IDEAS
Identité **DE**léguée **A**uto-**S**ouveraine

Self-sovereign Delegated Identity

April 19, 2017

Rebooting Web of Trust Conference, Paris

Author: Pierre Noizat

The goal of IDEAS is to combine the benefits of sel-sovereign identity with those of delegated identity. While this may sound like an oxymoron at first, this draft paper shows that trusted third parties can indeed complement a self-sovereign identity system where the user retains optimal control over her personal data.

To achieve this goal, IDEAS leverages three main properties of the Bitcoin network:

1) **Security**: By definition, Bitcoiners carry a Bitcoin wallet i. e a secure keychain: they are incentivized to keep their private keys secure by the monetary amount that they control. In a way, the security of their key chain is subsidized by this monetary incentive. Most previous identity systems run without obvious economic incentive for security, a shortcoming that too often leads to careless key management.

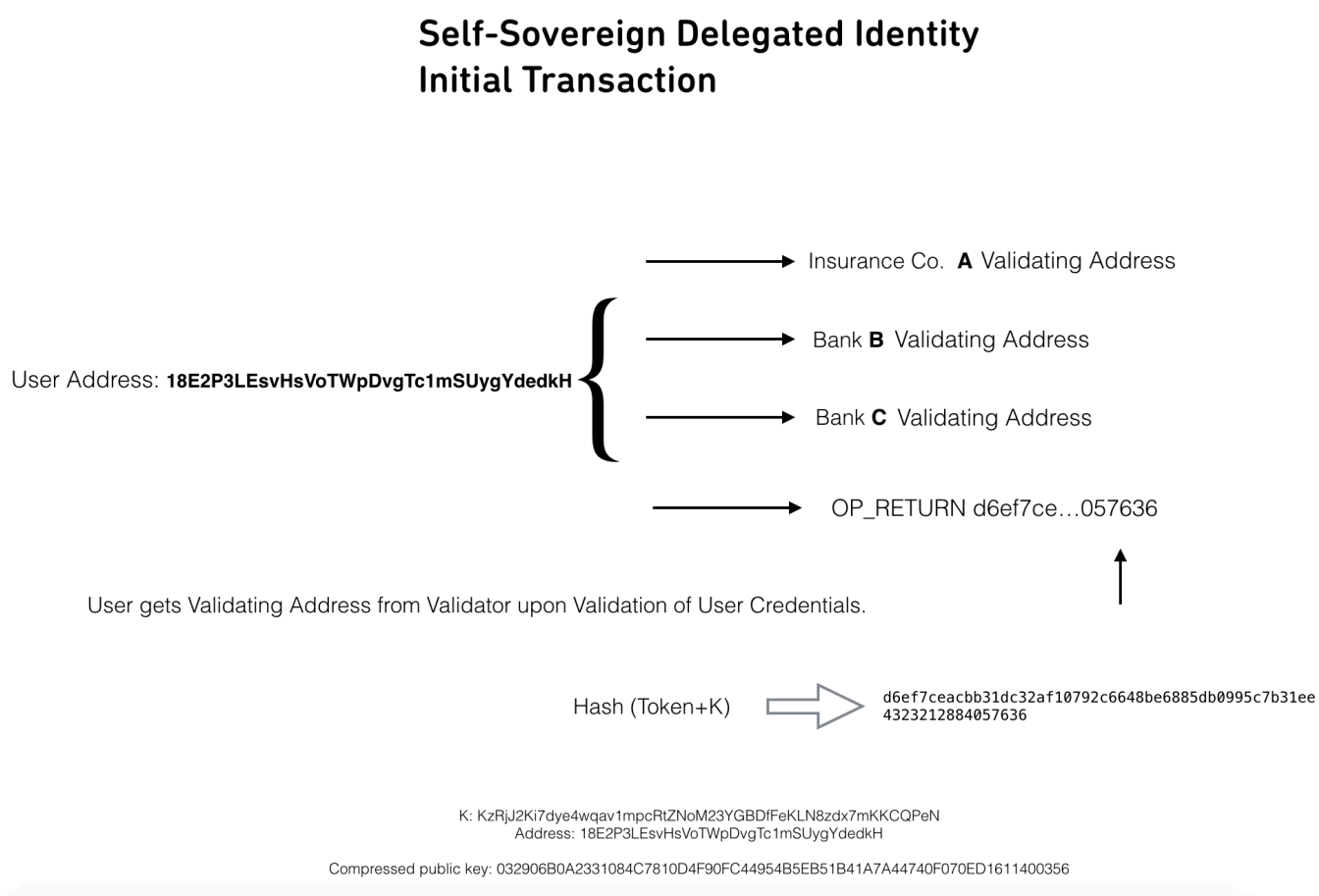
2) **Optimal Security/Convenience Tradeoff**: In a few years, Bitcoin has grown from zero to millions of users worldwide. A blooming eco-system of developpers, infrastructure and applications enables users with a wide range of options to manage their keys: stand alone (full node) wallets, hosted wallets and many shades of wallets in between these two extremes, including light clients (SPV wallets) and multi-signature wallets. Because Bitcoiners can use their wallets on a regular basis for financial transactions, they are more likely to find it convenient and use it for signup/signin transactions. Other identity systems dealing only with identity struggle to find the proper security/convenience tradeoff. Secure and inconvenient, nobody uses them. Convenient and insecure, they are useless for secure applications.

3) **Secure Timestamping**: IDEAS leverages the Bitcoin network as a public, secure timestamping (distributed) server. Because all initial setup and validating and transactions are dated and ordered in the Bitcoin blockchain, a compromised key can be revoked simply by publishing and validating a new key, making the compromised key obsolete. In contrast, key revocation is often a pain point in other identity systems, in terms of implementation cost and user experience.

How does it work ?

IDEAS user experience unfolds in three phases: setup, validations and signup/signins.

Initial (setup) transaction:



Alice decides to create an identity based on a self-generated address (e.g 18E2P3LEsvHsVoTWpDvgTc1mSUygYdedkH) including a set of credentials of her choosing (e.g. First Name, Last Name, DOB, Citizenship, Social Security Number).
Address here and in the rest of this document means compressed Bitcoin address.
IDEAS identifiers are compressed Bitcoin addresses.
Alice computes a hash of her identity as Token = H(Credentials)

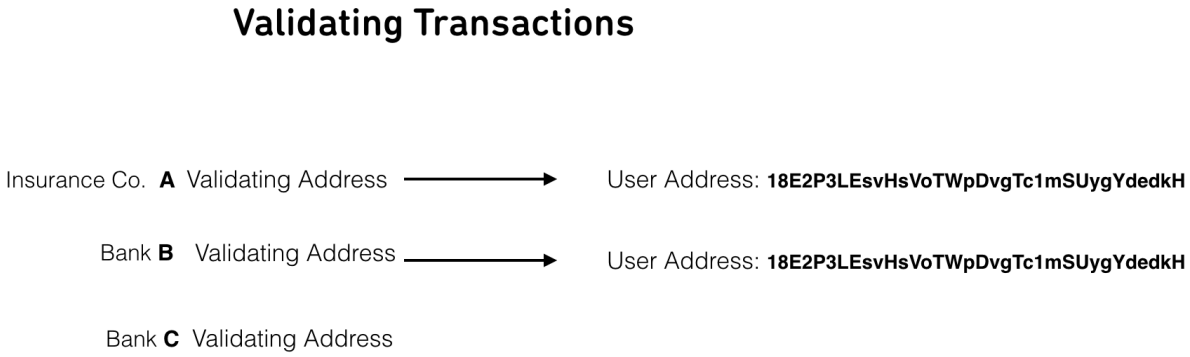
Alice selects a set of validators, supporting IDEAS, to endorse the validity of the above credentials.
User gets validating address from validator upon validation of her credentials.
For instance, if Alice is customer of bank A, she can request a unique validating address from bank A as a byproduct of the customer due diligence process (KYC) performed by bank A.

Alice links her IDEAS identitfier (18E2P3LEsvHsVoTWpDvgTc1mSUygYdedkH) to her validating addresses by sending micropayments to those in a transaction that will include also an OP_RETURN output showing a hash H(Token + K) where
Token is a hash of her identity, Token = H(Credentials) and
K (KzRjJ2Ki7dye4wqav1mpcRtZNoM23YGBDfFeKLN8zdx7mKKCQPeN) is the (WIF compressed) private key matching her IDEAS identifier.

Alice uses her IDEAS identifier as the sole input of this transaction, thereby logging in the Bitcoin blockchain a cryptographic proof of her selection of validators.

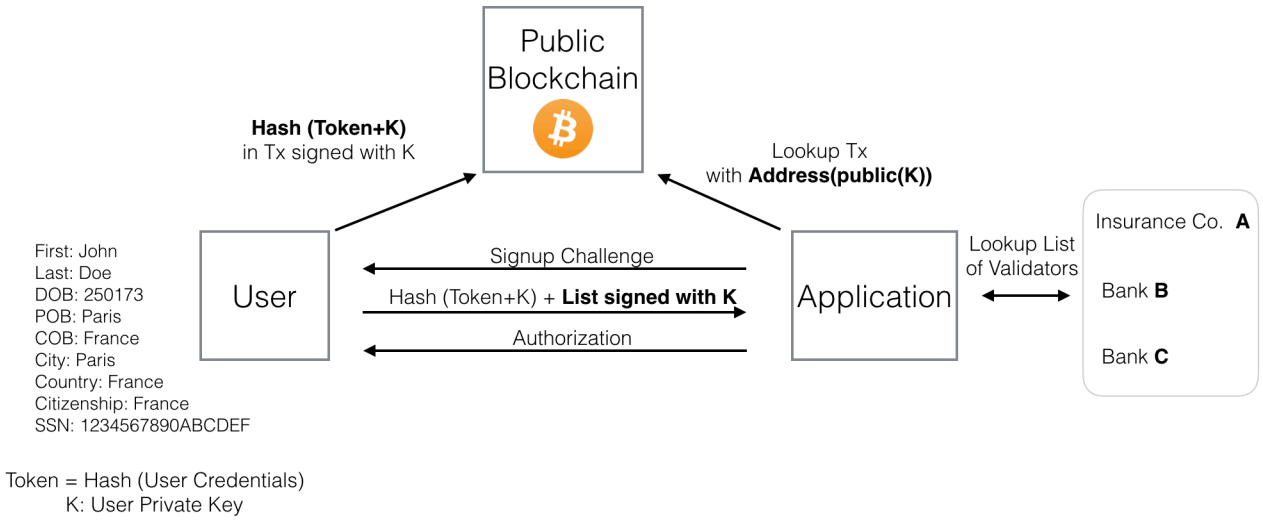
Validations:

Validator broadcasts validating transaction after or upon validation of user credentials, sending the micropayment back to her IDEAS identifier, possibly with a premium to incentivize user registration.



Signup:

An application supporting IDEAS must have access to a list of trusted IDEAS validators.
The application must also have access to the Bitcoin blockchain, either directly or through a blockchain API, to search transactions by addresses.
The application shall display a signup challenge consisting of a list of credential items requested by the application.
Alice shall respond with a list signed with K, signed list containing
a list of validators and
a list of credential items that can be provided by the validators with her consent

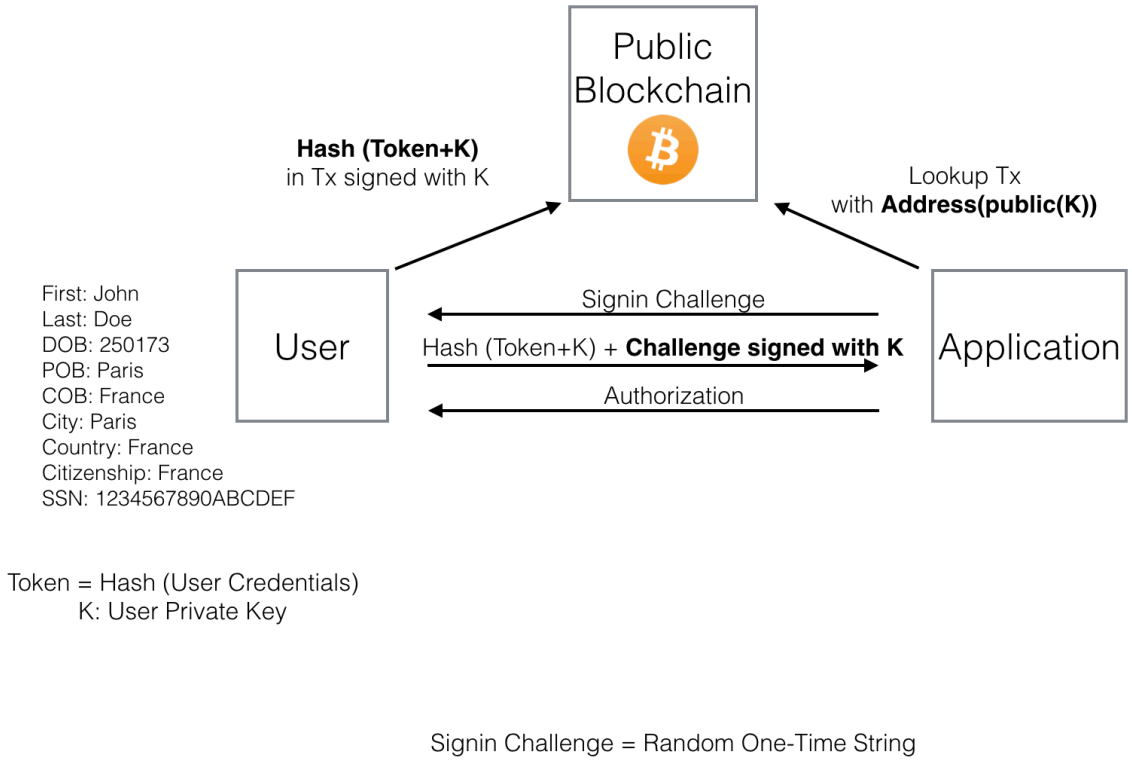


Signup Challenge = List of Credential Items asked by the Application

List signed with K =
List of Validators + List of Credential Items that can be provided by Validators with Consent of User

Signin:

The application shall display a signin challenge as a random one-time string that Alice shall respond to with her signature using K.



Business Model:

IDEAS proposes a viable business model for validators.
Users could be incentivized by a trusted validator to register with them because the validating transaction can send back an economic incentive added on top of the user micropayment.
Validators can earn new revenues from fees charged to applications for each validated signup.
Applications can save on customer acquisition costs by relying on validators for customer due diligence.

Scalability:

The Bitcoin protocol allows for only one OP_RETURN output per transaction.
This could set za limitations to adoption.
Fortunately, a protocol upgrade is on the roadmap of the reference implememtation (Bitcoin Core, version 0.13.1 and up).
The so-called segregated witness (SegWit) soft fork (new rule added to the protocol) shall enable the deployment of new scritping capabilities.
In particular, Merkelized Abstract Syntax Trees (MAST) allow transactions with thousands of OP_RETURN type outputs.

In addition, IDEAS could also leverage payment channels such as those envisionned by the Lightning Network developpers, potentially enabling millions of micropayment transactions per second.

Conclusion

In short, IDEAS proposes a Self-Sovereign Delegated Identity system leveraging the Bitcoin network as a resilient, permission-less infrastructure with significant advantages:

- Open set of validators
- User managed privacy
- Apps can pick and chose validators
- Secure timestamping rather than revocation
- New, scalable business models for validators