LTO NETWORK

LTO NETWORK

On-chain Identities and Credentials

LTO NETWORK

On-chain Identities and Credentials

Everything and everyone on the blockchain is only known by a number; the public address. Addresses provide a relative anonymity, which many consider a major perk. However, for businesses it hinders adoption, they are required by law to know the real-world identity of their clients, suppliers, and partners.

An on-chain identity system seems like the obvious answer. However, those that exist today have yet to make any impact on the blockchain ecosystem. They lack interoperability and rely on permissions and legal contracts to enforce network rules.

LTO Network is a hybrid blockchain which combines a public and private chain, this allows us to use a permissionless model where rules are purely enforced by network consensus, while still ensuring privacy.

Index

LTO NETWORK

Public identities

To sign transactions on the blockchain you use a public / private key pair. Your blockchain identity, the public address, is calculated from the public key. Any computer can do this; we don't rely on trust to connect your identity to your key pair.

Unfortunately, there's no such inherent relationship between a public key and a real-world identity. The owner of the key pair can make a claim about it's identity, but how do we know if this can be trusted?

Permissioned vs permissionless

Other on-chain identity solutions use a permissioned model, which appoints trust anchors. A trust anchor is an authoritative party for which trust is assumed and not derived. These trusted parties, typically banks and big corporations, are responsible for validating identities and keeping the network secure. The downside to this appointment is that it creates a barrier to entrance and potentially an unlevel playing field.

LTO Network is and will stay permissionless; there are no roles and network rules are only enforced through the consensus mechanism. Trust is established by utilizing existing methods and allowing it to emerge from the network naturally.

> The downside to appointed trust anchors is that it creates an unlevel playing field.

Public identities

Public key certificates

Using public / private key pairs for authentication isn't unique to the blockchain. We use public key certificates daily, often without even realizing it. Most notably this technique is used in SSL, which is the basis for HTTPS; the protocol that keeps the web safe and secure.

LTO introduces a new transaction type, the identity transaction, that enables businesses to publish a certificate on the blockchain. Future transactions can be signed with the key pair associated with this certificate, which is available on-chain to verify the identity.

Certificate authorities

Certificates can be issued by a certificate authority (CA), like Let's Encrypt, IdenTrust, and DigiCert. The CA is a trusted third party, responsible for validating the identity of the public key owner. The CA can be an intermediary, in which case it's entrusted by another CA, which may in turn be entrusted by another, until ultimately reaching the root CA, which is a trust anchor.

By utilizing CA certificates, LTO Network isn't tasked with appointing trust anchors. Instead, we leverage on an existing trust network; the one everyone relies on daily to keep the Internet safe.

LTO Network leverages on an existing trust network, the one that keeps the Internet safe.

Public identities

Web of trust

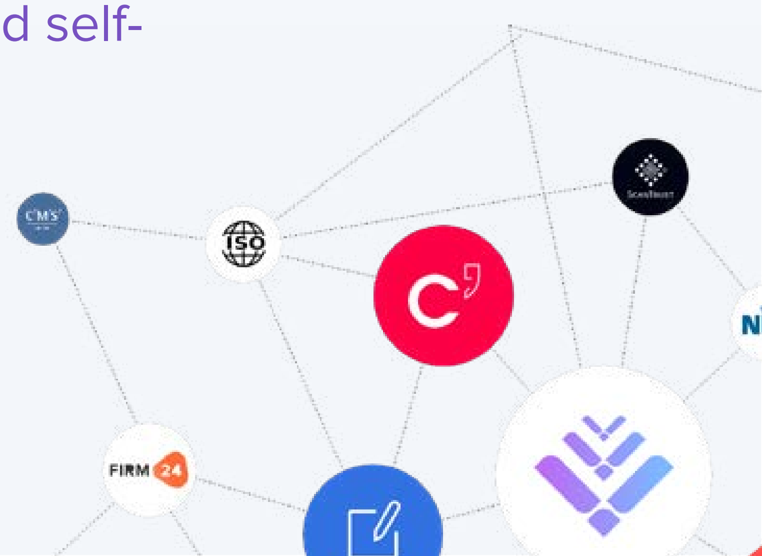
CA issued certificates have a strict hierarchy. The root CA, intermediate CAs, and certificate owner, form a chain of trust. Blockchain promotes collaboration on a level playing field, which doesn't fit well with an hierarchical trust network.

A web of trust is an alternative to the chain of trust. It's a decentralized trust model that doesn't rely on a hierarchy or trust anchors. Instead trust is obtained through endorsements of peers. Anyone can initiate a new trust network on LTO Network by endorsing others using LTO association transactions.

It's possible to publish CA issued certificates as well as self-signed certificates. Self-signed certificates are issued by the owner itself. The identity isn't verified when the certificate is issued, and must rely on endorsements for trust.

LTO Network uniquely provides businesses with the ability to create project-specific trust networks, which combine CA issued and self-signed certificates.

LTO Network uniquely provides businesses with the **ability to create project-specific trust networks**, which combine CA issued and self-signed certificates.



Public identities

Publishing certificates

Identity transactions allow businesses to publish public key certificates. Nodes not only check the validity of the transaction but also of the certificate itself.

Publishing a certificate also automatically creates an account on LTO Network, allowing the certificate owner to sign transactions with the certificate key pair.

Anyone can publish the certificate, it doesn't have to be the certificate owner. The publisher pays the transaction fee, but only the owner can use the new account. This makes it possible for the certificate issuer to publish the certificate instead of the owner.

Associations

Besides generic endorsement, the earlier introduced association transactions on LTO Network, can be used to state a specific relationship between businesses. For instance, a company can create associations to all its affiliates. These associations can be depended upon for authorization and access control in both centralized and decentralized applications.

Publishing a certificate automatically creates an account on LTO Network, allowing the certificate owner to sign transactions with the certificate key pair.

Private identities

Publically publishing certificates on the global blockchain provide businesses with a way to identify themselves. Individuals need a different method that respects privacy.

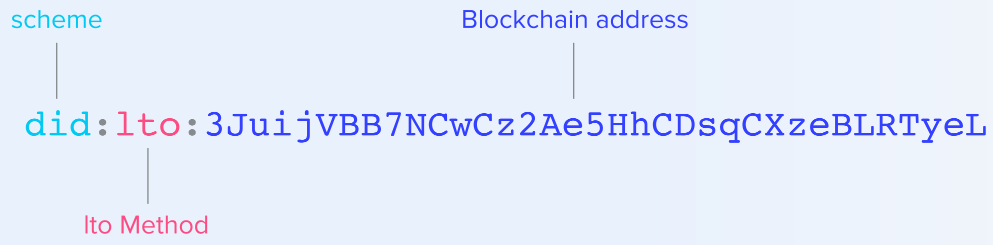
Self-sovereign identities is a method where users store and manage their own credentials. A business can validate a claim like “This is my name and address” through a KYC procedure. The user will receive a signed copy of the credentials.

LTO provides multiple node images, like the anchoring node, which provides additional services on top of the LTO public blockchain.

For self-sovereign identities, LTO will deliver a new node image, the identity node, which supports the W3C Decentralized Identifiers (DID) and Verifiable Credentials specification.

Decentralized Identifiers (DID)

DIDs are unique identifiers that specify both a blockchain and a blockchain address. For addresses on LTO Network, the DID URL is



```
did:lto:3JuijVBB7NCwCz2Ae5HhCDsqCXzeBLRTyeL
```

The identity node will provide information about a DID on LTO Network in the form of a DID document. The DID document contains the public key, which is required to verify a signature of the address owner.

Private identities

DID documents

The blockchain address is generated from the public key using a hashing function. Hashing is one-way; it's not possible to extract the public key from an address. The identity node will index all transactions on the public chain, storing addresses with their respective public key.

For basic usage, an address owner can use a simple anchoring transaction to ensure their DID is indexed. This is the cheapest option. Alternatively, the owner can use a public key certificate. This certificate must not contain privacy sensitive information.

Publishing a certificate to index your DID has some advantages. The purpose of a public key can be specified, something that's not possible in most SSI solutions. Also, the certificate can be published by a verifiable credential issuer, so the only issuer needs to handle transaction fees rather than all certificate owners.

Derived DIDs

It's not advisable to use DIDs of private identities for multiple purposes. Correlating information might allow a party to deduce information, undermining privacy.

A typical solution is to generate a new key pair for each use. LTO provides an alternative of generating many derived DIDs from a single public key. This is done by using a hmac hash instead of a regular hash to generate the address.

An hmac hash function takes a secret which must be known in addition to the public key to create the hash. The secret isn't published on the blockchain but added to the DID url as query parameter.

```
did:lto:3JcHcZ3dbRkbEUgs9GsddQyG3QDXj7nkwJZ?nonce=Gnrwes4G8LBfsJWxCCd9ks
```

This method can also be used to support combining DIDs with federated identities, like those provided by SAML. The public key taken from the certificate of the SAML server can be used to create DIDs for each of its users.

Cross-chain DIDs

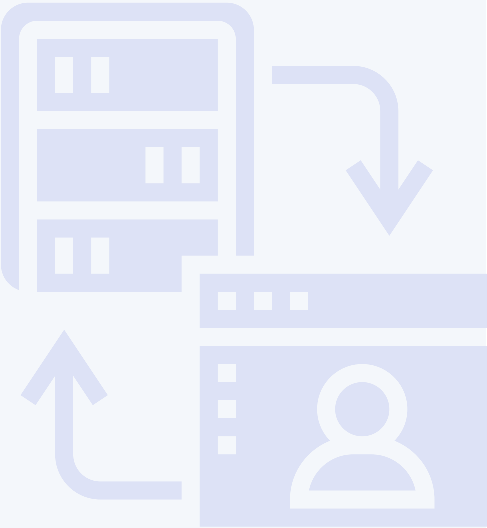
By default LTO network uses the ED25519 cryptographic algorithm to sign transactions. With public key certificates, LTO makes it possible to sign transactions with other cryptographic algorithms including RSA and ECDSA.

Users are able to use the key pair of another blockchain (like Ethereum) to generate a self-signed certificate. Publishing this certificate on LTO Network will give them a DID account and allows them to use the private key from Ethereum to sign transactions on LTO Network.

The identity node can index DID URLs of other blockchain in addition to the LTO address. These addresses are available in the DID document via the alsoKnownAs property. E.g. for Ethereum an ethr DID would be indexed;

```
did:ethr:0xf3beac30c498d9e26865f34fcaa57dbb935b0d74
```

It's possible to request the DID document using either the LTO DID or the ethr DID. This is important because it will increase the interoperability between blockchains moving forward.



Private identities

Cross-chain associations

Associations can be used to specify a relationship between accounts on LTO Network. By using associations with cross-chain DIDs, relationships between accounts on different blockchains can be established on LTO Network.

LTO Network is partnering with Chainlink to make this information available for smart contracts through its decentralized oracle network.

For example; an organization could add associations to establish an account belonging to an accredited partner. In this example, the accredited partners are allowed to certify businesses. By using Chainlink, it's possible to create a smart contract that can only be used by these certified businesses.

LTO Network is partnering with Chainlink to make associations available for smart contracts.

Verifiable credentials

A trust party, called the issuer, is responsible for validating the identity and/or other information about a subject, represented by a DID. This is similar to the role of a certificate authority (CA) for public key certificates.

The issuer provides the user with verifiable credentials, which is a signed copy of the personal information of the subject. It's the responsibility of the user to store these credentials and present them in order to verify it's identity.

The role of the blockchain in verifiable credentials is normally very small. Optionally an association is created, which should be checked before accepting the credentials. This allows the credentials to be revoked.

LTO is able to provide additional features to verifiable credentials, thanks to the hybrid approach. For example; combing verifiable credentials with an event chain on the private layer can help a projection comply with privacy regulations.

GDPR compliance

or GDPR, and similar privacy regulations, businesses are required to keep track of personal information they store and with whom that information is shared. Upon request, this needs to be communicated to the user.

Additionally the user is entitled to request for information to be destroyed. It's up to the business that initially received the data to ensure that any party with whom the data was shared, will also delete it.

This can be an administrative nightmare to handle manually. LTO has a decentralized solution to automate this process, which is being used by several enterprise clients since 2018.

Combining this solution with verified credentials gives the end-user full control over its personal data, while reducing the regulatory burden for all businesses involved.

Trust network

The Verified Credentials standard doesn't define how to specify which parties to trust as issuer.

Most current day identity solutions don't provide a solution for this, requiring applications to configure the DID URL of every party that may be trusted upon to issue credentials. This makes adding and revoking parties cumbersome, especially for distributed software. Additionally having this list off-chain voids immutability and hinders trustless verification.

Other SSI implementations employ a permissioned model, either through a smart contract or as part of the consensus model. The network itself is tasked with establishing trusted parties (trust anchors), which is done through governance and (off-chain) legal agreements. This creates a barrier of entrance for businesses. Also projects might not be able to accept credentials from all trust anchors on the network due to regulatory limitations. This means that those projects need to go back to configuring a list of trusted DIDs.

LTO Network uniquely provides a permissionless model for SSI. It allows applications to leverage existing trust models, like CA signed certificates, removing the need for the network to establish trust anchors. Using associations it's possible to create a custom trust network for each project, either with a strict hierarchy or as a web of trust, depending on the project needs.

LTO Network uniquely provides a permissionless model for SSI.

Verifiable credentials

Wallet integration

LTO identity nodes will follow the W3C Decentralized Identifiers (DIDs), W3C Verifiable Credentials (VCs), and Rosetta standards. Adhering to these standards will make it interoperable with software run by other stakeholders in this space, such as governments, enterprises, vendors, users, etc.

Rather than creating our own wallet to store credentials, the focus is on interoperability and integration in other applications. Blockchain specific identity wallets are often hardly used. The trend for integrators is to create project specific applications that hide technical details like the use of the blockchain.

This trend can be witnessed in the growing number of wallets as an integrated part of (enterprise) apps, such as Rabobank/Randstad Career wallet, Off-Blocks Signing app, and BlockChangEU wallet.

As launching partner, we'll be collaborating with Sphereon to integrate the LTO Network identity solution into their existing software, making it available to potentially hundreds of enterprise clients.

> The trend is to create project-specific applications that hide the use of blockchain.

Conclusions

Anonymity on the blockchain is a double-edged sword. It protects the identity of the user, but it also hinders business adoption.

DIDs and verifiable credentials help to replace anonymity with privacy, by connecting blockchain addresses to real-world identities. This puts the user in control of when and how to share personal information.

The aim of on-chain identity solutions should be to improve upon existing identification methods. We need to be careful not to repeat the same flaws, like depending on a small group of trusted third parties.

The LTO Network identity node combines verifiable credentials with public key certificates, which form on-chain trust networks. This allows LTO to present a permissionless solution that doesn't rely on network appointed trusted parties.

Unique features like cross-chain associations and the GDPR workflow make the LTO identity node stand well above other solutions. With the help of partners like Chainlink and Sphereon, LTO Network is set out to become the dominant identity solution of the blockchain ecosystem.