Credit: unisys.com

Blockchain in Telecom - How Blockchain Can Enable Telcos as Identity Service Providers

Published on August 26, 2016

Sawan Kumar | Follow
Senior Consultant (IT Strategy) at Deloitte

👍 6 🗨 2 ➦ 1

(Disclaimer: This post has been heavily influenced by this wonderful thought series by Dave Birch. While the ideas presented there are more centred around financial services, this post has been written with an eye on how Telcos can benefit from the Blockchain + Digital Identity innovations)

The way we currently do identity and authentication management is about to change, thanks to the potential of the blockchain. Currently, digital identity is fractured (multiple third parties store similar attributes) and outsourced (information owned and managed by third parties). This leads to inconvenience and security issues - the inconvenience of remembering many username/password combinations and the security aspect of centralised identity data stored and managed by third parties.

However, there are many parallel on-going efforts aimed at solving some or all of these issues using the blockchain (see Blockstack, Consensys, Factom, BitID, ShoCard).

This post is a thought experiment on how telcos, with their infrastructure and the gold mine of subscriber data that they sit on, can become a major part of the identity service provider story.

A Model for Digital Identity:

When we think of **identity**, we can think of a model that has three different kinds of identity:

1. ***Physical Identity*** - the identity of a person, object or organisation - identified by a fingerprint, DNA, serial number, registration number, etc.

2. ***Digital Identity*** - the identity bound to the physical entity that is entitled to use it. A digital identity can be thought of as a public-private key pair where the private key is linked to only one physical identity but the public key can be used to create many virtual personas. This is the link between the physical and the virtual identities.

3. ***Virtual Identity*** - the identity or persona that is used to interact online. All transactions are between virtual identities.

These can then be encapsulated into the three basic domains of an identity infrastructure:

1. ***Identification*** - binding the physical identity to the digital identity

2. ***Authentication*** - binding the digital identity to a person or organisation or object that is entitled to use it

3. ***Authorisation*** - binding the digital identity to the virtual identities that interact online to execute transactions

For example, a gaming site needs to know a few of my attributes (for example, that I am a real person above a certain age) but it doesn't need to know all my characteristics. So when I go to create my account at the gaming site (in others words, when I go to create my gaming virtual identity) I can present my telco virtual identity (created by the telco after linking me to my digital identity). The gaming site forces an authentication and once it gets the positive response it can then take the public key from the telco virtual identity, add attributes to it (e.g., games downloaded, name chosen, etc) and sign that with its own private key. This creates a new gaming virtual identity

How a Blockchain Can Enable this Model:

The blockchain can be used as the shared ledger that stores identity transactions. Let us see how.

As mentioned, a digital identity is essentially a public-private key pair. The private key needs to be stored safely (identification) and we also need an authentication mechanism so that control over the digital identity can be asserted. Then we need to provide the public key for a variety of uses (authorisation). Telcos could store cryptographic keys in the SIM in a mobile phone (or even on cryptographic eSIMs). In this system, the SIM generates the key pair and gives up the public key but the private key is never disclosed. I could have multiple digital identities associated with the same physical identity (that is, myself) that I use for various purposes - for example one for work (using the work phone SIM) and one personal (using my personal SIM). Each of these digital identities will have various virtual identities associated with them.

Now, we have made the assumption that all transactions are between virtual identities. If the transactions (create, read, update, delete) associated with a virtual identity were to be stored in a shared ledger, it would then provide a record of that virtual identity's activities.

The history of that virtual identity (which is available on the ledger) is a kind of reputation. A pointer to an entry in the shared ledger gives you a public key. One can then use this public key to encrypt a challenge for the digital identity (which can decrypt the challenge with the private key and hence provide authentication). Alternately, one can peruse the transactions associated with a public key on the ledger to see whether the identity has been deleted.

Example of an Implementation:

I go to my telecom service provider to open an account. The telco does all of the necessary background checks (most likely using the necessary government issued documents) and creates a digital identity. The private key associated with this identity is stored safely in the eSIM on my phone and a copy is downloaded to the telco application on my phone. The telco creates a virtual identity using the public key from the digital identity and adds a set of standard fields (name, address and so on and so forth) as required. It then adds a digital signature using its own private key. A pointer to this virtual identity along with necessary descriptors is then added to the blockchain.

Now imagine that I visit a partner website, say, an ecommerce site. The ecommerce site needs to see my identity so I run the telco app on my phone and select the option to provide my identity. A copy of the ledger entry is sent to the ecommerce site app. Now the ecommerce app can go to the blockchain and look at all entries for that same virtual identity (in particular to see whether it has been revoked or not). Once the virtual identity is established, the ecommerce site needs to know that the virtual identity belongs to me so its app takes the public key from virtual identity, encrypts a challenge and sends it to my app which decrypts it (because it has the associated private key) and responds. Now the ecommerce site can either use that virtual identity or in the more general case use it to generate an ecommerce virtual identity which is then stored in the ledger itself.

The next time I visit the same ecommerce site, I can be authenticated using the same

The ecommerce site can hence use that for running a recommendation engine. I can also use the same ecommerce virtual identity to login to a completely different ecommerce site using the same mechanism.

The telco virtual identity can be used to help create other virtual identities similar to the ecommerce one (such as a travel virtual identity). This identity need not know all my details from my digital identity, only the ones that are relevant (such as my home location) and add other attributes (such as my preferred mode of travel) to create a travel virtual identity. The possibilities of such identity management are limited only by the number of partner service providers that the telco can bring on to the blockchain

Benefits:

1. ***Interoperability*** - Identity information can be made interoperable across marketplaces. More importantly, the reputation of a physical entity can be enhanced by the various transactions that its virtual identity is involved in. For example, the financial transactions of the ecommerce virtual identity can act as a parameter in the credit ratings of the involved physical identity (the person buying the goods). So, instead of relying on a limited set of parameters for credit ratings, the everyday transactions carried out by an individual can provide for a more dynamic credit rating mechanism

2. ***Convenience*** - Users benefit from the convenience of not having to remember many username and password combinations and also from the fact that they need not share personal data from external vendors

3. ***Security*** - The immutable and decentralized blockchain solution allows for robust identity security. Users have more control over their data

4. ***Content Aggregation*** - Subscribers can be provided with central, convenient access to aggregated data and more visibility and control over which entities their data gets shared with

Do let me know what you think in the comments section

Tagged in: telecommunications, identity management, cryptography

Report this

Sawan Kumar

Senior Consultant (IT Strategy) at Deloitte

3 posts

Follow

2 comments

Recommended

Leave your thoughts here…

Mark Morris ··· 6s

All-Star -- Founder, lejer9.com -- inventor of the "Cognitive Blockchain" (tm)

Nice article Sawan! Enjoyed it. The more I read articles like these the more they are starting to sound like qrsign.in a security platform I designed that was at the time too far ahead to catch any eyes. Which was good for me, because it is now a core component of lejer9's "Cognitive Blockchain"(tm). AAA is central to most apps, including emerging permission-based blockchains. Looks like I have another opportunity for offer an identity app too that many will want or want to copy. I love the use of the term device, because everything is a device in qr-sign.in and devices can be anything :)

Like Reply

Prajeesh Jayaram FRM ··· 15h

Debt Capital Advisor & Blockchain Enthusiast

Hi Sawan! Excellent post and probably a genuine use case.
I understand the blockchain is selectively transparent here. In which nodes are the blockchain containing the identity details distributed? And while editing the blockchain (specifically primary identity details like name), who all takes part in the consensus mechanism?

Like Reply

Top stories from authors on LinkedIn

The 5 Incredible Things To Do To Live A Charmed Life

James Altucher on LinkedIn

Uber Loses $1.2 Billion by Q2 2016; Is This the End of the Sharing…

Brian Solis on LinkedIn

Hampton Creek faces criminal probe in vegan mayo buybacks; Obama…

John C Abell on LinkedIn

Looking for more of the latest headlines on LinkedIn?

Discover more stories