Blockchain and Distributed Ledger Technology - Transforming the Financial World

Often in the news, Blockchain is set to transform the way the financial markets operate, revolutionising the industry at every sector.

Elementum Metals: 25/02/2021

25/02/2021

To accompany our webinar on the emerging Blockchain sector (which you can view on the past events page), we have answered some of the questions our audience asked, encompassing technical enquiries, compare and contrasts, and even the influence of internet memes.
Got another question for our team? Use our contact page to get in touch.

What are the differences between public, private and permissioned Blockchains?

Public Blockchain: Is a Blockchain where anyone can join and participate in the activities of the Blockchain network. These blockchains are decentralised, meaning no single entity with have control over the network. Popular examples include Bitcoin and Ethereum.
Private Blockchain: A Blockchain that only allows authorised members to join the network. The operator has rights to override, edit or delete the necessary entries on the Blockchain. There is centralisation here. Examples include Ripple and Hyperledger.
Permissioned/Hybrid Blockchain: Has properties of both private and public Blockchains. They are becoming increasing popular due to their ability to allocate specific permissions to various users on the network. This varies from platform to platform, and many are much smaller than more established names.

The investment thesis behind decentralized finance is very sound - unprecedented money printing by central banks will likely lead to debasement, and a non-fiat store-of-value is a great way to protect against this. My question is

- why Blockchain? What advantages does it have against other secure payment networks? In the case of Bitcoin, it seems clunky - energy intensive, dogged history (black market), and the fact that every transaction needs to be verified by everyone in the world seems inefficient?

A great question, with a couple of components to answer. First, why use Blockchain for payments? Blockchain is immutable, democratic, decentralized, and written in code that cannot be altered. This gives it an unassailable advantage over other secure payment networks (Stripe, Apple Pay etc.), which are fundamentally centralized. If I make payment using one of these companies, that transaction is verified, approved and managed by that single centralized company. This can be associated with security risks (a single centralized target for hackers), higher costs (a single centralized body can charge fees on transactions) and undemocratic (a single centralized company can set their own terms and conditions). Blockchain, on the other hand, allows the infrastructure to be built from the ground up. This means that you design and define the economics and monetary supply once at the beginning, and no-one can “print” additional money at a later stage – this helps with the ‘store of value’ advantage that you mention. Bitcoin tried to do this (it has a limited supply of 21 million bitcoins that can be mined), but as you say, it’s associated with many inefficiencies, not least the intensive energy use required to mine the coins (see question 4, below, for more on this). Each transaction needing to be verified by other users should not be considered one of these inefficiencies, however, but rather as a strength of the system – it sidesteps the need for a centralized (and therefore vulnerable and potentially costly) platform inherent with other secure payment systems.

Whilst you are within your rights to flag the black market history of Bitcoin, this is more a reflection of the activities of early adopters, rather than a sign of any weaknesses – few would argue that physical currency should be totally discounted due to it having been used for nefarious reasons in the past.

So what else might be out there? New Blockchain-based payment concepts are emerging, for both wholesale and retail payments, some being decentralized, some more centralized. Examples of these include:

- Ripple: used for decentralised inter-banking and cross-border payments, settling transactions in 3 -5 seconds worldwide and handling 1,500 transactions per second using XRP.
- Diem (ex-Libra for retail): A permissioned Blockchain payment system proposed by Facebook.
- CBDCs (Central Bank Digital Currencies): These are emerging across the globe with China launching the world’s first central bank digital currency known as the DCEP, which is a digital version of the Yuan, backed by Yuan deposits in Chinas Central Bank.

So, in conclusion, you are right in saying that Bitcoin is a clunky system with some obvious and increasingly well-publicized drawbacks (it remains to be seen if they can be remedied). However, the technology that underlies Bitcoin, i.e., Blockchain, allows far greater

However, the technology that underlies Bitcoin, i.e., Blockchain, allows far greater efficiency over other, more familiar, payment systems that have been developed over the last two decades or so.

What is the distinction between “proof of stake consensus” used apparently in new blockchains / cryptocurrencies and the one used for bitcoin (“proof of work”)?

The Proof of Work (PoW) mechanism is used to secure the Bitcoin Blockchain and to create consensus. It works by having all nodes (participants/devices) in the network solving mathematical algorithms (in order to verify transaction as legitimate), with the first node finding a solution being rewarded (the miner reward is a number of Bitcoins). PoW provides further security benefits to Blockchain as it slows down the creation of a new block to approximately 10 mins, meaning if a hacker wants to tamper with one block, they must re-do the PoW of every block in the system which is nearly impossible to do due to the scales involved.

The negatives associated to PoW however are as follows:

i. Due to the mining rewards, large and larger mining firms are being created, consuming vast amounts of electricity (it was recently widely reported that Bitcoin mining consumes as much energy as the whole of Argentina).

ii. To increase chances of a successful mine, miners group together in “mining pools” which actually makes the Blockchain more centralized, thereby undermining the decentralizing ethos of the endeavour.

In online forums in 2011, a new algorithm was proposed called Proof of Stake (PoS), where instead an election process is used in which one node is randomly chosen to validate the

next block. Instead of miners, it uses validators that mint/forge new blocks. To become a validator, the node must deposit a certain number of coins as stake (think of this as a security deposit). The more you “deposit” the higher chance you will be a validator. This is fairer than PoW, as PoW favours those who have economies of scale in terms of their mining capital/energy, whereas the barriers to entry with PoS are comparatively lower. To ensure correct validations occur, validators will lose a part of their stake if they approve fraudulent transactions. As long as this loss is larger than their reward, the consensus holds up through price motivation. Lastly, PoS is more decentralized as it stops mining pools and its cheaper to set up a node within the PoS blockchain.
The negatives associated to PoS however are as follows:
i. 51% Attacks: Unlike PoW where you must acquire 51% of the network, for PoS you must acquire 51% of the market cap of the currency, which for small market cap cryptocurrencies could be relatively easy.
ii. PoS algorithms are not completely random as it depends on the stake of the validators (which can favour richer individuals).
At the moment, PoS is not common, although it is anticipated that the system will be used in Ethereum 2.0, to be released in 2021.

Any comment on Tesla and decision to buy Bitcoin rather than another form of digital asset? Is it pure speculation?

From a corporate Tesla perspective, it could be a consequence of negative interest rates and treasury management looking at ways on how to diversify asset allocation. From a Musk perspective it’s hard to say what his most profound motivation was. He invested in both Bitcoin and Dogecoin, causing price increases in both cryptocurrencies after his announcement of the purchases on Twitter.
Musk is sitting in a special seat, he can try out technologies and concepts resulting in positive market response, independently of any economic or business reason. Analysts at Wedbush Securities have estimated Tesla have already made $1 billion in profit from its Bitcoin investment. The company is on trajectory to make more from its Bitcoin investments than profits from selling EVs in 2020.
As to choosing Bitcoin and Dogecoin over other cryptocurrencies, things are less clear. Bitcoin is by far the largest and most obvious choice, perhaps therefore perceived as being lower risk, whereas Musk himself has often cultivated an image as being plugged into online culture – Dogecoin, having been borne initially out of internet memes (as well as having a market capitalization well into the billions) could be interpreted as being part of this. It is worth noting, however, that he is not the only high-profile figure to publicly back the cryptocurrency: claimed entries from musicians Gene Simmons and Snoop Dogg have also helped to drive interest.

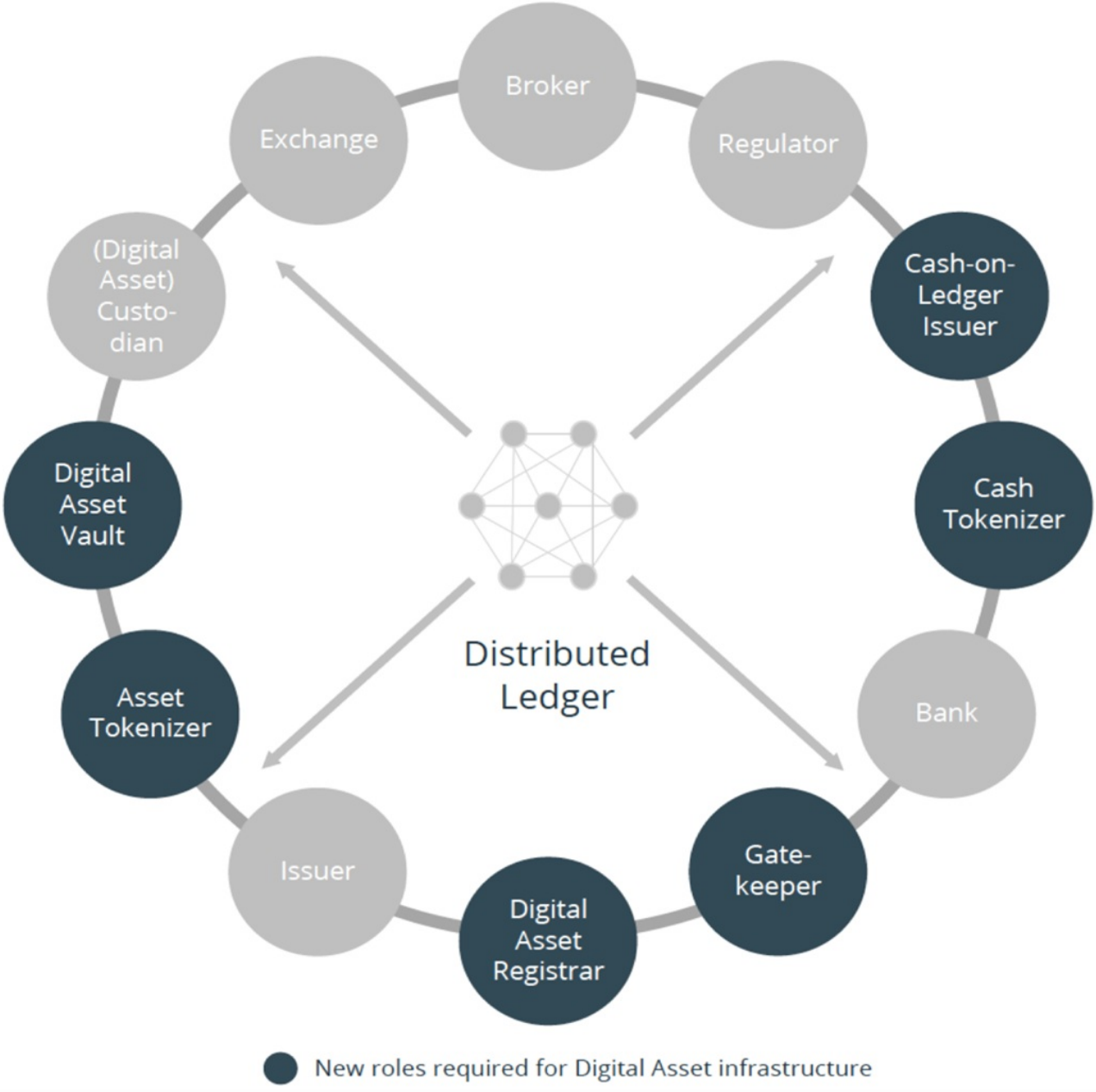
What’s the market capitalization of Decentralized Finance protocols?

As of February 2021, the market cap is 45 Billion USD.

How does Distributed Ledger Technology's (DLT) role in Capital Markets differ from traditional

role in capital markets differ from traditional stock exchanges?

Traditional exchanges present a bilateral, sequential way of communication and exchanging information. DLT has already begun to restructure capital markets value chains by changing traditional assumptions and creating trust without human operations.
DLT can add value to Capital markets through:
i) Shared information across all participants – reducing costs of reconciliation
ii) Smart contracts – Eliminating counterparty risk
iii) Immutable Audit trail – improved regulation
iv) Digitized processes – Allowing for pure automation
Most traditional roles in capital markets such as brokers, exchanges and custodians will continue to exist in a DLT capital market. However, new roles will be required in conjunction with the traditional ones. The diagram below illustrates this:



Source: Tokentrust AG
Changed features, properties and entities include:

- Custodians having digital asset vaults where they safeguard private keys required to access crypto wallets and hence assets.
- **Digital Asset Vault**, the software purchased by custodians to provide storage of

- **Digital Asset Vault**, the software purchased by custodians to provide storage of private keys.
- **Asset Tokenizer**, which enables legally compliant processes by providing smart contracts in order to tokenize financial instruments on behalf of the issuer.
- **Digital Asset Registrar,** that facilitates consensus across different stakeholders and governs the Digital Asset Registry via validating all transactions on the platform.
- **Gatekeeper**, that grants/restricts access to the platform via KYC/AML checks.
- **Cash on Ledger Issuer**, who manage the smart contracts and initiate fiat transactions through the bank and validate cash on ledger transactions.
- **Cash Tokenizer**, which provides infrastructure to issue 100% collateralized cash on ledger for on chain settlement (delivery vs payment settlement).

A real-world example is that of the Stock Exchange of Thailand which is creating an asset tokenization and exchange platform run by DLT. Information adapted from here.

What role do Central Bank-issued Digital Currencies (CBDC) play for the tokenization of capital markets?

Tokenization addresses the need for a dominant new format to represent assets and rights, bringing about greater flexibility and liquidity. As central bank money remains preferred for large transactions, CBDCs remain a promising medium for token-based exchange. They operate similar to the hard currencies but with digital opportunities. CBDCs can complement currency in circulation and serve as an alternative to card payments. Furthermore, they can facilitate diversified payment formats and allow for the exchange of tokens in central bank money, creating further confidence in tokenization. Lastly CBDCs facilitate direct payment relations, reducing the need for intermediaries and hence significantly reducing high transaction costs we traditionally see in capital markets.

Compiled by Jay Kumar, NTree International, for Metal.Digital.