MFSA FinSights | Enabling Technologies

Distributed Ledger Technology

The financial sector is continuously evolving through the rapid development and adoption of new technologies. The term 'FinTech' generally refers to financial innovation that seek to provide enhanced financial service offerings through the utilisation of enabling technologies. These generally include Distributed Ledger Technology & Smart Contracts; Artificial Intelligence, Machine Learning & Big Data, Cloud Computing, Web 3.0, Application Programme Interfaces and Micro-Services; Robotic Process Automation and the Internet of Things.

As part of the MFSA's initiatives to generate awareness, drive culture and deliver a cross-sectoral knowledge platform which can support the MFSA's functions in preparing for the financial services of tomorrow, these insights will delve into enabling technologies, enabling innovations and their sectoral applications.

1 What is DLT?

Building on the developments of the 1980s, namely the use of distributed databases[1] and the cypherpunk movement[2], Distributed Ledger Technology ('DLT') refers to the *"protocols and supporting infrastructure that allow computers in different locations to propose and validate transactions and update records in a synchronised way across a network" (BIS 2017, p.* 58). While such distributed ledgers systems have been in use for decades, newer applications of this technology have allowed for decentralised, distributed and immutable ledgers which maintain the integrity of the shared ledger[3] through consensus and cryptographic mechanisms rather than through a trusted central administrator.

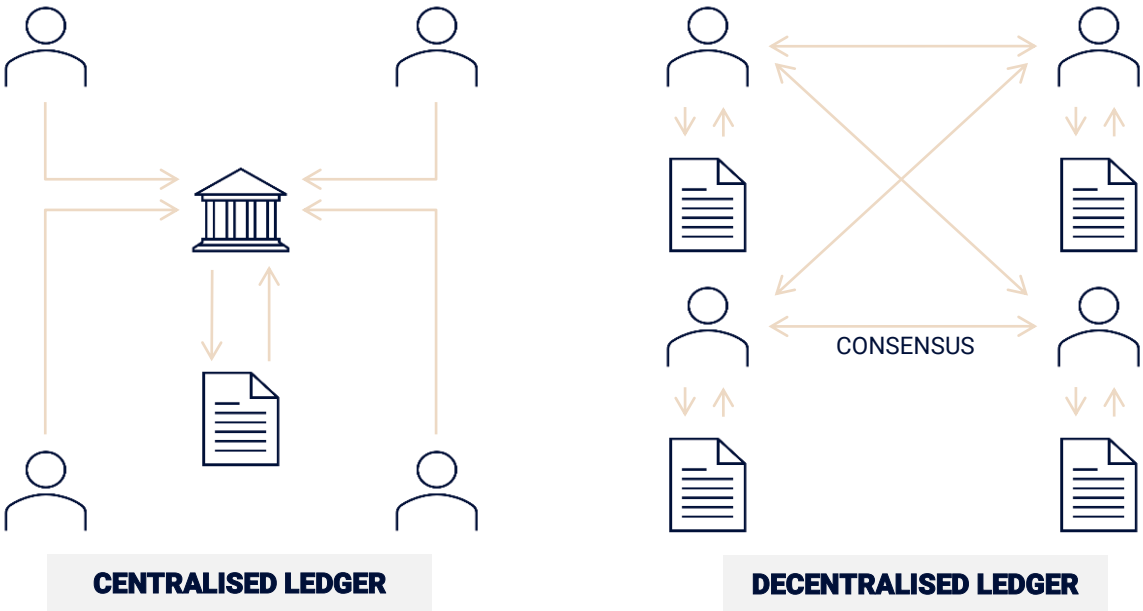

FIGURE 1: CENTRALISED VS DECENTRALISED LEDGERS
Source: BIS (2017)

[1] Distributed Databases – Prior to the 2008 Bitcoin Whitepaper, distributed databases relied on a *"system administrator to perform the necessary key functions to maintain consistency across the multiple copies of the ledger. In its simplest forms, this was done by periodically updating and sharing with all network participants a master copy of the ledger held by the administrator."* (BIS 2017, p.58)

[2] Further information on this movement may be found within the '*A Cypherpunk's Manifesto*', published in 1993 by Eric Hughes, here.

[3] Shared ledger is a broader category of Distributed Ledger ('DL') and refers to technologies which enable the sharing of a record of data across different parties (World Bank, 2017).

DLT encompasses a myriad of innovations. Since the 2008 seminal whitepaper by Satoshi Nakomoto on '*Bitcoin: A Peer-to-Peer Electronic Cash System'* various implementations of this technology have been explored with varying features, including (i) the **distributed nature of the ledger**; (ii) the **consensus mechanisms**; and (iii) **cryptographic mechanisms**.

Another important concept is **Forks**. A fork occurs whenever the DLT system is forced, either accidently or intentionally, to have two diverging paths. A fork may also be classified as hard or soft depending on the level of changes made to the chain, wherein soft forks are akin to software upgrades which maintain compatibility across whilst hard forks cause incompatibility across chains.

1.1 Distributed Nature of Ledger

Distributed ledger systems can be permissionless or permissioned depending on who controls access to the network. **Permissionless systems** allow open network access to all users participating ('nodes') on the DLT, with users only requiring a computer server with the appropriate software to conduct transactions. Alternatively, in **permissioned systems** access is controlled by an administrator or a predefined and limited number of participants, which also enforce the rules. **Hybrid systems** also exist which make use of permissionless and permissioned structures.

1.2 Consensus Mechanisms

As the name implies, consensus mechanisms allow users of the network to achieve consensus on the validity and legitimacy of the transaction of data being conducted on the DLT. These rules are specified in the algorithmic design of the DLT as predefined cryptographic validation mechanisms. While the main formats include, **Proof of Work ('PoW')** and **Proof of Stake ('PoS')** other methodologies, such as, **Proof of Elapsed Time ('PoET')**, **Proof of Authority ('PoA')**, **Proof of Burn ('PoB')**, and **Proof of History ('PoH')** have been explored.

PoW, which is used by amongst others by the Bitcoin Blockchain, consists of a computationally intensive mathematical puzzle which solved by competing network participants, call *miners,* which are incentivised to validate such transactions over the network to claim the transaction fees and newly mined tokens.

On the other hand, PoS, requires participants, called *validators*, to stake their funds to indicate commitment to the network. In general, the amount and the time during which the participants funds are locked in the network act as the determining factors for publishing new blocks. Hence, the likelihood of the participant publishing a new block and claiming the reward is linked to the aforementioned factors. One of the most prominent DLT systems to date, the Ethereum Blockchain, uses this protocol.

1.3 Cryptographic Mechanisms

Cryptography is at the core of secure data flows, especially in DLT, as it allows users to transact data securely over the network whilst maintaining the integrity of the ledger. Some basic cryptographic mechanisms used in DLT include **hashing functions**, **elliptic curve cryptography** and **asymmetric encryption**:

1. **Hashing functions** are one-way functions which scramble information into unique fixed length outputs or digest which cannot be decrypted. Various hashing functions exist, including Secure Hashing Algorithm (with SHA-256 and SHA-512 mainly being used in DLT), Message Digest Algorithm ('MD5') and Cyclical Reduction Check ('CRC32').

2. **Elliptic Curve Cryptography** is a method of encryption used to support the decentralisation of shared ledgers as it is used to generate transactions signatures which prove their legitimacy over the network.

3. **Asymmetric encryption** allows for the encryption of data by means of **private and public keys**. Private keys, which are private to the user, encrypt data whilst the public keys, as the name implies, are available to everyone and allow for decryption.

Another mechanism used in certain implementations of DLT is **Zero-knowledge Proofs** or **Zero-knowledge Protocols.** Such protocols allow parties to prove that the data is true without the need to reveal the content of the information and the details of the users. This mechanism also allows for greater anonymity within DLTs as most applications of DLT to date not using Zero-knowledge Proofs are pseudonymous and thereby allow for traceability of user's identity and transactions.

2 DLT and Crypto-Assets

Satoshi Nakomoto in 2008 introduced 'Bitcoin' as the first such DLT based **cryptocurrency** that is fully decentralised, and which did not require a trusted authority to function. This innovation eliminated the need for trust across one or more authority, such as banks. This proposed blockchain technology incorporated several computing concepts, as discussed, to create the first instance of electronic cash protected by cryptographic mechanisms. Although other electronic cash arrangements existed prior to Bitcoin blockchain (e.g., NetCash and Ecash) none have achieved a widespread adoption because unlike its predecessors, the Bitcoin blockchain is implemented in a truly decentralised and distributed nature.

Building on the Satoshi's development, in 2013 Vitalik Buterin conceived Ethereum which allowed users to attach value to the cryptocurrency using **Smart-Contracts**, thus paving the foundations of the crypto-assets we have today.

3 Benefits and Risks

Distributed ledgers have several advantages over traditional centralised ledgers and have the potential to enhance existing systems, business processes and applications, however the technology is still evolving, and many technological, regulatory, and legal issues have not, as yet, been resolved. This in turn brings about certain challenges and risks that require careful consideration prior to the implementation of DLTs in financial sector. Below are some of the benefits and risks of such systems.

BENEFITS

Decentralisation and Disintermediation - The disintermediation brought about by DLT enables direct transfers of value between participants and provides for decentralised record-keeping, which in turn lowers costs, enhances scalability and time-to-market.

Immutability and Verifiability - DLT provides for an immutable and verifiable audit trail of transactions of any digital or physical asset maintained on such a system.

Transparency and Auditability - Given that participants have open access to the complete copy of the distributed ledger and that updates to the ledger may only take place once the network consensus is achieved and are then propagated over the entire network, DLT allows for auditability and transparency among participants. This also enables the reduction of fraud and reconciliation costs.

Efficiency - Through disintermediation and automation, DLT has the potential to lower inefficiencies and reducing frictions in transactions and/or in clearing and settlement.

Cybersecurity and System Resilience - In view of the features mentioned above, DLT is seen as a more resilient and secure alternative to traditional centralised databases, even more so with the advent of Quantum Computing.

RISKS

Maturity - The nascent nature of DLT raises certain questions on its robustness and resilience, in terms of transaction throughput, scalability options, availability of standardised software applications and skilled professionals.

Scalability - Certain implementations of DLT, such as the Bitcoin blockchain which can only process between 4 to 7 transactions per second. This has raised scalability concerns in terms of transaction volumes and validation speed.

Governance - Depending on the nature of specific DLT, such structures may inherently pose governance challenges relating to the decision-making process. Proposals for alterations in Bitcoin and Ethereum Blockchain protocols have showcased how complex and contentious it is to reach decisions on critical updates in such systems. Additionally, regulation has traditionally placed the onus of instituting effective internal control and governance through centralised structures such as a legal person's management body.

Accountability - Further to Governance issues, the lack of centralisation may create accountability and liability matters given that it may be practically impossible to identify parties accountable for governance of the network.

Immutability - While such a feature is desirable, under certain scenarios such as in the context of reversals and/or dispute resolution, immutability may not be warranted.

Privacy - Depending on the nature of specific DLT, especially public implementations, such system may only allow for pseudo-anonymity as all transactions and addresses are open and visible to all network members. On the other hand, by virtue of their design public DLTs may also facilitate the concealment of identities and/or do not require identification and verification of participants prior to being admitted to the network.

Interoperability and Integration - In case of various DLT implementations, interoperability with other DLTs and integration with existing systems are crucial of the adoption and scalability. Such features are costly to implement, requiring industry-wide coordination and collaboration.

To conclude, nowadays, DLT, and all its variants have enabled the issuance of new platforms such as BNB, XRP, Cardano, Solana and Polkadot, with possible use cases spanning beyond the financial services sector, including trade and commerce (supply chain), education, health, agriculture, and food industries.

Supplementary Reads…

International Bank for Reconstruction and Development / The World Bank (2017), Distributed Ledger Technology (DLT) and Blockchain. *FinTech Note | No. 1*. Available online.

Bank of International Settlements (BIS) (2017), What is distributed ledger technology?, *Extract from page 58 of BIS Quarterly Review. Available online.*

Check our other **FinSights** and should you have any queries or wish to discuss your ideas, even within the context of our **MFSA Fintech Regulatory Sandbox**, contact us at **fintech@mfsa.mt**.