BIZCOMMUNITY

Blockchain? It's simpler than you think

Issued by Mesh Trade

22 Jun 2020

The exchange of products, such as cash for securities, can be a complex trust arrangement and requires the help of an intermediary. For example, when you buy a home, lawyers operate as the middlemen to ensure nobody gets conned. Escrow accounts also fall into this definition.

At a more technical level, this arrangement is enforced by a Delivery versus Payment (DvP) mechanism. Codified into regulations during the 1980s, DvP is a cornerstone of trustworthy financial transactions and a critical intermediary role.

Then how would it work if a DvP is part of a decentralised ledger, where there are no apparent intermediaries to keep everything honest?

For some, the concept of a distributed ledger seems problematic because it proposes precisely that situation. You may have encountered the idea in the blockchain world. Blockchain is one type of decentralised ledger system where centralised intermediaries are no longer required, and DvP actions can operate seamlessly on such a system. But decades of doing it the traditional way has developed some scepticism about how this approach would work.

A new type of atomic transaction

A DvP transaction is an atomic transaction – meaning that if either side's instructions are not included or followed, the entire transaction should implode. Yet whereas an intermediary would trigger that implosion, in a distributed ledger it's automatically part of the DNA.

There are two DvP scenarios: one on the same ledger and one between two different ledgers. Both scenarios make use of the following concepts:

- Hash function: this is a unique code created by a crypto algorithm that represents a specific digital asset. For example, if you produced a hash from a photo, that hash can be used to test if the photo is authentic. If someone tampered with the photo since the hash was generated, it would not respond to or produce the same hash.

- Private and Public crypto keys: a private crypto key is one half of a secure and unique arrangement, and only known to the key's owner. The public cryptokey is the other half, generated mathematically from the private key. Anyone can have access to the public key – this key is used to communicate securely with a private key holder, or to verify a private key signature.

- Digital signature: a digital signature is created using the above-mentioned tools and other information. The signature can be verified by anyone who has access to the public key, yet can't be duplicated without the private key.

DvP in single ledger and cross ledger transactions

A decentralised ledger is when copies of a ledger are distributed between independent systems. When a change is made to the ledger, all the independent systems take a vote to decide if the change should be allowed. To defraud a decentralised ledger, you would have to convince the majority of the independent systems to vote for an illegal change to the ledger.

A ledger could be entirely within an organisation, spread across different companies within a sector or any other configuration. The more participants there are holding copies of the ledger, the more transparent and honest the ledger maintenance becomes. There can be two scenarios. The first concerns a transaction happening on the same decentralised ledger. The second is when a transaction happens between two different ledgers.

In a single-ledger transaction, both parties create their respective instructions. The buyer digitally signs their instructions and attaches these to the seller's instructions. The seller then verifies the buyer's digital signature and signs their own instructions. This signature is verified, at which point the joint instructions – the atomic transaction – is verified and confirmed. It takes a total of four steps to achieve, and either party can validate the others' identity through their public keys.

A cross-ledger transaction requires eight steps, but the concepts are very similar. Different parties again create their own instructions, which are verified and confirmed separately. Each party will create buy and sell instructions on their respective ledgers. The fairness of this separation is managed through timelocks and a secret code. But it still uses the same cryptographic key and digital signature functions. Timelocks ensure that each party can get a refund if the other party does not want to play along. The combination of the timelock and the secret code is used to exchange the different assets without the different parties having to trust each other.

In both scenarios, there is no intermediary. Rather, the distributed ledgers ensure there is no tampering of the instructions, and the cryptographic functions such as the keys, hashes and signatures enable all stakeholders to validate the process.

Though there are some risks associated with these approaches, they return significant control to the transacting parties while still keeping the overall process honest and transparent.

Sometimes, eloquent simplicity can look very complicated, yet it isn't. Likewise, the simplistic beauty of a distributed ledger system can seem confusing through all the details. But it's not – and this is why blockchain and other distributed ledger technologies are more than revolutionary. They are the future.

- **Mesh.trade pioneers 'smart assets' a new frontier in capital markets** 6 Mar 2024
- **Tokenisation 101: A whole new world of investment opportunities, and why it matters** 22 Jan 2024
- **Finding Like Minds** 14 Aug 2023
- **All signs point to the emancipation of capital markets** 23 Jul 2023
- **Viva the (responsible and careful) revolution in financial markets** 22 Nov 2022

Mesh Trade

Mesh.trade is an institution-grade, multi-sided financial markets platform that facilitates trade in real-world financial assets on the blockchain, working towards a future where capital markets are easy to access, simple to use, and transparent.

Profile | News | Contact | Twitter | Facebook | RSS Feed