Practical Thoughts on Blockchain and Identity

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

Introduction

The blockchain is seen by many as one of the most significant developments in technology with many arguing that it has the potential to remake the world economy from the ground up by transforming and re-imagining the way business is done today. In this whitepaper, we start by describing the current state of affairs with identity, how we got here and describe some of the issues that we need to overcome. We then look at the unique capabilities of blockchain and describe how it has the potential to address many of these issues. We will then consider some of the practical hurdles that the industry at large has to overcome when using identity on the blockchain. Finally, we will look at how Okta is collaborating with our customers and partners to enable new use cases for identity with blockchain.

Issues With Identity Today

One of the key enablers for today's digital economy is identity. Both businesses and users are becoming increasingly frustrated by the convoluted methods they are forced to use to interact with each other. Let us review some of the major issues.

Issue 1: Identity Sprawl and Privacy

There isn't currently a universally accepted digital equivalent of the user's offline identity such as a passport or a driver's license. Users are issued a unique digital identity for each application they use on the Internet. This is difficult and counterproductive for users because they now have to remember all their usernames and passwords. Multiple credentials expose the user to a variety of security issues.

Federation has solved this problem to an extent by allowing the transfer of a user identity from one domain to another transparently. For the end user, it typically means that they can access online services seamlessly using an existing or valid session with an Identity Provider (IdP).

More recently, large social media companies such as Facebook have helped establish the concept of a social identity for users that can be leveraged as an alternative for some use cases. Some countries such as **Estonia** and **Singapore** are issuing digital identities so that citizens can safely identity themselves when they want to avail e-services.

Issue 2: Attribute Drift and Sync

A digital identity is a set of claims made by one digital subject about itself or other digital subjects. For example, John Smith, an individual with an identity may have attributes such as gender, height, weight, mailing address, email address, date of birth, place of birth, citizenship, driver's license number, etc. Some of these attributes will be unique identifiers (e.g. email address, SSN, passport number, etc.) because they are uniquely associated with John's identity.

It is worth pointing out that some identifiers can be permanent for life (e.g. SSN). Some are long lived (e.g. driver's license number, passport number). But, many identifiers can be reassigned (e.g. cell phone numbers) and therefore it is possible that the same identifier is associated with another identity at different times. With the duplication of identities for every entity, both users and businesses are burdened with having to keep the attributes and identifiers in sync across the silos every time there is a change.

Issue 3: Inconsistent Security Posture

Users have no guarantees that the identities issued are adequately secured by the institutions issuing them. Since these have tangible value, they are a juicy target for hackers and can result in identity theft (see below).

Issue 4: Identity Theft

In the offline world, identity documents are issued by trusted entities that design and keep updating them in a manner to deter forgery and counterfeiting. For example, your driver license is strongly linked only to you (e.g. with a picture, a fingerprint and a number of anti-forgery mechanisms visibly embedded in it). Therefore, if it is stolen, it is of limited value. In contrast, in the digital world, identity theft is a major concern for users. In most cases, the user or the entity have no idea that the user's digital identity has been stolen and being actively used by the fraudster.

Issue 5: Regulations

The government holds financial institutions to high standards when it comes to "Know Your Customer" (KYC) laws. These were introduced in 2001 as part of the Patriot Act. The core idea here is that they need to know their customer (i.e. verify their identity, make sure they are real, ensure they are not on a prohibited lists and keep money laundering, terrorism financing and fraud schemes at bay).

These help establish and verify the identity of the customer by using reliable and independent data or sources of information. On the flip side, these processes can be extremely manual, cumbersome and expensive for the entities involved. It is reported that the average institution spends in the region of $60M every year ensuring adherence to these checks.

Enter Blockchain

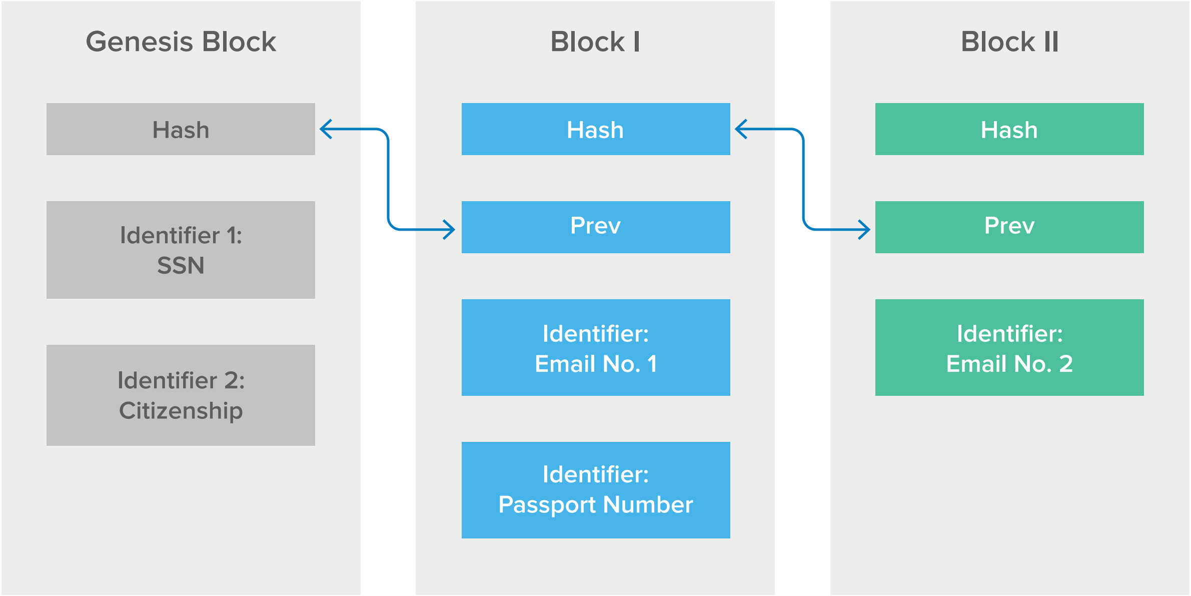
At its core, the blockchain can be thought about as a distributed database system that acts as an "open, shared ledger" to store and manage transactions. Each record in the database is called a block and is cryptographically linked to the previous block. Since the same transaction is recorded over multiple, distributed database systems, there isn't necessarily a single point of failure in the system. Let us look at some of the unique capabilities of blockchain.

1. Immutability

Each block in the blockchain builds upon its predecessor (a timestamp and a link to a previous block). The cryptographic nature of these blocks makes it hard to alter information in the existing blocks. In essence, one could say that blockchains enable the creation of permanent data that is locked in time.

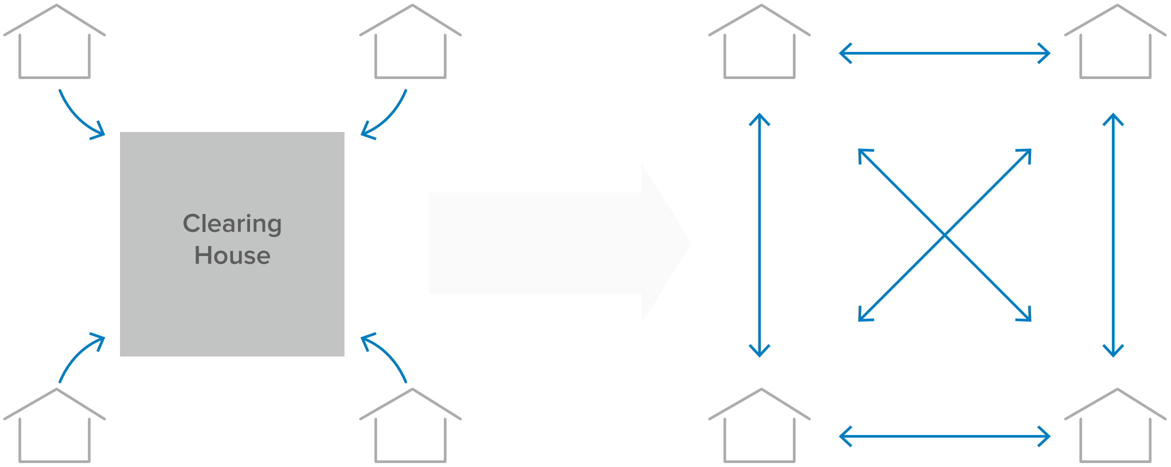
Therefore, it is technically possible to record a transaction and be confident that nobody can alter or manipulate its details. Anyone can start from the "Genesis Block", apply each block consecutively to arrive at the same result. This provides certain guarantees even when some participants are faulty or malicious. The blockchain uses cryptography and digital signatures to prove identity, authenticity and enforce read/write access rights. In summary, the blockchain has the potential of enabling "provenance of identifiers for an identity".

An immutable record on a distributed blockchain ledger that strongly associates identifiers with an identity can have advantages over a centralized database. Changes to every single identifier associated with an identity could be logged on the blockchain preventing fraudsters from being able to tamper records without leaving an obvious digital trail. In summary, incidents such as identity theft and account takeovers could be a thing of the past.



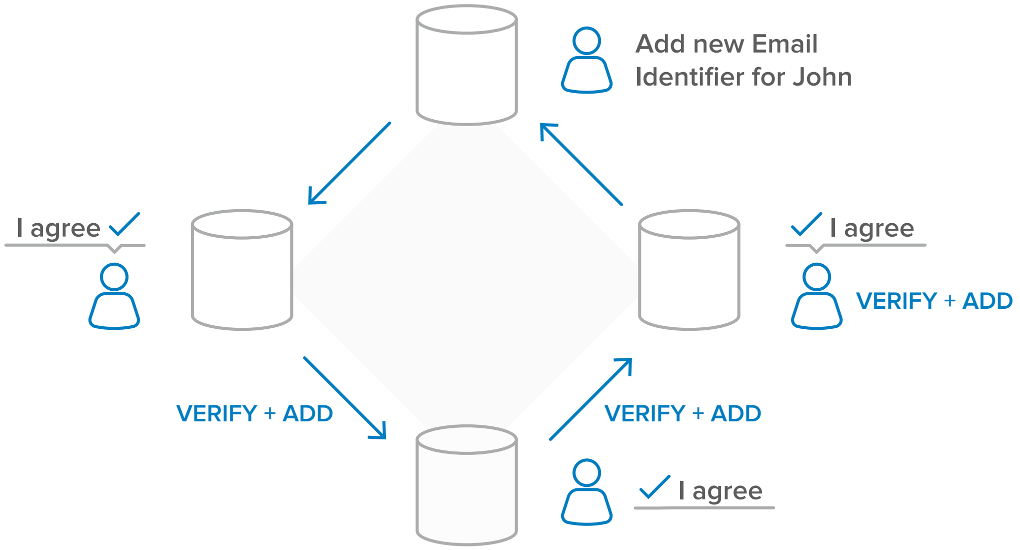
2. Distributed, Decentralized and Shared Database (aka Distributed Ledger)

Traditional databases are managed by a single entity bringing into question the integrity and accuracy of the data in the database. In contrast, a blockchain-based ledger is distributed across multiple entities. Each participant maintains a replica of a shared append-only ledger of digitally signed transactions. The participants maintain the replicas in sync through a protocol referred to as consensus (see #3 below). This capability removes the concern of single point of failure and removes control by a single entity. This unique capability is particularly well suited for complex, multi-entity business networks such as supply chains or consortiums. For example, a malicious bank employee will not be able to arbitrarily modify John's identifiers in the shared ledger for personal gain.



3. Consensus

Because any entity can request to add information to the blockchain, multiple operators of the blockchain need to evaluate and agree before this information is permanently incorporated into the blockchain (the distributed ledger). This "consensus" process helps keep inaccurate or potentially fraudulent transactions out of the database. The aim of the consensus approach is to secure the network predominantly through economic means (i.e. it should be too expensive to attack the network, and more profitable to help protect it). To illustrate with an example—if John changes his cell phone number (a re-assignable identifier associated with his identity), a majority of operators of the blockchain will have to agree before the changes are incorporated into the blockchain.

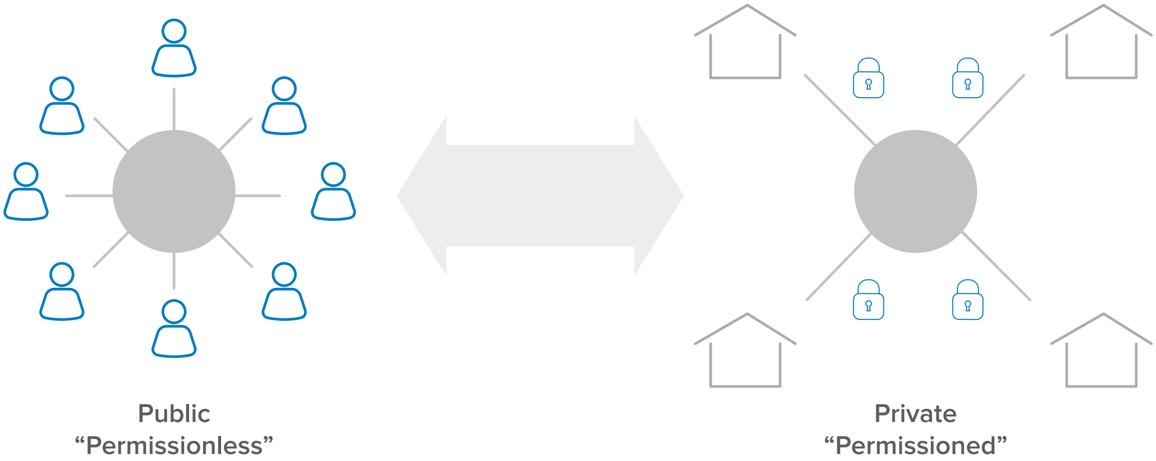


4. Private vs. Public Blockchain Networks

The primary difference between a public and private blockchain is who is allowed to participate in the network (i.e. execute the consensus protocol and maintain the shared ledger).

A public blockchain network is completely open (i.e. anyone can join and participate in the network). In contrast, a private blockchain network requires an invitation and must be validated before entities are allowed to participate. Think of the private blockchain as the "Intranet" of blockchains with the goal of adding gated accountability to an extended enterprise.

Organizations or consortiums that set up a private blockchain will set up a permissioned network that will place restrictions on who is allowed to participate and also what type of transactions they are allowed to perform. One of the key benefits of a private blockchain is that only the entities participating in a particular transaction will have knowledge and access to it.



Use Cases for Identity on Blockchain

The most common and successful application of the blockchain technology today is around digital currency. The Bitcoin phenomenon started in 2008 and the Bitcoin blockchain has operated without major disruption since then. As of Oct 27, 2017, a single Bitcoin was valued at approx. **$5,860** and the network has a market cap of **$96B**.

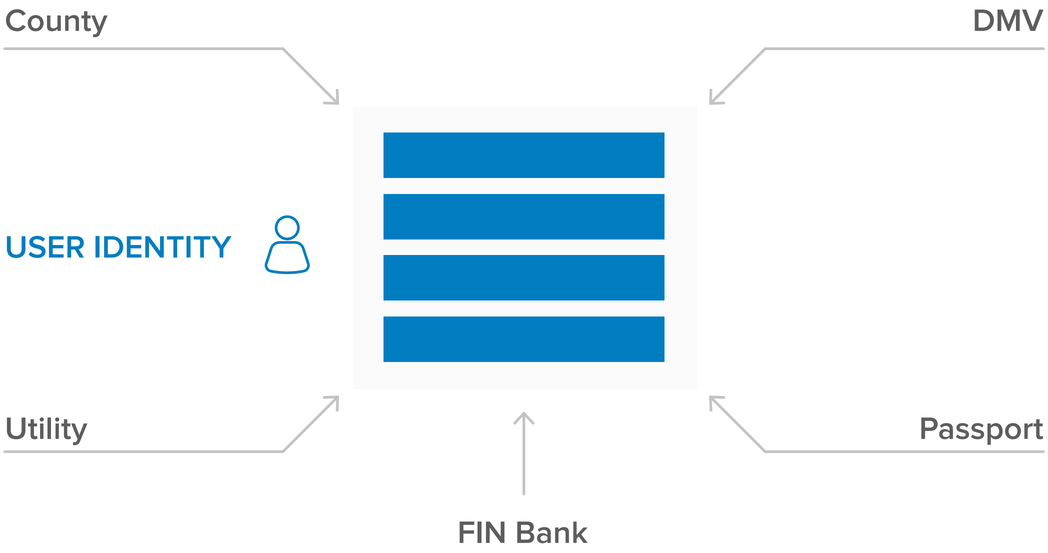
Some of reasons why bitcoin has thrived are because it is fast (relative to checks and international wire transfers that can take days), it can be anonymous (nobody knows who is behind a Bitcoin address), there is no middleman or need for a trusted third party (it is completely decentralized) and nobody can block you (unlike banks that can freeze accounts).

Let us look at some new and interesting use cases that the blockchain could help enable for identity and consider whether these are truly transformative in nature.

Opportunity No. 1: Self Sovereign Identity

With the blockchain's secure distributed ledger capabilities, it may be finally possible to put users in charge of their own identities so that they have complete control over it. If the user can be put in charge of their identity, it may be feasible to remove many of the issues related to identity today. For example, there will no longer be a need for identity sprawl, users do not have to worry about privacy or identity theft.

Several pilots are underway to try and make this a reality. For example, on 31st August, 2017, the Illinois Blockchain Initiative (IBI), a consortium of Illinois state and county agencies kicked off a pilot program to put birth certificates on a blockchain. The IBI is working to promote the use of "self-sovereign" digital identities that can remain under a user's control, capable of quick and secure validation without the need for a centralized repository.



Opportunity No. 2: Smart Contracts

Much of what we encounter on modern websites is mostly a shiny digital facade backed by relatively archaic, manual and time-consuming processes. The blockchain's decentralized ledger could be used for smart contracts enabled by identity on the blockchain.

These are sometimes referred to as self-executing contracts that can be converted to code, stored and replicated on the blockchain. This has the potential to help the industry transition to software defined contracts that execute automatically without the need for human intervention.

A good example of an entity at the forefront of this effort is the state of Delaware where ~2/3rd of the Fortune 500 companies are headquartered. The state is evaluating the use of blockchain to streamline the entire process and workflows associated with registering companies, tracking share movements, and managing shareholder communications into a modern, digital environment. The state is specifically pushing for the creation of a new type of corporate shares, dubbed "distributed ledger shares" that hold the promise of immediate clearance and settlement. They also working to move proxy voting (i.e. the practice of third parties voting on a stakeholder's behalf,) to a blockchain.

Opportunity No. 3: Identity for IoT

Identity is not limited to people. As new IoT devices (backed by asset identity) and services (backed by service identity) come online, managing these identities will be critical to help unlock new workflows that were not possible before. For example,

- IoT-to-User transactions (Example: an autonomous car authenticating the user, delivering a personalized experience based on the user's identity and history. Potentially also automatically charging rental fees for every minute of usage, recording this activity on the blockchain.)
- IoT-to-IoT transactions (Example: an autonomous car automatically paying for gasoline at a pump or a charging station leveraging its asset identity. The rental car company or the owner potentially getting automatically charged leveraging blockchain's smart contracts.)

Blockchain's ability to automate and keep transactions accountable via the secure shared ledger and smart contracts have the potential to enable new and interesting use cases that haven't been possible before.

Beyond the Rose-Colored Glasses

As we saw in the previous section, blockchain has the potential to both transform and enable new use cases for identity. But, progress has been slow and measured due to a variety of reasons—technical, some legal and some likely generational issues that just need time to play out. It is worth pointing out that it took about 30 years before TCP/IP enabled businesses to fully transition to Internet driven, platform business models. Let us look at some of the issues that the industry and standards bodies are working through as they consider blockchain for identity.

The Myth of Immutability

In theory, a blockchain is immutable and would take the role of critical infrastructure. But, the immutability doesn't necessarily hold in all conditions. There is the concern of a "51% attack" where the threat actor can effectively create a new branch that could overwrite and potentially reverse all of the transactions on a public blockchain.

Getting to 51% would require either money or an act of collusion which is an investment a state actor may be willing to make to undermine a public blockchain. Private blockchains can potentially implement countermeasures to prevent these threats.

Mind the Gap: Mapping Real Life to Digital

Blockchain can vouch for an identity once it is in the blockchain. But, given it is created and exists only in the digital world, blockchain cannot guarantee the physical identity of the user. So, businesses still need to figure out who is responsible to provide the trust mapping between real life physical identity and the digital identity. It will be extremely important to ensure that the identity provider with the weakest proofing (weak link) doesn't become an attack vector for identity takeover on the blockchain network.

Identity as a Moat for Business

For many organizations, there is no business incentive in sharing their customer's identity related data beyond their boundaries because of concerns associated with customer retention. This is particularly true for businesses that have invested and worked really hard to get to a market leading position.

Account Recovery

Trust in ownership of the identity on the blockchain (or for that matter any system) is predicated on the authenticators used for access to the system. When a loss of the authenticator occurs, users will need to rebind the replacement authenticators to their identity. Fraudsters will specifically make every effort to leverage these account recovery flows to take over identities because they would have access to a tenured and trusted identity on the blockchain which would be worth its weight in gold.

Legal Framework and Liability

In the absence of legal precedent, the entities involved would have to accept risk, uncertainty and potentially unbounded liability by agreeing to participate in an identity ecosystem. Large, regulated businesses are generally apprehensive of being the first mover when the risk is extremely high and ROI the lowest.

Okta and the Blockchain

While blockchain technology is nascent, Okta is working with our progressive customers who are already building concept solutions using blockchain. Okta is working closely with customers, consortiums and partners as we flush out industry specific use cases related to blockchain and identity. To highlight a specific example, Okta is working with some key customers in Canada who are extending their B2B and B2C applications to streamline cumbersome and expensive Identity Proofing flows leveraging blockchain.

SecureKey Technologies has developed a functional, secure credential sharing network between financial institutions and the Canada Revenue Agency to simplify the login process for Canadian consumers. They are working to extend this and launch a new digital identity and attribute sharing network based on blockchain. The end goal is for entities to streamline the manual and time consuming process of identity verification during the process of opening a new bank account, renewal of driver licenses, and submission of income tax returns, etc. This will require consumers to opt into the blockchain network. Once they do, they will have the ability to control which attributes associated with their identity they are willing to share with organizations of their choice.

Summary

In today's business networks, users are forced to create and maintain duplicate identities resulting in an identity sprawl. The use of blockchain's distributed ledger capabilities has potential to enable users to retain control of their identity.

Identity on the blockchain can ensure immutability of records. This has the potential to streamline experiences for users and businesses by eliminating unwanted manual checks and middlemen. It also has the potential to improve transparency which can help drive down the need for unwanted government regulations such as Know Your Customer (KYC).

Smart contracts can be executed on blockchain networks seamlessly powered by identity. This has the potential to help automate and streamline tasks that are very manual and require middlemen. The increased speed of execution and reduction in costs with lower risk can enable businesses to drive growth by opening new revenue streams that were previously not possible.

We are still in the early days of the use of blockchain for Identity. Okta plans to continue collaborating with our customers and partners in key verticals as we assess and validate transformative use cases related to identity on the blockchain.