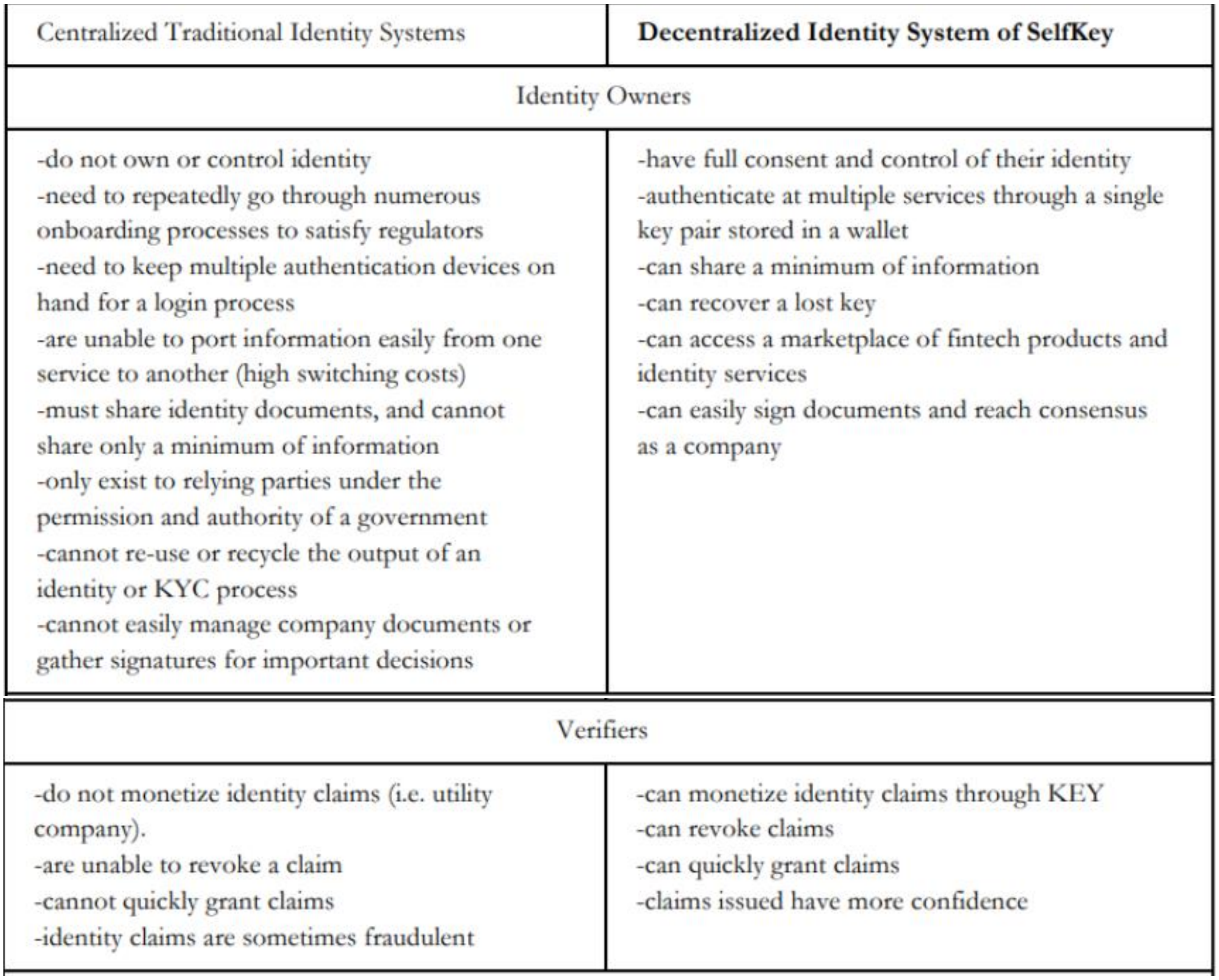
Consent: Identity owners must consent to any transfer or use of their data.

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.

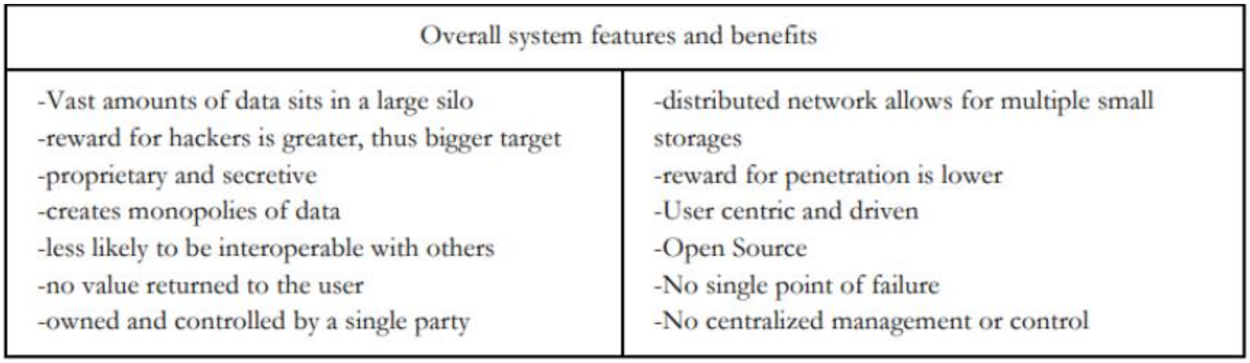
Protection: When a conflict occurs between the needs of the identity network and the rights of individual users, the SelfKey network will preserve the freedoms and rights of the individuals over the needs of the network. Identity authentication will occur through independent algorithms that are censorshipresistant 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

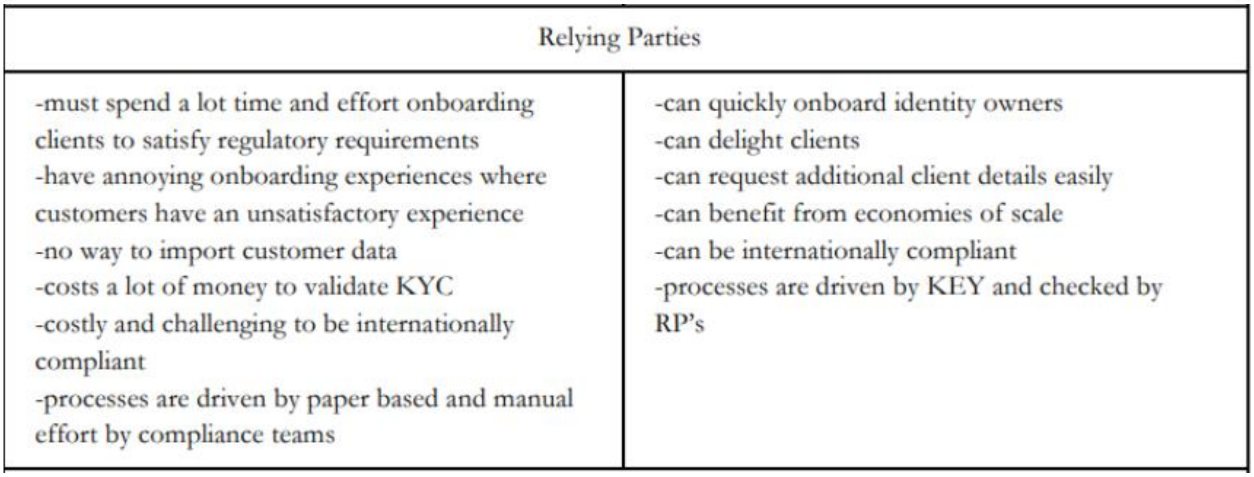
Adavntages of SelfKey over Traditional Ecosystems:



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



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



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

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 a 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.

References:

1. https://www.investinblockchain.com/cryptocurrency-projects-march-2018/
2. https://selfkey.org/
3. https://icodrops.com/selfkey/