



Tokenisation: The Technical Aspect

Author(s): Michael Waechter / Jonnas Porminal

What is Tokenisation?

Before answering this question, we should first define what is a TOKEN.

A token in the cryptocurrency space is a unit of value issued by an organization that is supported by an existing blockchain. Tokens can be grouped into several different types. Each token type provides unique features and can be best described by how they serve the end user. We will use the groups as defined by FINMA, the Swiss financial regulator:



PAYMENT TOKENS

Payment Tokens are tokens intended to be used as a means of payment for acquiring goods or services. These tokens often function like traditional currencies and usually have no underlying assets.



UTILITY TOKENS

Utility Tokens are tokens which are intended to provide digital access to an application or service.



ASSET TOKENS

Asset tokens represent assets such as participations in real physical underlyings, companies, or earnings streams, or an entitlement to dividends or interest payments. In terms of their economic function, the tokens are analogous to equities, bonds or derivatives.

This article will talk about Asset Tokens, therefore we speak about "tokenisation" in the context of representing assets through tokens. This is important to be noted, as representing assets like for example shares, bonds or derivatives comes with additional requirements like the possibility to pay dividends or interest to the token holders or limitation in the ownership. Such demands have to be addressed by the technical solution provided.

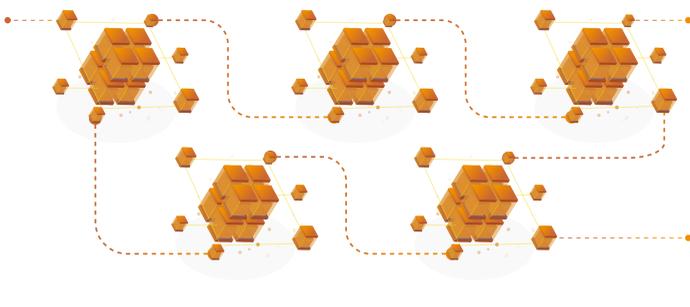
What is the Technical Foundation for Tokens?

Tokens are based on the blockchain technology, which allows to register the ownership and characteristics of a token in a distributed ledger. There are several blockchain platforms that provide a technical base to register tokens, for example Ethereum, Stellar, Hyperledger, R3, Ripple, or EOS. Each platform offers a set of functionalities. This set of functionalities is one of the factors taken into consideration by the developer to choose the best fitting blockchain technology. Other factors can be whether it is an open source technology or not, the size of the community using the technology, the number of distributed ledgers etc.

The blockchain is a system of distributed ledgers, that makes it difficult to change once recorded information. The token uses this system to ensure, that the definition of the token itself and its ownership can't be manipulated after it is recorded.

About Distributed Ledgers and Blockchain

A blockchain is a decentralised, distributed digital ledger that consists of records called blocks. The blocks are interlinked by using the hash (the output of a hashing algorithm, which produces a fixlength string unique for each document) of the prior block as part of its own hash. The effect is, that any change in an older block leads to a change of the hash, which is immediately reflected through the whole blockchain, as each following block includes the now changed hash of the prior block.



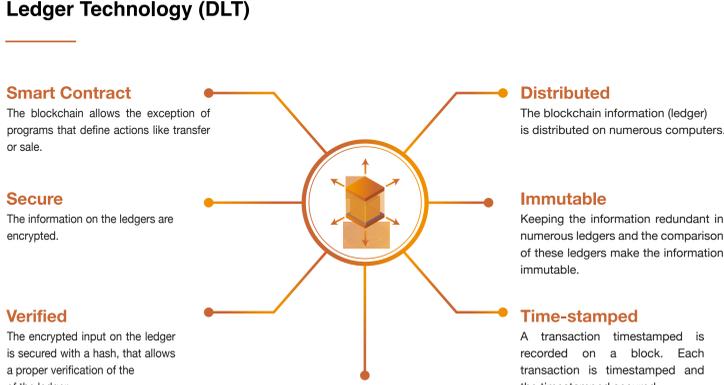
Mining is an additional security feature that secures the data stored on the blockchain: The blockchain system defines a characteristic of the hash (for example it has to start with "222"). "Mining" is now the process of "trial and error" to find a string of data, that gives the hash the desired characteristic. This process needs a lot of calculation power and the mining party is paid for its effort.

The additional security gained by mining is not just the shared and easily identified characteristic of the hash, but also the process of getting it: The time needed to search the data string is an additional security against manipulation of the data. Having said that: This inefficient "trial and error" is one of the major points of critic for the blockchain technology, as the energy required for mining in case of a big network is huge.

The blockchain of each token is duplicated and distributed across a (in a best case) big network of computer systems. The validity of the information (in this case the definition of the token and its ownership) is verified by comparing the hash of the last block in the blockchain on computers of the entire network. The hash of the majority of computers is considered to be the valid one. This makes it close to impossible to alter information retroactively.

The organisation of the distributed ledger is dependent on the blockchain system. Some of the systems consist of a very small number of computers (for example the Binance Smart Chain), where as others (for example Ethereum) are based on a huge network of distributed ledgers. When choosing a blockchain system, the size of the blockchain community and the number of ledgers play an important role together with the functionalities offered by the respective blockchain. On the other hand: Smaller networks require less energy for the mining process, an advantage that should be considered as well.

Properties of Distributed Ledger Technology (DLT)



About Smart Contract

A Smart Contract is piece of computer program stored on a blockchain that is executed automatically when a predetermined condition is met. Smart contracts are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome without any involvement of an intermediary.

Smart contracts aims to remove the human factor of decision making, which is proven to be the most error prone and unreliable element of the standard traditional contracts. Smart contracts are programmed using an if-then logic making them easy to code and seamless. The actions defined in a smart contract are executed by a network of computers when a predetermined condition is met and verified. These actions could include transferring funds to appropriate third parties, approving a loan request and etc. Once a contract is deployed and executed in the blockchain, it can't be stopped or altered. This gives a strong safety in regards to the fulfillment of contractual obligations.

It is important to note that not all the blockchains allow to program Smart Contracts. This is another important element to distinguish and to select the best fitting blockchain system.

About the Ethereum Technology

Ethereum blockchain technology was started in 2013 by Vitalik Buerin as an open-source, blockchain based distributed platform. Ethereum quickly became the industry standard as it provides a strong base for the programming and execution of smart contracts. Most of the blockchain systems available today are further development of the Ethereum blockchain technology.

Ethereum is supported by the Ethereum Enterprise Alliance (EEA), which is a non-profit organisation with members like Microsoft, Intel or JP Morgan Chase, who understand the technology to be a standard for the blockchain technology. Ethereum has a large online community, which supports product enhancements and updates.

Its large size is one of the disadvantages in comparison to blockchain technologies, that have a more centralised decision making process and smaller communities: It is slower in adapting new trends and technologies.

One special element of the Ethereum platform is Ether, its widely accepted own crypto currency. Ether facilitates the payment of the miner that work with the Ethereum system. This gives the platform an additional edge over its competition.

Although Ether is crypto currency, its purpose differs from crypto currencies like for example Bitcoin. Bitcoin was created as an alternative currency to FIAT money, the money defined by governments, where as Ether was mainly created to support the transactions on the Ethereum platform.

Both crypto currencies, Bitcoin and Ether, are based on the blockchain technology with distributed ledgers, they differ for example in the hash used. One major difference is in the smart contracts: The Bitcoin technology does not support the use of smart contracts on its blockchain. That's why Bitcoin is mainly a crypto currency, where as Ether is seen in the context of the Ethereum technology to facilitate the operations on this platform.

How to Use Tokens as Asset Tokens

Ethereum platform created a special protocol for the creation of tokens, the ERC20, which stands for Ethereum Request for Comment with 20 as the identifier of the version of the standard. Tokens based on ERC20 have become particularly popular as the token of choice for ICOs (Initial Coin Offerings).

The ERC20 protocol contains several functions required by tokens to comply with this standard:

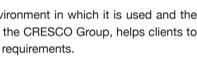
- TotalSupply**: The total token supply.
- BalanceOf**: The account balance of a owner's account.
- Transfer**: To execute transfers of a defined number of tokens to a specified address.
- TransferFrom**: To execute transfers of a defined number of tokens from a specified address.
- Approve**: To allow the withdrawal of a set number of tokens from a specified account
- Allowance**: To return a set number of tokens to a specified account.

The ERC20 protocol is the base for new protocols, that address specific requirements like the change in the total token supply (ERC621) or better handling of the approval process (ERC223). Developers are free to add functionality as long as they fulfill the minimal requirements of a standard.

This allows to address topics like the identification of the token holder, limitation of ownership based on nationality or imposing of a minimal holding period. Some of these add-ons are required for compliance with the jurisdiction of the issuing entity or based on the nature of the token (enabling of dividends or interest payment to the token holders).

The token protocol has to be chosen based on which blockchain system is chosen, the legal environment in which it is used and the specific use of the asset token in regards to the underlying asset. CRESCOTec, the IT company of the CRESCO Group, helps clients to define these parameters based on their business case and programs the token according to these requirements.

The Token Protocol of SECDEX

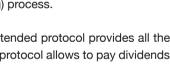


SECDEX is a Seychelles based Securities, Commodities & Derivatives Exchange. Hensley&Cook, the corporate service specialist of the CRESCO Group, is a sponsor on SECDEX and lists companies on this stock exchange as part of a normal IPO. In addition, SECDEX allows the listing of tokens on its platform and provides solutions to customize assets and issue tokens against the asset in custody. Hensley&Cook helps clients in this process and supports the whole ICO (Initial Coin Offering) process.

The token of choice for SECDEX is a Ethereum based token with an extended ERC20 protocol. The extended protocol provides all the functionality required by the Financial Service Authority Seychelles, the regulator of SECDEX. The token protocol allows to pay dividends to token holders and to support compliant trade, for example based on Smart Contracts.

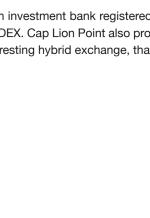
CRESCOTec has the expertise to guide and support the process of tokenisation for the use in the SECDEX environment. This allows clients to get the tokenisation done from A to Z from experts of the CRESCO Group.

E-Wallet from Cap Lion Point



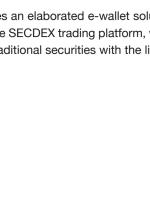
Cap Lion Point, an investment bank registered in the Seychelles, provides an elaborated e-wallet solution to keep asset tokens as used by SECDEX. Cap Lion Point also provides an easy access to the SECDEX trading platform, which enables the users to tap into this interesting hybrid exchange, that combines the listing of traditional securities with the listing of tokenised assets.

Meet the Authors



Michael Waechter

Michael is an entrepreneur with strong insights into finance, financial structuring and corporate advisory.



Jonnas Porminal

Jonnas is an IT specialist experienced in blockchain technology and the creation of tokens and related smart contracts.

