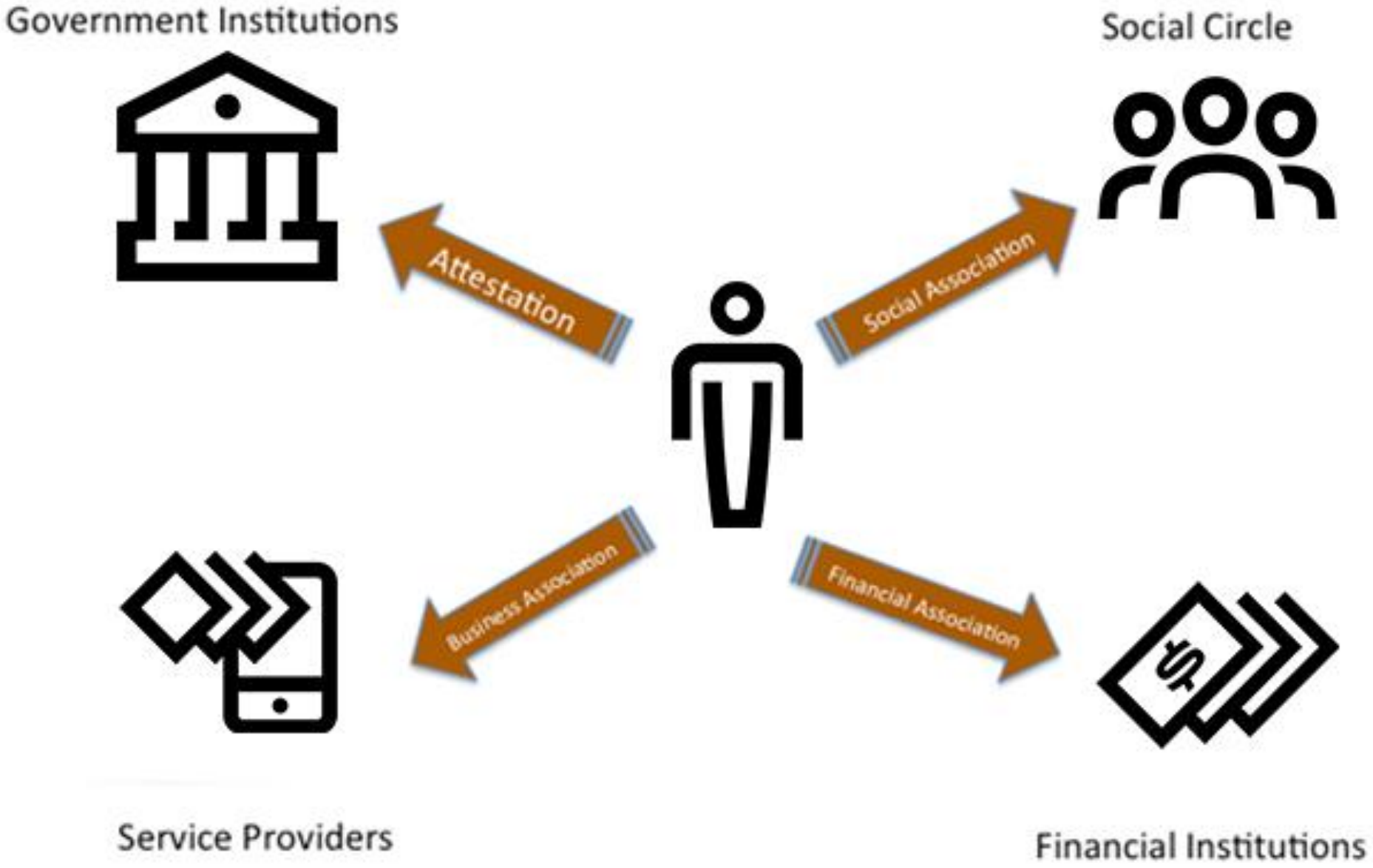
BlockChain Technologies

Public Keys as Identities


Government Institutions
Social Circle
Attestation
Social Association
Business Association
Financial Association
Service Providers
Financial Institutions

TRADITIONAL IDENTITY

- User’s identity defined from perspective of the provider for a specific purpose and is therefore only valid within the domain of that specific provider within that purview.
- People have all sorts of identities conferred on them in various forms (passports, proof of employment, diplomas) and by various third parties operating as sources of authority (e.g., credentialing bodies).

SELF-SOVEREIGN IDENTITY

- Individuals are the ultimate source of data about themselves: a citizen's identity pre-exists before the conferral of an identity by any third party.
- In building and governing a network of globally acceptable self-sovereign identity, in any such network the three core tenets of individual control, security and full portability must be met.

TEN PRINCIPLES OF SELF SOVEREIGN IDENTITY

Principle	Explanation
Existence	Users must have an independent existence
Control	Users must control their identities
Access	Users must have access to their own data
Transparency	Systems and algorithms must be transparent
Persistence	Identities must be long lived
Portability	Information and services about identity must be transportable
Interoperability	Identities should be as widely used as possible
Consent	Users must agree to the use of their identity
Minimization	Disclosure of claims must be minimized
Protection	Rights of the users must be protected

Useful trick:

- public key == an identity

If you see sig such that verify(pk, msg, sig)==true, think of it as

pk says, “[msg]”.

To “speak for” pk, you must know matching secret key sk

How to make a new identity

Create a new, random key-pair (sk, pk)

pk is the public “name” you can use
[usually better to use Hash(pk)]
sk lets you “speak for” the identity

You may use the hash of pk as your identity since public keys are large

One will have to check that

- pk indeed hashes to your identity
- the message verifies under public key pk.

You control the identity, because only you know *sk*

- If *pk* “looks random”, nobody needs to know who you are
  - You can generate a fresh identity that looks random, like a face in the crowd, and is controlled only by you

DECENTRALIZED IDENTITY MANAGEMENT

Anybody can make a new identity at any time make as many as you want!

No central point of coordination

You want to be somewhat anonymous for a while, you can create a new identity, use it for just a little while, and then throw it away

These identities are called “addresses” in Bitcoin.

addresses == hash of a public key

ADDRESS

- Addresses not directly connected to real-world identity.

- But observer can link together an address's activity over time, make inferences.
  - In Bitcoin you don't need to explicitly register or reveal your real-world identity, but the pattern of your behavior might itself be identifying

An **address** is a short, alphanumeric string of characters derived from the blockchain network user's public key using a cryptographic hash function, along with some additional data (e.g., version number, checksums).

Addresses are shorter than the public keys and are not secret. One method to generate an address is to create a public key, applying a cryptographic hash function to it, and converting the hash to text:

public key ⟶ cryptographic hash function ⟶ address

Each blockchain implementation may implement a different method to derive an address. For permissionless blockchain networks, which allow anonymous account creation, a blockchain network user can generate as many asymmetric-key pairs, and therefore addresses as desired, allowing for a varying degree of pseudo-anonymity.

In Bitcoin, the blockchain enabled users to be **pseudonymous**. This means that users are anonymous, but their account identifiers are not; additionally, all transactions are publicly visible.

Hence, it was essential to have mechanisms to create trust in an environment where users could not be easily identified.

Without trusted intermediaries, the needed **trust** within a blockchain network is enabled by four key characteristics of blockchain technology:

- **Ledger:** the technology uses an append only ledger to provide full transactional history. Unlike traditional databases, transactions and values in a blockchain are not overridden.

- **Secure:** blockchains are cryptographically secure, ensuring that the data contained within the ledger has not been tampered with, and that the data within the ledger is attestable.

- **Shared:** the ledger is shared amongst multiple participants. This provides transparency across the node participants in the blockchain network.

- **Distributed:** the blockchain can be distributed. This allows for scaling the number of nodes of a blockchain network to make it more resilient to attacks by bad actors. By increasing the number of nodes, the ability for a bad actor to impact the consensus protocol used by the blockchain is reduced.

In the blockchain, transactions are ‘digitally signed’. This means that a private key is used to encrypt a transaction such that anyone with the public key can decrypt it.

Since the public key is freely available, encrypting the transaction with the private key proves that the signer of the transaction has access to the private key.

THE USE OF ASYMMETRIC-KEY CRYPTOGRAPHY IN MANY BLOCKCHAIN NETWORKS

- **Private** keys are used to digitally sign transactions.
- **Public** keys are used to derive addresses.
- **Public** keys are used to verify signatures generated with private keys.
- Asymmetric-key cryptography provides the ability to verify that the user transferring value to another user is in possession of the private key capable of signing the transaction.

TYPES OF BLOCKCHAIN

Blockchain networks can be categorized based on their permission model, which determines **who** can **maintain** them (e.g., **publish** blocks).

If anyone can publish a new block, it is **permissionless**. If only particular users can publish blocks, it is **permissioned**.

Permissionless blockchain networks are decentralized ledger platforms that anyone has the right to publish blocks, this results in the property that anyone can read the blockchain as well as issue transactions on the blockchain, without needing permission from any authority.

Permissionless blockchain platforms are often open source software, freely available to anyone who wishes to download them.

In the **permissionless** blockchain networks malicious users may attempt to publish blocks in a way that subverts the system.

To prevent this, permissionless blockchain networks often utilize a multiparty agreement or ‘consensus’ system that requires users to expend or maintain resources when attempting to publish blocks.

The consensus systems in permissionless blockchain networks usually promote non-malicious behavior through rewarding the publishers of protocol-conforming blocks with a native cryptocurrency.

In the **permissioned** blockchain networks, only authorized users are publishing blocks and maintaining the blockchain.

Permissioned blockchain networks may allow anyone to read the blockchain or they may restrict read access to authorized individuals.

They also may allow anyone to submit transactions to be included in the blockchain or, again, they may restrict this access only to authorized individuals.

Permissioned blockchain networks may be instantiated and maintained using open source or closed source software.

Permissioned blockchain networks can have the **same** traceability of digital assets as they pass through the blockchain, as well as the **same** distributed data storage system as a permissionless blockchain networks.

They also use consensus models for publishing blocks, but these methods often do not require the expense or maintenance of resources and usually are faster and less computationally expensive. Since, those maintaining the blockchain have a level of trust with each other and they were all authorized to publish blocks and their authorization can be revoked if they misbehave.

Permissioned blockchain networks may also be used by organizations that need to more tightly control and protect their blockchain. However, if a **single** entity controls who can publish blocks, the users of the blockchain will need to have trust in that entity.

Permissioned blockchain networks may also be used by organizations that wish to work together but may not fully trust one another. They can be partners to record their transactions on a shared distributed ledger and the consensus model selected **based on** how much they trust one another.

Some permissioned blockchain networks require all users to be authorized to send and receive transactions.

In such systems parties work together to achieve a shared business process with natural disincentives to commit fraud or otherwise behave as a bad actor (since they can be identified).

If bad behavior were to occur, it is well known where the organizations are incorporated, what legal remedies are available and how to pursue those remedies in the relevant judicial system.