iquality

Why blockhain technology is needed to bring us self-sovereign identity

Is blockchain just here to lure people and money in, or does it provide fundamental value?

Introduction

Over the course of the last two years, there has been a great deal of interest in what has been coined as 'self-sovereign identity'. Arguably, a blog post by C. Allen in 2016 [ref] started a wave of interest in pushing identity management practices to a new era. In his post, he said "I want to share a vision for how we can enhance the ability of digital identity to enable trust while preserving individual privacy. This vision is what I call "Self-Sovereign Identity".

The keyword here is trust, which is what identity management is all about. To illustrate this statement, let's use the most common example. Say you walk into a liquor store to buy a bottle of wine. The cashier wants to verify that you are over 18, so he asks for identification. In nearly all cases, people will show the cashier their driver's license. Why? Because the cashier trusts that the driver's license agency correctly registers birthdates.

You may be thinking, alright I get that, but can't we do that with current systems? We have Facebook Connect, what do we need blockchain for? While Facebook Connect has gained wide scale adoption, its merits are not aligned with the idea of having individuals enable trust and preserve privacy. What Facebook Connect - and other social media platforms like Google or Twitter - does, is act as a middleman. Users can create an account with Facebook and enrich their profile. This is a direct relationship between the user and Facebook.

But what happens when I use Facebook to log into another website? That website will hand over the authentication responsibility to Facebook. This means that you use your Facebook credentials to log in to the website, and then passing over your personal data from Facebook to the website. This might seem like a well-designed solution, and indeed, the user experience is (nearly) exactly as it should be, simple and fast! The problem however, is that we put trust in Facebook to manage our identity. They control my personal identity, and I have little means to protect my privacy.

So, can blockchain technology be the trust layer?

In short, no, not in and by itself. While blockchain is a term used for multiple technological configurations, at the basis it consists of a distributed ledger, a peer-to-peer networking protocol, and a consensus mechanism. It lets a network of peers transact with each other via one shared database. The unique property is that everyone who connects to the network will have the exact same copy of that database. This is achieved by a consensus mechanism, which - as the name implies - makes sure that all the peers achieve consensus on the state of the database. These properties have multiple advantages; practical immutability, low entry barriers, transparency, and accessibility.

However, there are also drawbacks of using blockchains. Again, drawbacks vary for different blockchain configurations -- for now we will discuss public blockchains such as Bitcoin and Ethereum. In their current development status, they are slow, expensive and not privacy-preserving. On Ethereum, a transaction will take at least 14 seconds to process (in practice, often around 2 minutes), every transaction costs between a few cents to multiple euros, and everyone can see every transaction. In many use cases, and especially for identity management, **blockchain might not seem like a good system to build upon**, right?

But one of the things blockchain does really well, especially in the context of identity management, is provide anyone with a decentralized public key infrastructure (DPKI). A DPKI lets anyone - people, organizations, things - generate cryptographic key pairs, each pair consisting out of a public and private key.

We won’t go in depth about the technical underpinnings of public key cryptography, but the main operations we can perform with these keys are encryption and digital signing. Quick introduction for the non-technical readers; encryption enables you to transform your data into meaningless ciphertext for anyone not intended to read the data, signatures let you prove that a message was sent by you. Public key cryptography has been widely used for decades already. However, we always had to rely on so-called certificate authorities. You can think of **certificate authorities** as organizations who have the power to declare a public key valid or invalid.

This might not make much sense to everyone, but compare this with our Facebook example. Facebook is the certificate authority for all its users. They have the power to declare your account valid or invalid. The problem with certificate authorities, is that they have full control. This is exactly the reason why a blockchain-based DPKI is of vital importance to self-sovereign identity. You must have ultimate control over the administration of your identity. This requires **independent identifier registration**, and a blockchain’s DPKI provides exactly that.

Decentralized identity on the blockchain, how does it work?

Before we dive deeper into how a blockchain-based DPKI is of great value to self-sovereign identity, we should explain a little more about the digital identity ecosystem. It’s important to notice that identity is contextual. You likely have different personas across multiple platforms, each with other data associated to them. This personal data can be about anything; your favorite food, sports preferences, job title, hair color, gender, driving reputation, anything really!

In the identity community, we often talk about three different kinds of stakeholders: issuers, holders and verifiers. Each one of these stakeholders will get a short introduction here.

Issuers are entities that provide other entities with identity information. A very common offline example is the Government issuing you a passport. In online scenarios, this can be any website providing an account to you on their website.

Holders are entities that build a rich identity profile from their interactions with issuers and want to share that contextual (!) identity with other parties. Recall the earlier example where an individual wants to buy liquor, he is the holder of his driver's license, which he uses for proving his age to the cashier.

Lastly, verifiers are entities who wish to provide a service to the holder, but have to verify identity information about that holder first. Each of these different stakeholders - issuers, holders, verifiers - have a unique identifier, registered on the blockchain by using its DPKI. These identifiers are used as a starting point to interact with each other. No single authority other than the identity owner itself is able to revoke that identifier.

All these stakeholders have to exchange data with each other. Issuers have to provide holders with data, holders have to store the data and present it to verifiers, and verifiers have to consume the data and verify it.

In the self-sovereign identity world, we use what are called verifiable credentials. As the term implies, **verifiable credentials** are digital objects which are used to prove contextual identity facts. Issuers can issue these verifiable credentials to holders, who in turn can present them to verifiers. The powerful property is that they are independently verifiable by any third party, the issuer does not have to be contacted. This is achieved by having the issuer sign the credential upon issuing it to the holder. The signing relies upon the key pair, of which the public half is anchored on the blockchain! When a verifier receives a credential and wants to verify it, he uses the public key of the issuer to check if the signature is valid. Only the issuer itself can revoke its public key. This model provides us with a strong identity ecosystem, where each stakeholders is self-sovereign. Everyone is able to make their own decisions, with their privacy preserved.

The way forward

For most of the processes in the self-sovereign identity ecosystem, we do not need a blockchain. For private encounters, where data must not be public, nearly all interactions happen off the blockchain. Only public information, most notably identifiers, are registered on the blockchain. This empowers stakeholders to have an independent existence and removes the need for large intermediaries to manage our identity, such as Facebook Connect.

There are still many hurdles to overcome to materialize this grand vision. There is no ecosystem of issuers, holders and verifiers yet. Managing cryptographic keys is hard. We need a lot of standardization and interoperability. Despite these challenges, the vision of self-sovereign identity management is compelling.

With Purple Unity, we are working on a platform called igree, which aims to help people and business set their first step in the self-sovereign identity ecosystem. Feel free to reach out to us to learn more!

Contact

For more information regarding Igree or related matters, please contact

John van Beek
Managing partner
john.van.beek@iquality.nl