DIGITAL IDENTITY, ASSET AND INTERNET OF THINGS

Dr. Jianjun Cui and Wolfgang Blumental

cui@inasset.de

wechat: cui8161188

Summary

The Bigtangle provides a decentralized identity solutions to power the 4th industrial revolution and internet of things, bringing secure identities (“Digital Twins”) to person, machines, algorithms, and other non-human entities. As smart identify solution, it can provide information without to reveal the detail information such as whether the age of the user is over 16 or 18.

The Bigtangle decentralized identity is a self-Sovereign Identity solution and the identity is issued by an authorized government or third party and transfer to user and then managed by user.

Instead of logging into Wechat, Facebook, Uber, et al, you will log into your own self-sovereign browser, and will have the same ability to rent a hotel room, use social media or hail a car.

The Bigtangle is a public chain with inherent exchange service, Near-Time Confirmation, Infinite Scalability, Feeless, Permissionless, Trustless, and Decentralized.

Table of Contents

Digital Identity

Digital Identity is the digital form of identity.

Identity solution comprises all the processes and technologies within a person and organization that are used to identify, authenticate and authorize someone to access services or systems in that said organization or other associated ones.

A digital identity is the replacement of paper-based identity such as birth certificates, national id cards, passports or driver’s licenses.

Identities need to be portable and verifiable everywhere, any time, and digitization can enable that. But being digital is not enough. Identities also need to be private and secure.

Several industries suffer the problems of current identity management systems:

– Government: The lack of interoperability between departments and government levels takes a toll in the form of excess bureaucracy. Which, in turn, increases processes' times and costs.
– Healthcare: half of the world's population does not have access to quality healthcare. The lack of interoperability between actors in the healthcare space (Hospitals, clinics, insurance companies, doctors, pharmacies, etc) leads to inefficient healthcare and delayed care and frustration for patients.
– Education: It is estimated that two hundred thousand fake academic certificates are sold each year in the USA alone. The difficulty in verifying the authenticity of these credentials leads to hiring of unqualified professionals, brand damage to the universities and the hiring companies.
– Banking: the need for login details such as passwords decreases the security of banking for users.
– Businesses in general: the current need to store clients' and employees' personal data is a source of liability for companies.

A personal data breach may result in huge fines due to GDPR infringement – such as the British Airways case – or simply due to customer trust loss and consequential damage to the organization's brand.

Bigtangle

The Bigtangle is new generation of blockchain. The Bigtangle extends the blockchain technology with integration of Markov Chain Monte Carlo (MCMC). Thus BITCOIN and ETHEREUM are special cases in Bigtangle.

Through the use of industry-grade big data technology in conjunction with its parallelizable architecture, Bigtangle is a successor to Bitcoin that can fulfill economically important key use-cases.

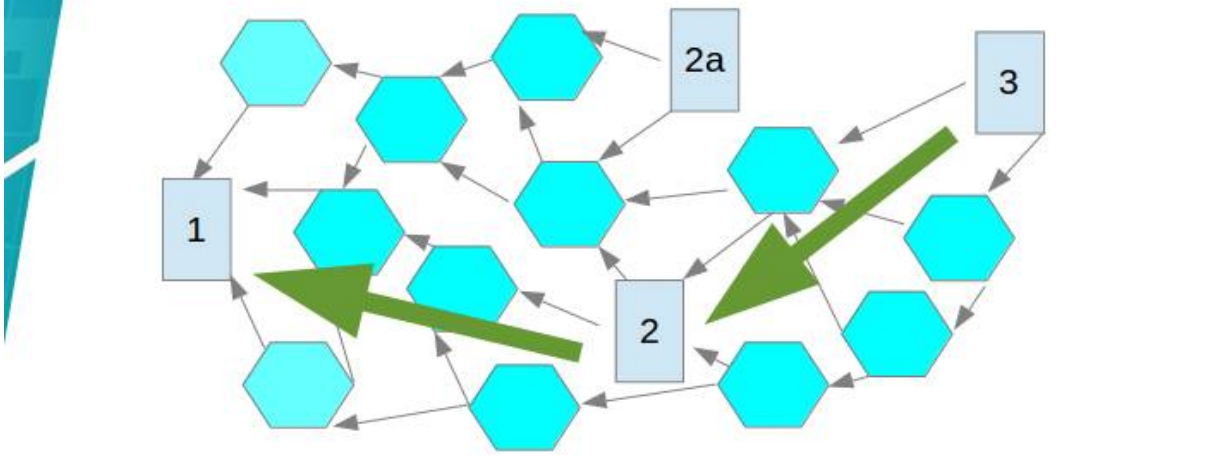
The Bigtangle is a decentralized cryptocurrency, payment, exchange, supply chain and e-commerce platform with the advantages:

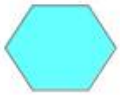
1. Near-Time Transactions ,
2. Infinite Scalability,
3. Smart Contracts, Permissionless, Trustless,
4. Decentralized Exchange,
5. Ease of use,
6. Completely Feeless,
7. Quantum Security.

Bigtangle is inherently a client and server architecture. The Bigtangle requires the same power consumption as Bitcoin as any systems based on PoW.

However, comparing the transactions per seconds (TPS), e.g. 10 TPS in Bitcoin or 200 TPS in Ethereum, Bigtangle with 10 server nodes in our clusters can achieve 1 Million TPS with the same power consumption. Big Data and blockchain parallelization are the only solution to get significant TPS at affordable costs. Keep in mind that replacing other technical processes with the Bigtangle network will also reduce total power consumption.

Maximum security, decentralization, scalability by integration into a genealogical tree





Block with Transactions. Transactions are usually independent except for double spends. The MCMC consensus algorithm performs the selection process to solve conflicts.

Mining Reward Blocks are blocks with coinbase transactions only. Mining reward block must be in a chain over the Tangle. In the example above, blocks 1, 2 and 3 are such a chain. Let blocks 2 and 2a be in conflict. The MCMC consensus algorithm will solve this conflict by (in this case) having selected block 2 due to higher rating.

Subtangle

The Bigtangle software can be deployed in private or other trusted environments, allowing one to run private, owned Bigtangle networks with different rule sets.

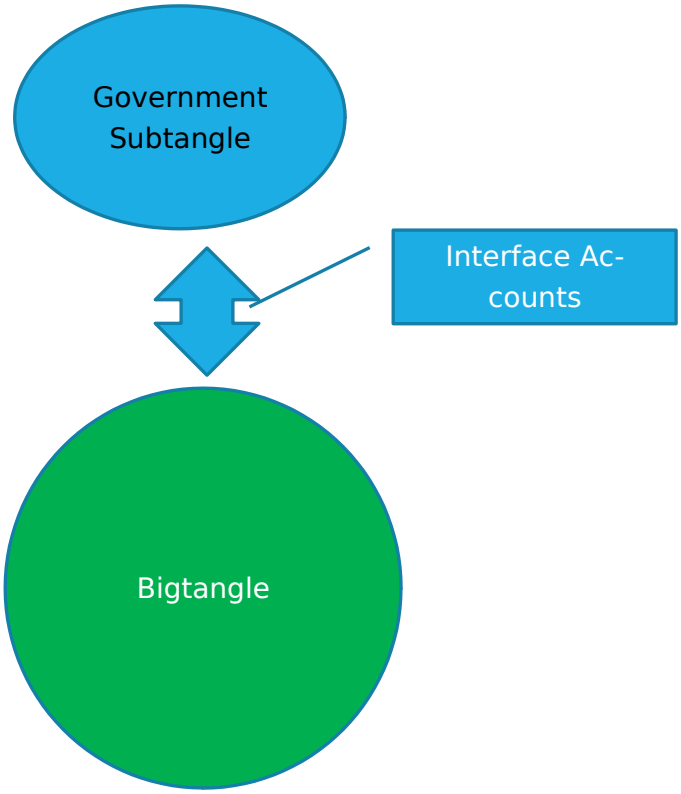
These Bigtangle networks are arranged in a hierarchy, i.e. they possess a parent Tangle such as the Mainnet between which a transfer of values is facilitated. For this purpose, each new Subtangle has its own interface accounts (addresses) possessed by the private operator from which it is possible to transfer funds into the parent Tangle and vice versa.

A user interested in transferring funds from the parent Tangle into one of its registered child Tangles can transfer tokens to one of the child Tangle's interface accounts, at which point they are either accepted into the child Tangle or returned by the trusted intranet owner.

Inside of such intranets, consensus protocol, transparency, permissiveness and other rules are set by the trusted intranet owner. Transfers of value can be performed internally as it is pleased. For example, in a work agency intranet it would be possible for clients to pay values to work forces in private and in arbitration of the owning work agency.

In general, enterprises and governments can deploy the software internally and e.g. do KYC (Know Your Customer) as well as privacy protection while remaining compatible with Bigtangle's Mainnet.

This allows Bigtangle to offer a holistic and flexible approach to value management, enabling privacy, transparency and accountability wherever needed by banks, stock exchanges or enterprises.


Government
Subtangle
Interface Ac-
counts
Bigtangle

Use Case for Government as Identity Issuer

1. Government create a domain in bigtangle, for example id.gov
2. Government create a token for ID card of person, where token name must be the public key of the user. The data will be saved as encrypted data of the token with the public key of the government.
3. Government transfers the token to user account and encrypt the identity data using the user public key. A digital identify is created only for a given public key
4. Government can revoke the token and an application can validate the digital identify.
5. User can request new digital identity for new public key.

Use Case for IDNOW as ID service provider on Bigtangle

1. IDNOW create a domain id.idnow.de
2. IDNOW check the paper form ID cards and then create a token for ID card of person, where token name should be the public key of the user. The data will be saved as encrypted with the IDNOW public key.
3. IDNOW transfers the token to user account and encrypt the data using the user public key.
4. IDNOW can revoke the token and an application can validate the digital identify.
5. User can request new digital identity for new public key.

Use Case for ePerso as eID service provider on Bigtangle

1. create a domain eid.eperso.de
2. Install a Bridge server for ePerso service.
3. User login to this server by using PIN, smartphone and NFC.

4. The server get the permission from user and read identity data and then create a token with this data, where token name must be the public key of the user. The data will be saved as encrypted with the service provider public key.
5. The service provider transfers the token to user account and encrypt the data using the user public key.
6. The service provider can revoke the token and an application can validate the digital identify.
7. User can request new digital identity for new public key.

Use Case for check and validation

1. Enable the authentication of the digital ID for service using Bigtangle Wallet.
2. Self-Sovereign Identity: Instead of logging into Wechat, Facebook, Uber, et al, you will log into your own self-sovereign browser, and will have the same ability to rent a hotel room, use social media or hail a car.

Identification

Information on the identification, in the languages of the issuing state plus English, accompanied by numbers that refer to an index that lists the meaning of these fields in all languages:
On the top of the identification page there is the code "P" for passport, the code (ISO 3166-1 alpha-3) for the issuing country, and the passport number. On the left side there is the photo. On other places there might optionally be a national identification number, the height and security features.

- Code
- national identification number,
- Surname
- Forename(s)
- Nationality
- Date of birth
- Sex
- Place of birth
- Date of issue
- Date of expiry
- Authority
- Signature of holder
- Photo

- machine-readable
- Name at birth

All above use cases are implemented in Bigtange. The detail description can be found in Bigtangle user guide. We show here only two important functions.

Create a domain for issuer

Bigtangle has a distributed domain name service similar to internet domain name system. There is system group to enable the creation of top domain name gov, com etc. The owner group of top domain can create new sub domain with multi signature. The domain name is unique and protected by multi signature. All token belongs to a domain name and is then also unique in the form of tokenname@domainname.

Create a Token as digital ID

The identity will be created by domain owner group. The identity is issued on the given public key and it is only valid for this public key. The identity data is encrypted by user public key and has a signature of issuer to verify the identity. All identity data are encrypted except the date of expiry.

Transfer digital ID to user.

The identity token can be transferred to user public key address with encryption. It cab be checked using public balance that this address has a token with full name as publickey@id.gov.

Authentication Service

The Bigtangle wallet supports the authentication service standard FIDO2. This enables the password-less, reliable, secure and Multi-factor authentication service.

> At its core, FIDO2 consists of the W3C Web Authentication (WebAuthn) standard and the FIDO Client to Authenticator Protocol (CTAP). FIDO2 is based upon previous work done by the FIDO Alliance, in particular the Universal 2nd Factor (U2F) authentication standard.

> Taken together, WebAuthn and CTAP specify a standard authentication protocol[2] where the protocol endpoints consist of a user-controlled cryptographic authenticator (such as a smartphone or a hardware security key) and a WebAuthn Relying Party (also called a FIDO2 server). A web user agent (i.e., a web browser) together with a WebAuthn client form an intermediary between the authenticator and the relying party. A single WebAuthn client Device may support multiple WebAuthn clients. For example, a laptop may support multiple clients, one for each conforming user agent running on the laptop. A conforming user agent implements the WebAuthn JavaScript API.

As its name implies, the Client to Authenticator Protocol (CTAP) enables a conforming cryptographic authenticator to interoperate with a WebAuthn client. The CTAP specification refers to two protocol versions called CTAP1/U2F and CTAP2. An authenticator that implements one of these protocols is typically referred to as an U2F authenticator or a FIDO2 authenticator, respectively. A FIDO2 authenticator that also implements the CTAP1/U2F protocol is backward compatible with U2F.

For example to create single sign service for web application using Bigtangle android apps.

The apps send a request to web server with a public key and get a secure access token, which is signed by the public key of apps. The wallet

can decrypt the secure access token and signs the secure access token and send the signed message as header in the web request to web server. The web server verifies the secure access token and can create session, if the verify process is successful.

For two factor authentication service, the computer transfers the signed secure access token to Bigtangle blockchain using multi signature and the user get the signed token and decrypt it for login on the computer. The Bigtangle wallet can be installed on USB device for local and direct authentication.

Live Person Authentication

Download the real person authentication APP from https://bigtangle.oss-cn-beijing.aliyuncs.com/app/identity_verify.apk, and run the real person authentication APP after installation.

After entering the user name, password and the password of the big net wallet (if the wallet is encrypted), click the "Real Person Authentication" button to start the real person authentication process.