Aaro Capital

An Introduction to Web 3.0

Disclaimer

The material provided in this document is being provided for general informational purposes. Aaro Capital Limited does not provide, and does not hold itself out as providing, investment advice and the information provided in this document should not be relied upon or form the basis of any investment decision nor for the potential suitability of any particular investment. The figures shown in this presentation refer to the past or are provided as examples only. Past performance is not reliable indicator of future results.

This document may contain information about cryptoassets. Cryptoassets are at a developmental stage and anyone thinking about investing into these types of assets should be cautious and take appropriate advice in relation to the risks associated with these assets including (without limitation) volatility, total capital loss, and lack of regulation over certain market participants. While the directors of Aaro Capital Limited have used their reasonable endeavours to ensure the accuracy of the information contained in this document, neither Aaro Capital Limited nor its directors give any warranty or guarantee as to the accuracy and completeness of such information.

Please be sure to consult your own appropriately qualified financial advisor when making decisions regarding your own investments.

Acknowledgements

Oscar Pacey and Peter Habermacher would like to thank Ankush Jain, Dr. Jerome Rousselot, Dr. Giovanni Ricco, Dr. Daniele Bianchi and Dr. Spyros Galanis for their input on this paper.

Executive Summary

In this paper, we review the idea of Web 3.0, and how it relates to wider concepts such as money, social media and securitisation.

A key aim of the early design of both the Internet and the Web was to limit central coordination – essentially to reduce the risk of system failures, political conflicts or market power that exploit users and prevent universal participation. Neutrality, openness, and decentralisation were key objectives of software engineers and activists, however the Internet and the Web have so far not offered strong guarantees that they can adhere to these ideals. The associated market power of platform owners and the difficulty in securing data have emerged as the high-hanging fruit still to be picked.

Web 3.0 introduces the idea of money linked to protocols (e.g. Bitcoin) and decentralised applications (dApps) offering online services which are owned and controlled by its users, via the concept of distributed ledgers. By bringing economic incentives into the fabric of our digital infrastructure, Web 3.0 proposes a means to address the challenges of the Web by removing the need to rely on service providers and other third parties.

Distributed ledger technology transfers the responsibility of data security from the intermediary to the end user. Note that this does not necessarily mean better security, rather a shift in who is responsible. In many cases however, there may be an improvement to security as the lack of a central data holder makes for a less rewarding target, also known as a “honeypot”. Although Web 3.0 intermediaries can be built in the model of Web 2.0 intermediaries and therefore exercise user oversight, form honeypots and even sell user data to advertisers, the underlying protocols keep a check on market power and mean the most important functions of asset access and transacting are available without the need for service providers.

Data processing services where privacy matters are a tricky problem for decentralised systems. Sharing raw data online with third parties inevitably leads to unwanted disclosure. Bitcoin and similar blockchains have transparent, public transactions but hide real world identity via public keys as pseudoidentities. Alternative solutions may be required for the processing of information which is itself sensitive or could reveal the real identity of a person. Research in this field is starting to bear fruit in the form of techniques which can process data in its encrypted form, whilst outputting an encrypted result that is only decryptable by the source data provider.

DApps generally aim to offer a marketplace for smaller service providers and consumers, as opposed to providing a centralised service directly. This decentralisation allows users to access services which are transparent, trustless, permissionless and autonomous. There are dApps that have their own purpose-built DLT infrastructure, with Bitcoin being the pioneering example. DApps may also exist as software hosted on top of a general purpose DLT platform. Further possibilities exist as smart contract dApps can interact with one another to enhance their capability.

Although it is broadly correct to say that a dApp’s security can only ever be as good as the security of the ledger on which it is based, this overlooks several important safeguards. If a dApp was running on, for instance, a Proof-of-Work blockchain with very low mining rates which were exploited by a 51% attacker, it would only be exposed to negative effects for a limited amount of time. The malicious miner could act to inhibit new transactions entering the ledger, however to do so forever would cost them a large amount of electricity. It would therefore be likely that it would be only a temporary denial of service.

Most dApp interactions happen at the full capacity of a user’s hardware, which makes them independent of any other remote user or even the quality of the network connection. Changes to the state of a dApp depends on the capacity of the underlying DLT infrastructure which is subject to its network scaling limits. Just like the Internet, scalability in DLT and Web 3.0 is achieved both horizontally (improvements in each layer) and vertically (the addition of higher layer, use-case-specific protocols). Technical progress can narrow the trade-off gap between resilience and efficiency.

Anonymity is difficult to achieve on permanent public records, so instead dApp users settle with “pseudonymity”. If we accept that data ownership can only be meaningful in the context of the control afforded by absolute secrets, then DLT is a means of determining absolute cryptoasset ownership via the ownership of data - in other words, via secret keys. Replacing an intermediary service provider with DLT may reduce the need for terms and conditions as well as market power arising from centralised data ownership.

DApps can solve the market inefficiencies of traditional apps by introducing an alternative revenue model, that issues a token on the network. Participants (users, developers and investors) earn these tokens by contributing in various ways to the dApp and its ecosystem. Tokens generate economic value to holders through mechanisms such as network voting rights or as a means of payment between network participants. If the dApp succeeds, then the value of the token increases and participants get rewarded, depending on their individual contribution. Because there are no free riders, participation increases and more valuable dApps can succeed, thus improving the efficiency of the market.

There are two important aspects to the continuity of a platform. First, it is important that the technical distribution of a system ensures high uptimes of the service. Second, a system should be resistant to change but only if the majority are willing to uphold the status-quo – which they are economically incentivised to do.

Cryptoassets aim to solve economic problems (e.g. how to align the incentives of service providers and users) and achieve an efficient outcome by assigning a price to everything. Distributed ledgers are now able to assign market prices to areas where it was not previously possible to do so, through the innovation of cryptography and the digital scarcity it enables. This idea is based on free market thinking.

Cryptoassets can be divided into distinct groups, each with their own defining characteristics. There are two broad top-down approaches which are used to do this: the regulatory and technical approaches. In the regulatory approach, we can distinguish between three broad categories of cryptoassets: cryptocurrencies, security tokens and utility tokens. All require a distributed ledger to exist. At the time of writing, stablecoins do not fit clearly in any one of these categories. From a more technical point of view, we can distinguish between two types of cryptoassets: cryptocurrencies and tokens.

Cryptocurrencies are designed to be used as a general means of payment for goods or services. In addition to this, they are designed to act as incentive and coordination mechanisms that prevent attacks aiming to corrupt data stored in their ledgers. Without a well-designed cryptocurrency, a distributed ledger is of little use as it cannot be trusted, particularly as there is no central governing body maintaining the integrity of the platform. The exact game theory of how this is achieved depends on the sybil resistance mechanism used by the distributed ledger (e.g. Proof-of-Work and Proof-of-Stake protocols).

Utility tokens are used to digitally access (or reward for providing) an application or service within a distributed ledger. For a dApp to succeed, it requires users, developers and investors to contribute their time and resources. By issuing utility tokens, each participant is rewarded according to their contribution and can pay for services within the ecosystem using these tokens. Categories of utility tokens include (but are not limited to) payment tokens, work tokens, reward tokens, non-fungible tokens, and voting tokens.

Payment (or access) tokens are the most common type of utility tokens. They are issued by a dApp or company and are used to access a defined service, similar to traditional paper tickets. The key differences are that they are often limited in number and trade on a wider secondary market.

Work tokens are used to provide a service (supply-side), unlike payment tokens which are used to acquire a service (demand-side). An individual who wishes to contribute towards a service must acquire the relevant tokens and submit them to the smart contract or protocol in the form of security bonds, which can be forfeited if the work is substandard. In return, the worker is awarded with some positive cash flow – hopefully greater than the cost at which the work tokens were initially acquired at.

Customer loyalty points, air miles, gift cards and coffee stamps are tokens that stand to benefit from digitisation in the form of utility (reward) tokens. Users can trade their collections on secondary markets at a premium or discount, and issuers can have more granular interactions with their customers.

Non-fungible tokens (NFTs) fall into four key categorisations: 1) Personal digital identity; 2) Personal digital reputation; 3) Collectables; 4) Digital membership. In-game items have been an early and popular test bed for this technology. Players can create and earn assets which they fully own and trade.

There are also voting tokens. Decentralised entities require a governance structure due to the issue of incomplete contracts. To avoid centralisation, this governance is via stakeholder voting. This is achieved via the issuance of voting tokens which are freely traded on secondary markets. Voting tokens allow holders to not only express their view, but also the intensity of their view by buying more tokens.

Security tokens are connected to assets that exist outside the blockchain and comply with existing legal frameworks. The advantage of security tokens is that they can automate and streamline certain aspects of the process by removing third parties, thus reducing costs and time delays, especially in settlement and payments. Forms of security tokens include equity tokens, debt tokens, and asset backed tokens.

Equity tokens allows investors to hold traditional equity, but in the form of DLT tokens. Investors have the right to vote at annual general meetings, receive dividends, and are subject to the usual palette of corporate actions such as accounting splits and mergers. Equity tokens can offer more features than traditional equity instruments, given that they rely on software. Their pay-outs are automated, meaning there are no accounting errors. Voting may also be carried out securely via the distributed ledger.

Debt tokens exist in the same technological and regulatory niche as equity tokens, with the difference being that they follow the rules of debt rather than equity instruments. The par value, maturity date, coupon sizes and payment dates are all pre-scripted and fixed in the smart contract behind the token. Whoever holds the debt token at the time of any coupon payment date will receive the interest to their ledger address automatically.

For centuries, businesspeople have been bundling assets up into pools and issuing IOUs, certificates of deposit, shares and other liens to investors. Asset backed tokens can be considered the next technological step in this area.

Stablecoins are designed to reduce price volatility relative to a reference asset, either by directly linking to it, or by providing a hedging mechanism. A stablecoin can be pegged to: a currency or basket of currencies; exchange traded commodities; or other cryptocurrencies. Stablecoins have the potential to take a notable role in the global payment system over the medium term, especially in international remittances and e-commerce.

The emergence of the crypto ecosystem has given rise to new tools which projects and companies can use to raise capital from investors. These include initial coin offerings (ICOs), security token offerings (STOs) and initial exchange offerings (IEOs). These new mechanisms give rise to an interesting new dynamic of liquid venture capital investing, where investors can potentially benefit from exchange traded secondary markets for early stage investments in token form.

Initial coin offerings (ICOs) draw on ideas from the initial public offerings (IPOs) model of the corporate equity market. Unlike IPOs, they are directly accessible to individuals without the need for financial intermediaries. DLT, typically Ethereum, is used as a decentralised and permissionless intermediary between fundraisers and investors. An advantage of the ICO model is that it can deliver a user base for a project from the day it launches.

Security token offerings (STOs) may be considered a sub-class of ICOs, which have been given approval or exemption by the local regulator within the traditional regulatory framework. STOs, partly by convention and partly by necessity, contain explicit rights and obligations. Most current security token projects operate within the exemption rules of securities regulators which tend to restrict their availability only to accredited and professional investors. Due to their inherent programmability, security tokens lend themselves well to legal compliance by auto-enforcing the rules under which they operate.

Token venture capital funds invest in tokens issued by start-ups. By building a portfolio of tokens rather than private shares, they are relatively insulated from the J-curve effect as the tokens tend to reflect some book value or premium for the project they represent through the development lifecycle. Increased liquidity also allows funds to adjust holdings depending on progress of the project or diversify risk by buying into competitors.

The two key technological tools underpinning the modern economy - the Internet and the digital payments infrastructure - currently utilise different technology stacks and achieve different outcomes in terms of user experience and cost. The Web's designers envisaged a payment technology layer which would interact with the Web, enabling users to quickly and cheaply pay for goods and services. However, the digital payment infrastructure continued to be developed by the financial system largely independent of the Internet and remains highly fragmented relative to the Internet.

For fully digital services such as social media, where information itself is the value, distributed ledgers are a natural building block for combining payments with the service provision. When purchasing a virtual product, users exchange one piece of data for another, where one piece is the product and the other is electronic money. It thus makes little sense to keep the information and payment layers of the digital world separate.

Regulatory requirements in the distributed ledger services field so far have focused on streamlining Know Your Customer (KYC) and Anti-Money Laundering (AML) rules. On public DLT networks, we are observing the potential for a partition of assets into a set of KYC compliant coins and a set of coins which do not have a complete KYC record. There are bridges between these two partitions though. Protocol developers are researching techniques to prevent partitions from occurring for any such reason as they might be deemed to harm the value of a cryptocurrency.

Distributed ledger technology offers interesting features for marketplaces: trust minimisation, open data, reduced fraud and embedded logic in cryptoassets. Decentralised marketplaces can operate without the need of a legal entity, as profits can be generated and distributed without the requirement of a bank account or any other specific third party. They have no single server or data centre and therefore can operate reliably around the clock and be accessible globally. They can also make use of smart contract-based escrows to keep parties safe while physical goods are shipped, and thus maintain trust.

Decentralised markets enabled via distributed ledgers can offer benefits across three key areas:

1. Reduced administrative costs when making payments
2. Trust minimisation and fraud reduction
3. Data sharing and ownership

Examples of proof-of-concepts for decentralised marketplaces include open finance, prediction markets, online gambling and labour marketplaces.

Contents

1 Why Have a Decentralised Web?

Sir Tim Berners-Lee invented the World Wide Web (WWW), commonly known as the Web, in 1989 while working at CERN in Switzerland. The Web comprises of a set of standards and protocols, including HTTP and HTML, which are designed to run over the infrastructure of the Internet. The Internet itself is also structured through a set of standards and protocols, which enable separate networks to come together to form an international network of networks. CERN went on to open license the WWW to successfully accelerate its adoption and status as a global system. The first website was hosted on Berners-Lee's own PC, accessible to anyone with an internet connection and a copy of the WWW software.

A key aim of the early design of both the Internet and the Web was to limit central coordination – essentially to reduce the risk of system failures, political conflicts or market power that exploit users and prevent universal participation. Neutrality, openness, and decentralisation were key objectives of software engineers and activists, however the Internet and the Web have so far not offered strong guarantees that they can adhere to these ideals.

Nation states, dominant web platforms, commercial software providers and data centre providers are just some of the actors who have gained notable control and influence as a result of the Web. These actors are known to routinely practice surveillance, censorship and manipulation for their own best interests. An example of the centralisation of the Internet is the domain name system, which has always been largely under the control of the International Corporation for Assigned Names and Numbers (ICANN). Additionally, when an Amazon AWS datacentre in northern Virginia experienced a five-hour long fault in February 2017, it took offline a vast swathe of popular hosted services associated with it.[1] Lastly, the mass surveillance opportunities associated with the current degree of centralisation of data and communications were highlighted by Edward Snowden's leak of the PRISM project.[2]

Regulators have struggled to contain the competition issues which have arisen via new network and data-driven business models used by tech giants. Incumbents now not only secure their dominance through economies of scale as in traditional markets, but also though network effects, data and protocol ownership. Regulators have attempted to approach this through traditional competition economics frameworks on multiple occasions, as was the case when the EU Competition Commission enforced actions against Google and Microsoft.[3,4] However, traditional competition economics frameworks have not been designed for digital data markets, which face distinctly different structures and sources of market power than traditional markets. Data laws have therefore been introduced to increase the control of users over their data and protect against data abuses, such as the EU General Data Protection Regulation (GDPR)[5].

There have been many radical suggestions which often lack enough economic substance to benefit consumers.[6] On the market design side, there is now a growing movement to re-design cyberspace, and replace tech network giants with decentralised networks. This movement is commonly referred to as "Web 3.0".

[1] For more information on the Amazon AWS outage, see: https://www.theregister.co.uk/2017/03/01/aws_s3_outage.

[2] For more information on the PRISM project, see: https://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29.

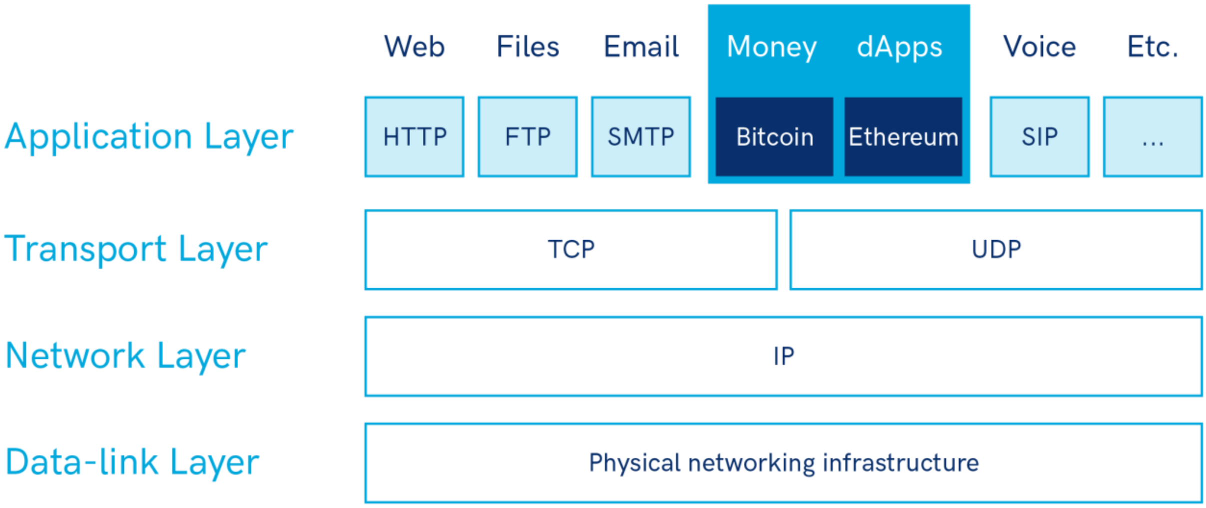
[3] For more information on the EC enforcement against Google, see: http://europa.eu/rapid/press-release_IP-18-4581_en.htm.

[4] For more information on the EC enforcement against Microsoft, see: https://web.archive.org/web/20071019031601/http://www.ecis.eu/issues/CFI_Microsoft.htm.

[5] For more information on GDPR, see: https://eugdpr.org/

[6] For more information on proposals that force tech giants to share their data, see: https://uk.news.yahoo.com/force-tech-giants-share-data-rather-break-them-124032106--finance.html.

Figure 1: Where distributed ledger technology fits into the internet technology stack, thus facilitating a new "Web 3.0" paradigm



Source: Aaro Capital Research

Web 3.0 introduces the idea of money linked to protocols (e.g. Bitcoin) and decentralised applications (dApps) offering online services which can be owned and controlled by its users, via the concept of distributed ledgers. Key properties where users gain value include: public and private communications, resilience, and data security.

There is however a hurdle on the Web 3.0 roadmap, and that is data. Distributed ledgers are not designed to handle data in the same way that servers are. The coordination of decentralised global consensus combined with the replication of work and data make distributed ledgers unappealing as a medium of storing anything much larger than the refined footprint of a monetary account ledger. In other words, the Achilles' heel of a distributed ledger… is the ledger. The Web 3.0 solution so far has been to outsource the storage of bulk data to other systems which then make reference to the ledger, and vice versa. A project called the Interplanetary File System (IPFS) has emerged as a leader in this field, by enabling data to be stored across the empty space of strangers' hard drives and then referenced by DLT-based smart contracts[7]. The off-chain data does not have the reliability guarantee or auditability of the on-chain data, but can be far larger and attested to by the ledger.

In summary, the Web has evolved considerably over the last few decades, and has indeed overcome many technical challenges to become mainstream. The associated market power of platform owners and the difficulty in securing data have emerged as the high-hanging fruit still to be picked. By bringing economic incentives into the fabric of our digital infrastructure, Web 3.0 proposes a means to address these challenges by removing the need to rely on service providers and other third parties, including financial intermediaries.[8] Decentralised platforms result in less concentration of control, and therefore less market power which may be exploited.[9,10]

[7] For more information on IPFS, see: https://ipfs.io/

[8] In competition theory, simply the threat of a credible outside option is enough to dissipate all market power, but this may not happen in reality for various reasons.

[9] Market power arises when there is control over the protocol and data layers of a network, while the positive network effects on the network layer cause platforms to naturally consolidate and enable further exploitation.

[10] Market power of decentralised platforms is explored further in section 2.3..

2 Centralised vs Decentralised Applications

As with decentralised ledgers, it is helpful to contextualise decentralised applications within the two spectrums of political control and execution architecture. Table 1 plots some popular traditional applications in this two-dimensional space. Web 3.0 dApps are a special case of the distributed and decentralised class, and benefit from properties of DLT such as the ability to maintain a trustless currency, payment autonomy and reliable historical records.

Table 1: The two dimensions of application control and architecture

		Political Control	
		Centralised	**Decentralised**
Execution Architecture	**Concentrated**	Proprietary PC apps e.g. Microsoft Word, Adobe Photoshop	Open-source[11] PC apps e.g. LibreOffice, Gimp
	Distributed	Proprietary networked apps e.g. Google Docs, Oracle Database (i.e. the 'cloud')	Open-source[11] networked apps e.g. BitTorrent, RethinkDB

Source: Aaro Capital Research

There are dApps that have their own purpose-built DLT infrastructure, with Bitcoin being the pioneering example. Particl is another example; it is architecturally similar to Bitcoin, but has a built-in native marketplace for physical and virtual goods and services.[12] DApps may also exist as software hosted on top of a general purpose DLT platform. For example, Augur is a prediction marketplace coded as smart contract software hosted and executed by the Ethereum blockchain.[13]

Further possibilities exist as smart contract dApps can interact with one another to enhance their capability. Most dApp development and experimentation has been happening at the smart contract level. These higher level dApps offer a more familiar programming paradigm for developers, and the complexities of organising consensus can be delegated to the DLT layer. The disadvantage is that dApps and their users are dependent on the underlying DLT platform with little control over its functionality. They must also pay fees in the native cryptocurrency each time they make a record on the ledger.

DApps generally aim to offer a marketplace for smaller service providers and consumers, as opposed to providing a centralised service directly. This decentralisation allows dApp users to access services which are transparent, trustless, permissionless and autonomous.

[11] For more information on open source software, see: https://en.wikipedia.org/wiki/Free_and_open-source_software.
[12] For more information on Particl, see: https://particl.io/
[13] For more information on Augur, see: https://www.augur.net/

Case Study: 0x

The 0x protocol ("zero ex") is a smart contract based dApp hosted on the Ethereum blockchain. It offers a decentralised exchange platform for other tokens hosted on the Ethereum blockchain. To achieve this, external orderbook managers, known as relayers, are required to aggregate and match orders before they are handed over to the Ethereum network for settlement. These relayers are paid for their service in the native token currency of the dApp by traders submitting orders. Holders of the 0x token can vote on changes and upgrades to the dApp on which their business ecosystem depends. The token has value for users of the dApp by incentivising order execution. It also has value for relayers who can have some say over the development of their infrastructure and sell token earnings for cash revenue.

Case Study: Particl

Particl is an open source, permissionless blockchain project which offers an eBay style marketplace for goods. It is both a decentralised and distributed system, since the application is a set of rules enforced by a blockchain network. A native token currency unit, PART, is minted and used to pay nodes enforcing the rules of the system.

Existing marketplace services have policies on what sort of goods may be offered and what behaviour will not be tolerated from users. Particl is different in that it has no management team to create and enforce policy, only a group of anonymous and transient individuals who happen to be running copies of the software. For the system to be a welcoming environment to as many users as possible, the designers have included tools to help the community collectively govern the application themselves. For example, trading of illicit goods can be prohibited through algorithmically controlled voting. This governance process is open to all PART token holders who each may propose and vote on collective actions.

2.1 Cyber Security

2.1.1 Data Security

Table 2: A comparison of data security risks

	Data Security Risks
Proprietary Networked Apps (the 'cloud'	Administrator risk: Service provider can survey, leak or wipe user data and cut access Honeypot risk: Large online database of private information Phishing risk: Counterfeit web portals can surreptitiously steal account credentials
DApps	Software bug risk: Open source, but exploited bugs can lead to irrevocable asset loss Edge security risk: Users may not have the knowledge to be able to appropriately manage their own data

Source: Aaro Capital Research

Distributed ledger technology transfers the responsibility of data security from the intermediary to the end user. This is sometimes referred to as "edge security", as sensitive data is moved from central controllers to the users themselves at the edges of the protocols. Note that edge security does not necessarily mean better security, rather a shift in who is responsible for the security. In many cases however, there may be an improvement to security as the lack of a central data holder makes for a less rewarding target, also known as a “honeypot”. Honeypots are pools of valuable data or assets that are far more tempting (and require less effort) to target relative to data or assets that are spread across numerous locations and systems.

Digital honeypots, such as customer databases of corporations, are getting larger as centralised online services have ballooned in popularity. Data breaches resulting in the publication of users’ private information, leading to mass credit card fraud, and even targeted extortion, have become a familiar occurrence.[14] In 2017, a software flaw at Equifax led to the theft of the personal information of around 200,000 people.[15] It is worth noting that most of those affected had no direct relationship with Equifax – the services they used elsewhere had data sharing agreements with Equifax. Similarly, the Cambridge Analytica exposure of Facebook user data was notable as it included histories of personal messages, locations and friendship links.[16]

In peer-to-peer systems, honeypots are typically small. An attacker has to work harder to locate and retrieve the same amount of information as the identities and whereabouts of participants are mostly unpublished.

End users are generally not as practised in data security as specialist firms, so there is an implied onus on protocol developers to create, or at least cater to, more user-friendly security tools. Private key management is a security problem which does not have a perfect solution and probably never will, much like passwords. The creation of the Hierarchical Deterministic Wallet and Seed Phrase standards are examples of peripheral developments to the Bitcoin protocol, designed to assist users with the complex task of secure key management.[17,18] These standards have been widely adopted by crypto users and have triggered a proliferation of new and easy-to-use wallet software and hardware. Third party service providers, such as private key custodians, have also emerged to satisfy users who cannot or are not yet ready to manage data security themselves. Although Web 3.0 intermediaries can be built in the model of Web 2.0 intermediaries and therefore exercise user oversight, form honeypots and even sell user data to advertisers, the underlying protocols keep a check on market power and mean the most important functions of asset access and transacting are available without the need for service providers.[19]

DApps aim to mitigate administrator and honeypot risks. However, due to their autonomous and deterministic nature, software bugs can still pose some risk. With this in mind, nuclear power, aviation, life support and other safety critical activities which depend on digital control have developed techniques and languages which are highly resistant to coding errors - these are being adopted by the smart contract community. Formal specification and verification techniques are used to mathematically compare executable software against rigorously defined specifications to highlight any logical deviations. Additionally, all dApp code is open source such that any user can theoretically perform an independent audit before engaging.

Phishing attacks are a means of extracting authentication information such as passwords or keys from users by subtly directing them to counterfeit versions of the service they are expecting to use. Web browsers accustom

[14] For more information on notable data breaches, see: https://en.wikipedia.org/wiki/List_of_data_breaches.
[15] For more information on the Equifax data leak, see: https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population.
[16] For more information the Cambridge Analytica scandal, see: https://qz.com/1245049/the-cambridge-analytica-scandal-affected-87-million-people-facebook-says.
[17] For more information on the Hierarchical Deterministic Wallet, see: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki.
[18] For more information on Seed Phrase standards, see: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
[19] Users should consider the jurisdiction of their chosen third parties. For example, the US’s PATRIOT and CLOUD Acts are not considered compatible with EU GDPR: https://www.devoteam.com/newsroom/cloud-act-new-measures-companies-european-personal-data/.

users to download code and user interfaces from remote servers daily and then input passwords onto them. Web 3.0 users do not need to access third party servers, and instead access their own local copy of the DLT to interact with various services. In other words, they do not need to use web browsers to download fresh code. This change in habitual behaviour makes phishing a much less effective exploit.

Data processing services where privacy matters, such as automated medical diagnoses, financial portfolio analysis and facial recognition, are a tricky problem for decentralised systems. Sharing raw data online with third parties inevitably leads to unwanted disclosure. Bitcoin and similar blockchains have transparent, public transactions but hide real world identity via public keys as pseudoidentities. Alternative solutions may be required for the processing of information which is itself sensitive or could reveal the real identity of a person. Research in this field is starting to bear fruit in the form of techniques which can process data in its encrypted form, whilst outputting an encrypted result that is only decryptable by the source data provider.

Case Study: Secure Multi-party Computation

Secure Multi-Party Computation (MPC) is a complex cryptographic scheme which, in certain cases, can solve the problem of absolute privacy in the context of the public domain and third-party services. The users of the service work together to run some function over a set of inputs, in order to agree on the correct result without revealing anyone's inputs.

The role of a stock exchange's order matching engine is to analyse all incoming orders from traders and match up bids and offers in order to execute trades. An MPC version could take in encrypted orders, and yet still manage to output correctly matched buys and sells. None of the participants learn what orders are being placed by others – a form of blind auction but without an auctioneer. MPC has a role in securing Web 3.0 by keeping shared key material private and user data hidden from the public.

Case Study: ZEXE Protocol

The ZEXE protocol is a blockchain proposal based on a zero-knowledge proof system, which achieves both data and functional privacy. Functional privacy means that some software function, such as the addition of two numbers, can be carried out correctly without revealing either the inputs or the result to the person or persons executing the function.

Let's say Alice has two numbers, 34 and 26, and wants to use the ZEXE blockchain to add them together and record the output on the chain. Critically, she does not want anyone else to know any of these numbers. She first encrypts the inputs using her private key: 34 becomes "0x7a37d8c3" and 26 becomes "0x2f9e8e4b". She broadcasts the values to the network and waits for a miner to compute and publish the result in a new block. Bob, a miner, sees the request and runs the inputs through the addition function: zexe_addition(0x7a37d8c3, 0x2f9e8e4b), and gets the result "0x3d6a4f9a". Only Alice can decrypt that result and when she does, using the same private key she encrypted the inputs with, she finds that it is 60.

Functions executed by the protocol operate exclusively on encrypted data. Therefore, they learn nothing about the real content of the input data or result data.

2.1.2 Platform Security

Table 3: A comparison of platform security risks

	Platform Security Risks
Proprietary Networked Apps (the 'cloud'	Software bug risk: Not open source or verifiable, down to service provider Infrastructure risk: Data centre faults can cause disruption to service and data loss
DApps	Infrastructure risk: Poorly supported DLT can be vulnerable to denial-of-service attacks Incentive misalignment risk: Oracles are semi-trusted and may have unknown incentives

Source: Aaro Capital Research

DApps, depending on their design, generally inherit the platform properties of the DLT on which they are hosted: immutability of transaction history; consensus-based validation of transactions; historical auditability; open source code; and lack of trusted intermediaries.[20] Like traditional cloud applications, dApps exist online and operate continuously around the clock. Although it is broadly correct to say that a dApp's security can only ever be as good as the security of the ledger on which it is based, this overlooks several important safeguards. Traditional centralised cloud applications are only as secure as the systems and people in charge of them, and can in theory be fully undermined (i.e. total data loss, barred access, full private data leak, malicious data modification which can be extremely difficult or even impossible to trace). If a dApp was running on, for instance, a Proof-of-Work blockchain with very low mining rates which were exploited by a 51% attacker, it would only be exposed to negative effects for a limited amount of time. The malicious miner could act to inhibit new transactions entering the ledger (interactions with the dApp), however to do so forever would cost them a large amount of electricity. It would therefore be likely that it would be only a temporary denial of service. Attackers would not be able to affect other user accounts in the dApp or steal their cryptoassets without access to private keys – something which is generally uneconomical to attempt due to the absence of central honeypot-style databases.

Oracles are services that help to verify the legitimacy of inputted data. They supply external information to a dApp so that smart contracts can query and verify inputted data where necessary. If a participant's contribution is deemed unreliable or malicious by a sufficient number of other participants, it may be rejected. This approach to validation can be gamed but can usually be set up to organise risk/reward sufficiently in favour of cooperative behaviour. In comparison, traditional cloud applications almost always rely on third party data suppliers who do not have explicit capital at risk of challenge by members of the public.

[20] For a detailed overview of DLT platform security, see the paper "*An Introduction to Distributed Ledger Technology*"

2.1.3 Resilience vs Efficiency

Table 4: A comparison of resilience and efficiency

	Resilience	Efficiency
Proprietary Networked Apps (the 'cloud'	High trust requirements and single points of control mean that, despite progress in systems distribution and redundancy, there are still occasional catastrophic failures	Data communication, storage capacity and bandwidth continue to expand by orders of magnitude. Cloud applications directly benefit from this
DApps	Low trust requirements and auditable code lead to high reliability and availability of service	DApps run locally and can therefore scale with the user's hardware. DApp communications depend on DLT infrastructure scalability limits

Source: Aaro Capital Research

DLT networks are made up of nodes, and Web 3.0 dApps are executed by those nodes. Web 3.0 users can run all of their online cloud dApps locally from their own node on their own hardware, which can be thought of as the functional equivalent of Web 2.0 browser software except that it communicates with a trustless peer-to-peer network of other nodes rather than trusted servers. In Web 3.0, all remote communications are handled by the node backend according to distributed protocols. Most dApp interactions therefore happen at the full capacity of a user's own hardware, which makes them independent of any other remote user or even the quality of the network connection. Changes to the state of a dApp, for example when making a payment, depends on the capacity of the underlying DLT infrastructure which is subject to its network scaling limits.[21] Just like the Internet, scalability in DLT and Web 3.0 is achieved both horizontally (improvements in each layer) and vertically (the addition of higher layer, use-case-specific protocols).[22] Technical progress can narrow the trade-off gap between resilience and efficiency.

2.2 Privacy

Table 5: A comparison of privacy characteristics

	Privacy
Proprietary Networked Apps (the 'cloud'	Intermediaries and service providers mediate all interactions Regulation is needed to enforce privacy rights and responsibilities
DApps	Accessed using personal secrets (keys) which are confined to users' own devices Non-personal secrets (relationships) are kept between relevant parties without oversight by intermediaries, but are considered public domain

[21] For an explanation of the scalability trilemma faced by distributed ledgers and dApps, see: https://multicoin.capital/2018/02/23/models-scaling-trustless-computation/.
[22] For an explanation of scalability via additional layers of software, see: https://hackernoon.com/2019-blockchain-layer-2-solution-review-d00385147396.

Source: Aaro Capital Research

Over 150 national constitutions mention the right to privacy and the EU has taken steps to give individuals the right to be forgotten through GDPR.[23] Human nature has us existing with a balance between the power and freedoms of the individual versus that of the rest of society. As protection of individual privacy falls, the easier it generally is for agents such as a companies or governments to increase their influence.[24] In theory, laws and legal systems can be put in place to protect individual liberties and prevent the concentration of power, but in reality almost all contracts are imperfect and incomplete.[25] Further, human capabilities are rapidly evolving with technology, leaving regulators constantly on the back foot.[26]

Privacy is a relative measure of secrecy within a given scope or context. There is the absolute privacy of personal secrets like memories and thoughts. Democratic voting requires private ballots to mitigate corruption via coercion and there are indeed many DLT projects aiming to mediate trustless internet democracy. Non-personal privacy exists where there are social interactions which are not in the public domain, such as a business contract. From a security point of view, these classifications of privacy are different given that personal secrets are fully under the owner's control, whereas non-personal secrets can be made public at any time by the other party or parties - essentially a trust issue.

Privacy is therefore closely related to the control of information and, by extension, the concept of data ownership. Where traditional web services have become accustomed to acquiring the control of user data, regulators have stepped in to assert citizen rights, and the results are lengthy sets of terms and conditions, increased concentration and higher costs which are passed onto end users.

Permissionless distributed ledger networks exist in the public domain and therefore need to balance transparency with privacy. Anonymity is generally the goal – the public being aware of the information but not whom it relates to. Anonymity though is difficult to achieve on permanent public records, so instead dApp users settle with "pseudonymity".

Pseudonymity requires that the records are in the public domain, but are associated only with pseudonyms rather than real identities. Pseudonyms take the form of public keys or addresses and thus every user may theoretically masquerade under multiple, separate pseudonyms. If Alice sends Bob a payment to his address "123abc", then Alice will know that Bob owns that address and will be able to extrapolate his historical and future transactions using that address. Bob can choose to avoid the reuse of his address and create a new one for each payment received. This approach can help maintain pseudonymity fairly well, although is not perfect.

While DLT relies on cryptographic mechanisms, most implementations do not use cryptography to hide the data. There is a significant amount of research being carried out on more extensive encryption and obfuscation of ledger data, without undermining the ability of other network participants to validate transactions and payloads.

[23] For more information on GDPR, see: https://gdpr-info.eu/art-17-gdpr.

[24] The boundary between individual privacy and state overreach are discussed in relation to the US Patriot Act here: https://www.theguardian.com/world/2014/jan/23/nsa-bulk-collection-chorus-surveillance-under-patriot-act.

[25] Laws and legal systems are nonetheless important to prevent political or corporate overreach.

[26] A clear example of this is the tactics used by Cambridge Analytica, which showed how easily a democratic election can be swayed using news, social media platforms and the data they provide. The resulting *Disinformation and 'fake news'* report by a UK Commons Selection Committee mentioned that UK electoral laws are 'not fit for purpose': https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-report-published-17-19/.

Techniques include Confidential Transactions, Ring Signatures, Graftroot, and zk-SNARKs.[27,28,29,30] DApps can inherit these privacy preserving features from their DLT hosts.

If we accept that data ownership can only be meaningful in the context of the control afforded by absolute secrets, then DLT is a means of determining absolute cryptoasset ownership via the ownership of data - in other words, via secret keys. All other data in this context is published to the ledger or the peer-to-peer network, and so the ownership of that data must be considered public domain. This does not preclude the enforcement of judicial rules on who has rights to use the data, however the underlying technology does not help in this respect. Replacing an intermediary service provider with DLT may reduce the need for terms and conditions as well as market power arising from centralised data ownership. Any licensing of owned data remains a non-technological issue.

Case Study: Medicalchain

Medical data is very private, however must be shared with a wide range of medical practitioners and researchers over a person's lifetime. A blockchain can help by enabling the patient to be the primary custodian of their medical records and share them with a consultant of their choice. The consultant can then verify the authenticity and integrity of the patient records against the data recorded on the blockchain. Medicalchain also makes longitudinal record keeping feasible by associating all health notes to the user's account.

2.3 Market Efficiency

The centralised nature of today's Internet relies on the existence of third parties, or trusted intermediaries. The unintended consequence is that these intermediaries obtain market power that they can abuse, thus reducing the efficiency of the market. Market power can arise in many different ways. For instance, once trust is established within a network, it may be difficult or costly to leave and join a new one. This "lock-in" generates market power for the owner of the network or application, who may abuse it. Moreover, information about all transactions/interactions is captured by the owner, who may then sell it or use it to maximize profits. In many cases, a user cannot export and reuse this information if they choose to leave a specific application or network.

If incentives between users and the owner were aligned, market power would not be an issue. However, this is not usually the case, thus creating the following principal-agent problem. Although the users (principals) provide the information that is crucial in order to operate the application/server, the intermediaries (agents) have the incentive to use this information in ways that are against their best interests (e.g. by raising fees).

The decentralised nature of DLTs, together with the Web 3.0 dApps that they enable, has the potential to revolutionise the way information is distributed and stored, by realigning the incentives of all market participants and alleviating the principal-agent problem. The main change is that each user is the true owner of their own information and chooses when, and under what conditions, it is made available to other market participants. More

[27] For more information on Confidential Transactions, see: https://elementsproject.org/features/confidential-transactions.

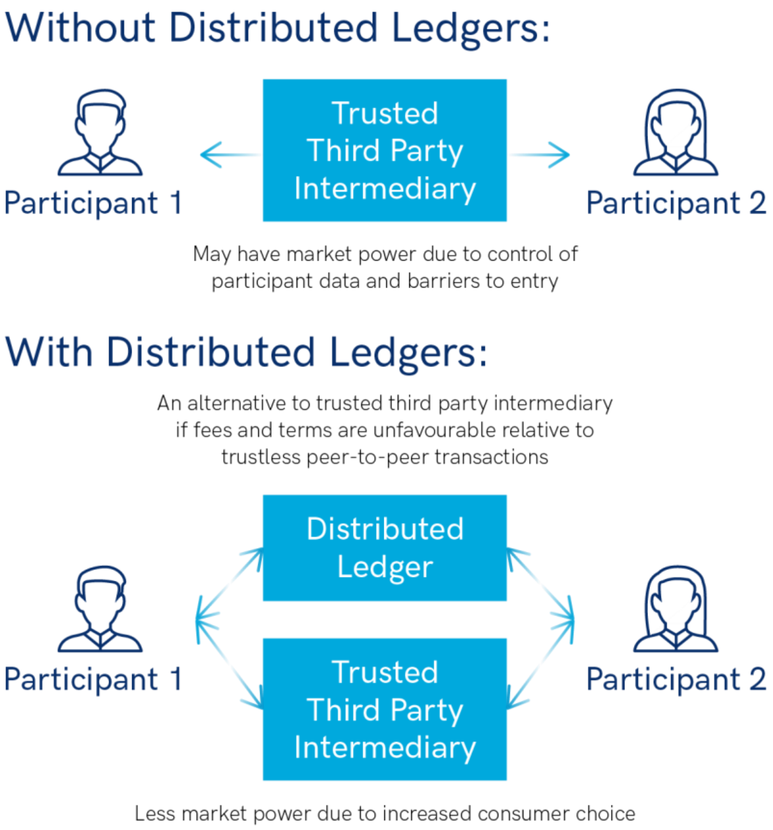
[28] For more information on Ring Signatures, see: https://medium.com/coinmonks/ring-signatures-and-anonymisation-c9640f08a193.

[29] For more information on Graftroot, see: https://bitcoinmagazine.com/articles/graftroot-how-delegating-signatures-allows-near-infinite-spending-variations.

[30] For more information on zk-SNARKs, see: https://z.cash/technology/zksnarks/.

importantly, rules are hard-coded and open-sourced within the dApp or DLT, instead of being decided (and changed arbitrarily) by the CEO of a public company.

Figure 2: Moderating market power via decentralised ledgers

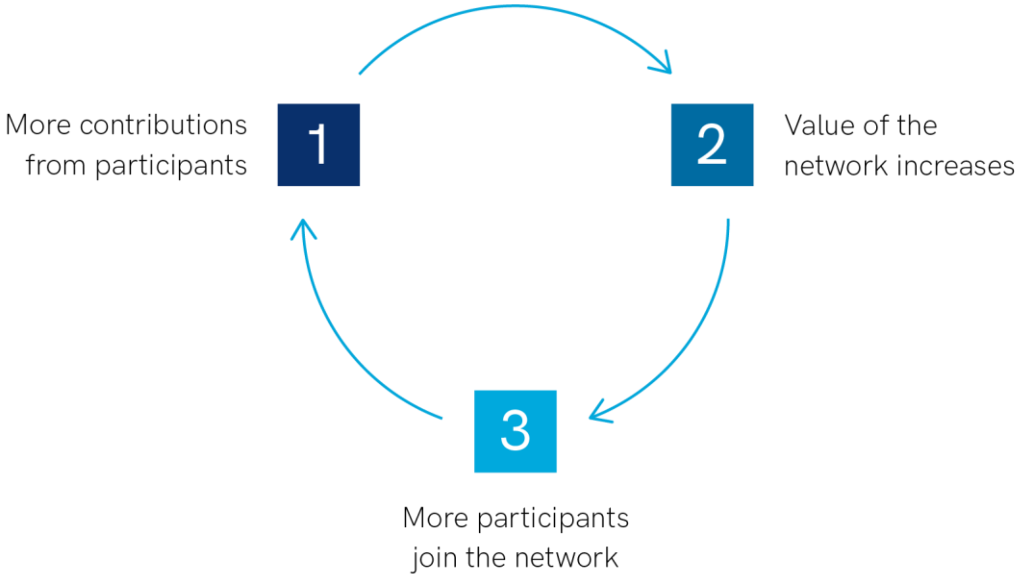

Without Distributed Ledgers:
Participant 1
Trusted Third Party Intermediary
Participant 2
May have market power due to control of participant data and barriers to entry
With Distributed Ledgers:
An alternative to trusted third party intermediary if fees and terms are unfavourable relative to trustless peer-to-peer transactions
Distributed Ledger
Participant 1
Trusted Third Party Intermediary
Participant 2
Less market power due to increased consumer choice

Source: Aaro Capital Research

DLTs and their dApps also offer a different revenue model that has the potential to increase market efficiency.

The traditional revenue model of an app is that the owner initially invests heavily in order to create and develop it. However, the app is of little benefit unless a critical mass of people starts using it and/or enough developers create a valuable ecosystem around it. This implies that the initial users/developers of the app create a positive externality to all subsequent users, but they are not adequately rewarded for their efforts. Moreover, if the app succeeds, then the owner attempts to recuperate the initial cost of investment, usually by retrospectively changing the pricing scheme, or by selling information/adverts at terms not foreseen by the initial users. Such a revenue model means that some apps that are valuable may never be successful, because not enough initial users accept to participate without being rewarded, or because the initial investment cannot be recuperated at a later stage. As a result, the market is not as efficient.

Figure 3: The "chicken and egg" issue faced by new networks


More contributions from participants
1
2
Value of the network increases
3
More participants join the network

Source: Aaro Capital Research

DApps can solve these issues by introducing an alternative revenue model, that issues a token on the network. Participants (users, developers and investors) earn these tokens by contributing in various ways to the dApp and its ecosystem. Tokens generate economic value to holders through mechanisms such as network voting rights or as a means of payment between network participants.[31] If the dApp succeeds, then the value of the token increases and participants get rewarded, depending on their individual contribution. In other words, all externalities are internalised and each participant is rewarded in a fair and consistent way, that is difficult to change retrospectively.[32] Because there are no free riders, participation increases and more valuable dApps can succeed, thus improving the efficiency of the market.

Case Study: Steem

Steem is a blockchain-based blogging platform which competes with the likes of Reddit and Medium. Users publish their content, and a native token is automatically paid to authors depending on the popularity of their work. The blockchain is supported by core participants who are also paid in the native token. Therefore, participants are incentivised to act collectively within a decentralised hosting service. Steemit.com is a centralised web service which collects its data from the underlying blockchain, Steem, and serves it up to web browsers. There are other competing web sites which feed off the same blockchain – users can therefore freely migrate from one portal to another through an inherently open model.

[31] Token economic design is critical to the value of the token. There must be economic benefit for holding the token beyond speculation (where many tokens failed in 2017/18). This is covered in more detail in Section 3.

[32] A detailed discussion on how DLT can solve the "tragedy of the commons" problem faced by networks be found at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598.

2.4 Platform Continuity

There are two important aspects to the continuity of a platform. First, it is important that the technical distribution of a system ensures high uptimes of the service. Second, a system should be resistant to change but only if the majority are willing to uphold the status-quo – which they are economically incentivised to do.

On the technical side, traditional server-based web services tend to have numerous central points of failure, such as server or data centre power supply, internet connection or management company. As a result, web-based services tend to quote minimum uptime guarantees to their paying clients. These typically are above 99%, but never at 100%. Software upgrades may also require the temporary suspension of services. A major advantage of decentralised platforms is that users are not dependent on a fixed group to run the platforms, nor any single server or location. As each participant runs at least a subset of the service's functions in parallel with the others, through wide scale distribution there is an effective 100% uptime.

On the economic side, decentralised platforms are run by a set of core participants, often referred to as miners or validators. Core participants choose to perform the full set of functions of the protocol at some cost, in return for some reward. Non-core participants depend on there being at least one functioning core participant at any time, and ideally many, many more. If there are many non-core participants, but a dangerously low quantity of core participants, then a well-designed decentralised system will bring down the barrier to entry (cost) for becoming a core participant such that it is worthwhile for the non-core participants to change role. The effect of this self-calibrating arrangement is that anyone who wants to use the network can be assured that there will either be a healthy community to support them, or they can easily run the protocol themselves along with their chosen counterparties, albeit at a lower level of 'security'.

It is important to also consider the prospect of platform continuity over the long term in the absence of a central service provider. Protocol upgrades, additional features, multiple implementations, obsolescence of older features and forks can make it difficult to be sure that some future version of the platform is a continuation of historical platform, or a new platform in its own right. In the case of contentious forks, a user who returns to a platform after a few years have passed will have to choose a current node or wallet package which reflects their own view of which fork of the network represents the continuation of the platform they earlier left. Economic security is a phrase often used to explain the power of DLT to unwaveringly do what it is designed to do. In this context 'security' means that the system adheres to its set of rules in perpetuity. This turns out to be a comparable paradigm to social law and governance. Decentralisation is a means to insulate the system and its rules from the control of any human participants. More decentralisation means a more reliable and predictable system, and therefore a more secure system.

3 Cryptoassets

Cryptoassets aim to solve economic problems (e.g. how to align the incentives of service providers and users) and achieve an efficient outcome by assigning a price to everything.[33] Distributed ledgers are now able to assign market prices to areas where it was not previously possible to do so, through the innovation of cryptography and the digital scarcity it enables.[34] This idea is based on free market thinking. However, the invisible hand is not the only mechanism by which economic equilibriums can be achieved. Other mechanisms include centralised matching mechanisms, social planner's problem and lotteries, all of which can achieve preferable outcomes to free markets in given situations. Further, not all economic equilibriums are efficient and, even if they are, they may be unobtainable or socially undesirable due to market failures.

Different economic problems require different types of tokens. Cryptoassets can be divided into distinct groups, each with their own defining characteristics. There are two broad top-down approaches which are used to do this: the regulatory and technical approaches.[35]

In the regulatory approach, we can distinguish between three broad categories of cryptoassets: cryptocurrencies, security tokens and utility tokens. All require a distributed ledger to exist. At the time of writing, stablecoins do not fit clearly in any one of these categories.

From a more technical point of view, we can distinguish between two types of cryptoassets: cryptocurrencies and tokens.

The table below summarises the three widely accepted categories, the terminologies used by the regulators and different agencies in charge, as well as the technical terminology.

Table 6: Cryptoasset Classification Frameworks

	SEC (unofficial)	FCA	FINMA	Technical layer
Cryptocurrencies (BTC, ETH, etc.) Decentralised issuance	Cryptocurrencies Regulator: FinCEN	Cryptocurrencies Regulator: EU 5th directive	Cryptocurrencies Regulator: EU 5th directive	Cryptocurrencies
Security tokens Centralised issuance	Security tokens Regulator: SEC, CFTC	Security tokens Regulator: FCA	Asset tokens Regulator: FINMA	Tokens
Utility tokens Centralised issuance	Utility tokens Unregulated	Utility tokens Unregulated	Utility tokens Unregulated	

Source: Aaro Capital Research

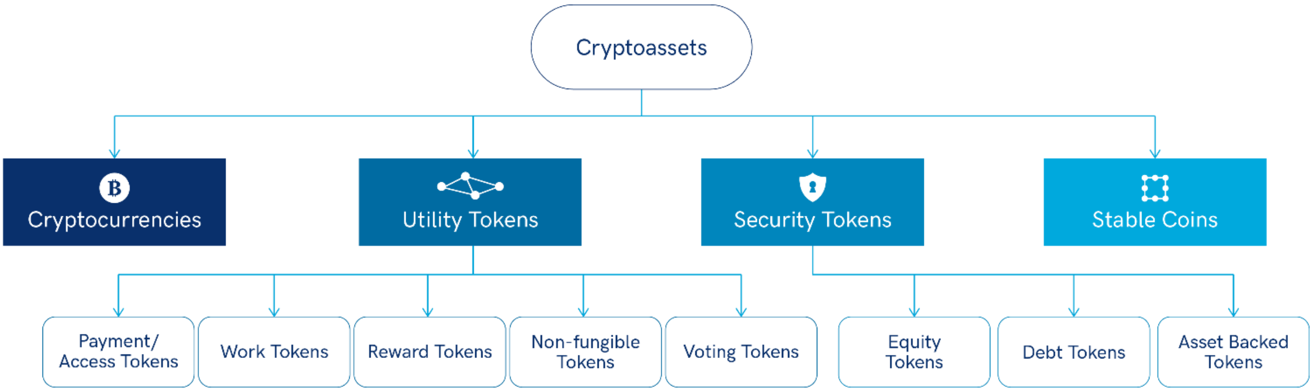
In the subsections below, we outline the underlying economic models behind a number of different token types. Note that this is a non-exhaustive list.

[33] A simple economic optimisation of a token model is provided here: https://hackernoon.com/utility-tokens-discussion-economic-model-and-simulation-in-r-798c0ff3d26c.

[34] The only limiting factor is the security of the distributed ledger, where scarcity depends on the robustness of the ledger's governance.

[35] There are other approaches to classify cryptoassets, some of which are explored in more detail at: https://www.cryptocompare.com/media/34478555/cryptocompare-cryptoasset-taxonomy-report-2018.pdf.

Figure 4: Some economic models for cryptoassets



Source: Aaro Capital Research

3.1 Cryptocurrencies

Cryptocurrencies are designed to be used as a general means of payment for goods or services.[36] They are not issued or backed by any central authority. While they are currently outside the perimeter of securities regulators, they still fall within Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations and international sanctions. In the US, the federal agency enforcing these regulations is FinCEN (Financial Crime Enforcement Network). In the EU, the fifth AML/KYC directive defines the rules to be applied by national agencies. Examples of cryptocurrencies include bitcoin, Ether, litecoin, ZCash, EOS, etc.

In addition to their function as a means of payment, cryptocurrencies are designed to act as incentive and coordination mechanisms that prevent attacks aiming to corrupt data stored in their ledgers. This is important in terms of game theory and aligning the incentives of all users. Without a well-designed cryptocurrency, a distributed ledger is of little use as it cannot be trusted, particularly as there is no central governing body maintaining the integrity of the platform. The exact game theory of how this is achieved depends on the sybil resistance mechanism used by the distributed ledger.

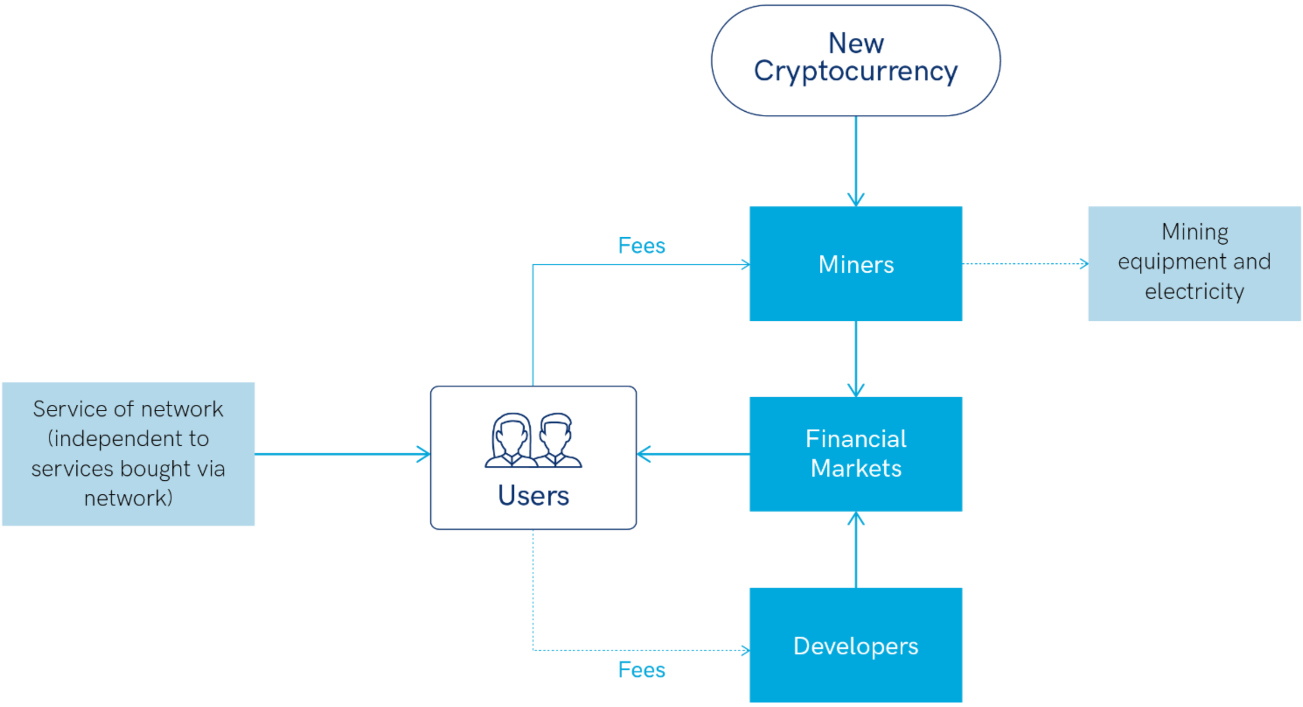
In a Proof-of-Work protocol, the blockchain's transaction validators (i.e. "miners") solve mathematical problems for the chance to propose the next block, and receive compensation for successfully doing so.[37] This means that they face large upfront computer hardware and electricity costs, and receive compensation in the cryptocurrency they are mining.[38] Mining equipment is limited in that it can only be used for mining cryptocurrency (and more often than not, for a specific cryptocurrency only). If the cryptocurrency fails, this investment cannot be recovered. On the other side, network users pay transaction fees in cryptocurrency when using the network, and may also choose to transact in it. This creates user demand for the cryptocurrency. Finally, on some ledgers (e.g. Dash) a proportion of the fees go to developers. In the absence of fees, developers can monetise their work via the appreciation of the cryptocurrency they hold.

[36] Some supporters of Bitcoin argue that it is a first and foremost a store of value which will eventually develop into a means of payment. This argument is derived from the economic thought of the Austrian school and the historical observations of Nick Szabo in "Shelling out: The Origins of Money", For more information, see: https://bisq.network/blog/bitcoin-and-the-store-of-value-narrative/.

[37] A comprehensive overview of the Proof-of-Work protocol and the game theory underpinning it is provided in the paper, "An Introduction to Distributed Ledger Technology".

[38] Block Reward = Transaction Fees + Block Subsidy

Figure 5: Stakeholder Incentives in a Proof-of-Work protocol

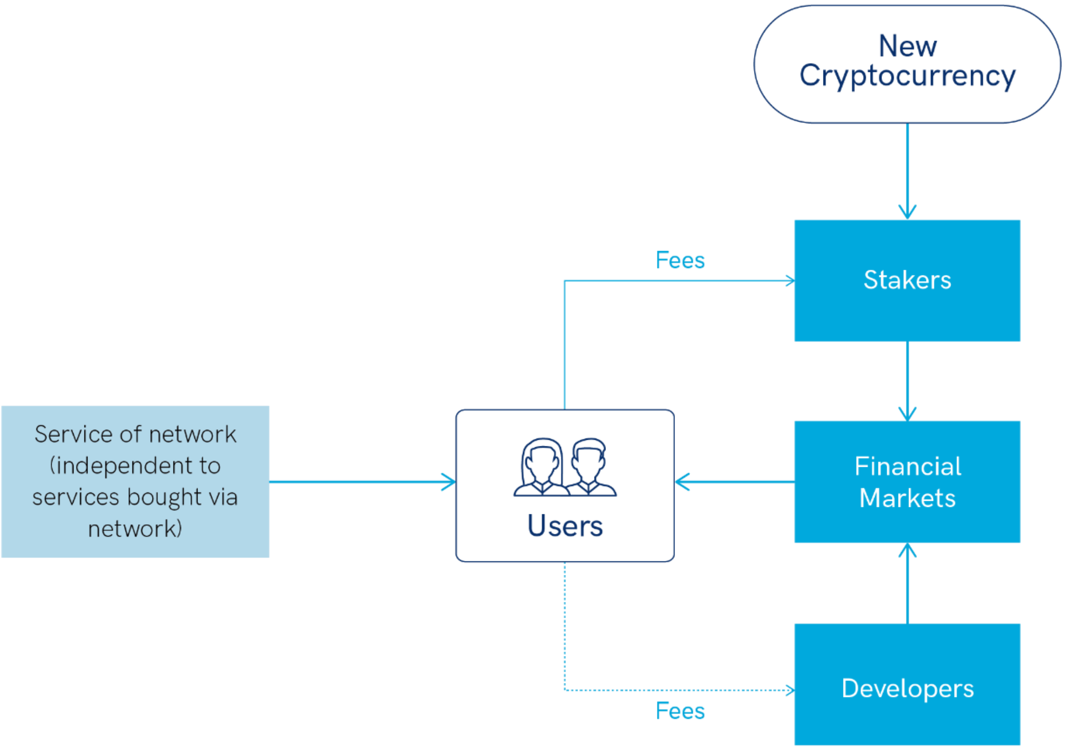

New Cryptocurrency
Fees
Miners
Mining equipment and electricity
Service of network (independent to services bought via network)
Users
Financial Markets
Developers
Fees

Source: Aaro Capital Research

In a Proof-of-Stake protocol, the blockchain’s transaction validators (i.e. “stakers”) lock their cryptocurrency away for the chance to propose the next block.[39] This means that they face large upfront costs to purchase the cryptocurrency, and receive the compensation in the cryptocurrency they are staking.[40] The cryptocurrency is an income-generating asset for stakers, incentivising them to hold it and act in a manner which allows the cryptocurrency to retain its value. The same incentive structure from Proof-of-Work holds for users and developers.

[39] A comprehensive overview of the Proof-of-Stake protocol and the game theory underpinning it is provided in the paper, “An Introduction to Distributed Ledger Technology”.
[40] As with Proof-of-Work, Block Reward = Transaction Fees + Block Subsidy

Figure 6: Stakeholder Incentives in a Proof-of-Stake protocol



Source: Aaro Capital Research

In both systems, as the usage of a platform increases, so does the demand for its cryptocurrency, thus increasing its market price. In Proof-of-Stake systems, the increased price makes staking rewards more valuable which tends to increase the portion of cryptocurrency locked up for staking, thereby exacerbating the demand. Miners and stakers are therefore incentivised to support the platform to encourage usage and consequently increase their income.[41]

3.2 Utility Tokens

Utility tokens are used to digitally access (or reward for providing) an application or service within a distributed ledger. Coupons, gift vouchers and loyalty points are straightforward use cases for utility tokens.[42] They are also used to influence the development of a dApp or a network, because in many cases they grant voting rights to their holders. More importantly, as explained in Section 2.3, utility coins provide an alternative revenue model for the development of a dApp. For a dApp to succeed, it requires users, developers and investors to contribute their time and resources. By issuing utility tokens, each participant is rewarded according to their contribution and can

[41] There are scenarios where participants may be incentivised to manipulate the cryptocurrency against the best interests of everyone else. This requires the malicious participant to be able to recover the cost of their investment before the price of the cryptocurrency declines. This has shown to be possible for smaller cryptocurrencies, where the same mining hardware can easily be used to mine multiple cryptocurrencies. For larger cryptocurrencies which require specialist and very costly mining equipment, this condition of profitability of a network attack seems less plausible. Such an attack has not yet been successfully undertaken on the largest cryptocurrencies.

[42] In paper form, they are generally fixed to a face value equal to the amount they are sold for. This fixed exchange rate prevents them from being considered securities, even though they otherwise have much in common with debt instruments (i.e. they are transferable, redeemable, have a fixed maturity date, etc.).

pay for services within the ecosystem using these tokens. If the dApp succeeds, then the value of the utility token increases and participants are rewarded depending on their relative contributions. Investors can bet on dApp success by buying utility tokens and, at the same time, support early adopters and developers as the price increases.

Some of the most prominent examples of utility tokens are those that adopt the ERC-20 Ethereum standard. ERC-20 defines a minimal set of functions and properties that a token must implement, such that it can be interoperable with other tokens adopting the same standard. Examples of projects include Maker (MKR), Basic Attention Token (BAT), USD Coin (USDC) and Augur (REP).

Regulatory perspectives of utility tokens vary by jurisdiction. In the UK, utility tokens include either current or prospective products, only if they do not give similar rights to security tokens. In the US, the SEC seems to restrict utility tokens as giving access to a service already available. In Switzerland, the FINMA allows classification across multiple categories (i.e. a hybrid token).

3.2.1 Payment / Access Tokens[43]

Payment (or access) tokens are the most common type of utility tokens. They are issued by a dApp or company and are used to access a defined service, similar to traditional paper tickets. The key differences are that they are often limited in number and trade on a wider secondary market.[44] Fairgrounds and gaming arcades have adopted payment token models to reduce the risk of currency theft, however outside of such environments there is little economic benefit of adding a representative token into the system.[45,46] Payment tokens therefore tend to be used as fundraising tools and are made available only in limited supply. This fosters a volatile secondary market and gives the token an independent valuation – an opportunity for investors to make a profit.

When more user-friendly applications are developed, users will likely be able to seamlessly buy and redeem the payment tokens they require without needing to be aware of their existence. This decreases the price risk of tokens to users, but implies that token velocity would be perpetually high. In other words, even if application usage increases, there may be a limited relationship between application demand and token price. This is known as having high velocity in the Quantity Theory of Money (QTM), characterised as having far more units of money than what is required to support transactions within an economy.[47] The issuer may be able to support thousands of purchases per day with the same fixed quantity of tokens being redeemed and re-issued again and again. Introducing an additional token of any sort may add another layer of friction to transactions, via conversion or liquidity costs, execution risks, tax implications, counterparty risks, or time delays. Thus, in the absence of any additional function of a payment token, they may be of little benefit to end users.

[43] There are varying definitions and interpretations of payment tokens. Amongst others, the Swiss regulator, FINMA, considers cryptocurrencies (e.g. Bitcoin) to be payment tokens, because they are designed as currency units. Given that 'token' itself means 'representative of', we tend to think of the term as inappropriate for cryptoassets with inherent value (such as bitcoin). Since the term came about, utility token has become an umbrella term for a number of sub-classes, one of which is more suited to the moniker 'payment token'.

[44] Ticket issuers often try and prevent the resale of tickets, however large secondary markets for tickets are common for events like football matches or concerts. Examples of such markets include https://guides.ticketmaster.co.uk/.

[45] For more information on fairground tokens, see: https://www.carterssteamfair.co.uk/tokens-of-fun-at-the-fair/.

[46] Another example of payment tokens are the chips used at casinos, which provide additional security as well as convenience.

[47] For more information on the quantity theory of money, see: https://www.investopedia.com/insights/what-is-the-quantity-theory-of-money/.

3.2.2 Work Tokens

Work tokens are used to provide a service (supply-side), unlike payment tokens which are used to acquire a service (demand-side). An individual who wishes to contribute towards a service must acquire the relevant tokens and submit them to the smart contract or protocol in the form of security bonds, which can be forfeited if the work is substandard.[48] In return, the worker is awarded with some positive cash flow – hopefully greater than the cost at which the work tokens were initially acquired at.

Work tokens are designed to be bonded and locked out of circulation for an extended period of time, decreasing velocity and increasing price. As demand for the service increases, so will revenues, leading to an influx of additional demand for the work token from new competitors on the supply side. This leads to a better standard of service which should attract even more new users. Developers and early adopters can monetise positive externalities as the network grows, compensating them for the high risk they initially took. The incentives of service providers with consumers are therefore aligned.

3.2.3 Reward tokens

Customer loyalty points, air miles, gift cards and coffee stamps are tokens that stand to benefit from digitisation in the form of utility tokens. Users can trade their collections on secondary markets at a premium or discount, and issuers can have more granular interactions with their customers.

Singapore Airlines has launched KrisFlyer, a blockchain based scheme where frequent flyers can convert air miles into tokens used to pay for goods and services from partner firms.[49]

3.2.4 Non-fungible tokens

Fungibility refers to the characteristic of goods, securities, or instruments that are equivalent and, therefore, interchangeable. This is useful in the case of securitisation and the fractionalisation of asset ownership. However, there are use-cases where the opposite is useful, where each token represents an entire, unique asset distinct from any other related asset. Non-fungible tokens (NFTs) fall into four key categorisations.[50,51]

- Personal digital identity
- Personal digital reputation
- Collectables (e.g. digital baseball cards)
- Digital membership (e.g. to a society)

In-game items have been an early and popular test bed for this technology, with CryptoKitties being the flagship example.[52] Players can create and earn assets which they fully own and trade. Real world collectibles may also

[48] This is easily measurable, as defined in the terms of the initial contract between service provider and user. For example, for providing server services, the provider must offer a certain amount of up-time and latency under a specified level. User feedback also provides an indication of the level of service provided.

[49] For more information on KrisFlyer, see: https://www.coindesk.com/singapore-airlines-blockchain-based-loyalty-program-takes-off.

[50] This is not necessarily an exhaustive list of categorisations.

[51] For more information on the categorisation of NFTs, see: https://www.cryptocompare.com/media/34478555/cryptocompare-cryptoasset-taxonomy-report-2018.pdf.

[52] For more information on CryptoKittes, see: https://www.coindesk.com/google-and-samsung-cute-cats-power-serious-15-million-cryptokitties-round.

be tokenised using NFTs – for example, stamps, classic cars and vintage bottled wine. This could reduce costs around authenticating and trading collectables.

3.2.5 Voting Tokens

Decentralised entities require a governance structure due to the issue of incomplete contracts.[53] To avoid centralisation, this governance is via stakeholder voting. This may be achieved via the issuance of voting tokens which are freely traded on secondary markets. This is similar to shares in traditional publicly traded equities, however only grant voting rights to token holders. Voting tokens allow holders to not only express their view, but also the intensity of their view by buying more tokens.[54] The upfront cost of voting tokens helps aligns the incentives of token holders. The more votes they "buy", the more they have to lose if they decide to vote against the best interests of the wider community.

3.3 Security Tokens

Security tokens are connected to assets that exist outside the blockchain and comply with existing legal frameworks. Examples of connected assets include equity stakes in companies, debt, and units in a fund.

In the UK, security tokens are cryptoassets that have the characteristics of a Specified Investment. In Switzerland, FINMA defines asset tokens as cryptoassets that represent a claim on the issuer. In the U.S., the Howey test is used to determine whether a financial instrument qualifies as a security. It defines a security as anything which meets all three of the following criteria: there needs to be (1) an investment of money, (2) in a common enterprise and (3) with reasonable expectation of profits derived from the efforts of others. In April 2019, the SEC published a framework for analysing whether tokens satisfy this test.[55] According to the framework, the first two criteria are usually satisfied in the offer and sale of cryptoassets. Therefore, the security classification depends on whether the third criterion is also satisfied. The framework interprets the third criterion in relation to the actions of active participants, who are those responsible for the development and the operation of the network. For example, does an active participant control the supply of tokens, and therefore their price? If a service is sufficiently decentralised (e.g. bitcoin), then active participants do not possess any informational or market advantage, and hence tokens would not be considered securities.

The advantage of security tokens is that they can automate and streamline certain aspects of the process by removing third parties, thus reducing costs and time delays, especially in settlement and payments. Registrars, as the ultimate keeper of the record of ownership, can be decentralised using DLT, custody can be mutualised using cryptography, rules can be enforced with smart contracts and voting, and payments can be processed within the blockchain natively.

[53] Governance is necessary because contracts are inherently incomplete, meaning that there will always be conflicts which cannot be resolved by a contract or smart contract. For more information on the key causes of contract incompleteness, see: https://medium.com/prysmeconomics/incomplete-contracts-and-blockchain-ac9f348a2e6fhttps://medium.com/@PanteraCapital/a-masterclass-on-blockchain-governance-design-b793695cb134.

[54] The lack of ability to express the intensity of preferences in national or regional government voting systems likely leads to sub-optimal election results. On the plus side, one vote per person makes it harder for one individual to disproportionally influence an election. For DLT based systems, if a malicious player gains outsized influence of a protocol, other users can choose to fork the ledger and remove the malicious player. This cannot easily be done with governments, and therefore sybil attack resistance is a higher priority.

[55] For more information on the SEC's guidance on cryptoassets, see: https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

Table 7: Examples of how and where security tokens can be implemented

Example	Explanation
Multi-trading venues	Remote and local registrars have to share data and be able to delineate and satisfy their respective responsibilities cleanly. DLT can offer a trustless multi-version concurrency control mechanism which simplifies international collaboration. International liquidity for access and trading could therefore be increased thanks to reduced administrative friction.
Automation of equity shares	Shareholder participation and dividend payments can be automated. Two-way communication and authentication of votes can be handled by the DLT, quicker and cheaper than AGMs. Dividends and interest payments can be distributed by the same mechanism - the issuer simply posts a payment transaction crediting the public keys of all current holders as recorded on the ledger at the record date.
Liquidity	Liquidity of traditional securities is already high and benefits from digital infrastructure. However, pre-trade credit arrangement, post-trade settlement of assets, and reconciliation between a hierarchy of intermediaries all add delays and costs to movement. Since the rules of credit, verification of identity, and settlement can all happen coherently on the same DLT in close to real-time, the catchment area of liquidity will be increased.

Source: Aaro Capital Research

The Security Token Offerings (STOs) industry includes new security token exchanges dedicated to DLT-based securities, as well as traditional security exchanges who are transitioning to DLT. Both the Stuttgart and Australian stock exchanges are developing such platforms.[56,57] Given that much of the world's securities rules are bound up in the current infrastructure of the securities markets, without the help of these platforms it will be difficult for DLT-based securities to be ratified by regulators despite meeting the spirit of the law. As a stop-gap, it is possible for a firm to issue traditional securities and sell them to a special purpose vehicle or trust which holds shares on behalf of the investors, who are in turn issued with tokens as IOUs for the shares. These are tokenised securities.

Since tokens are by default a bearer asset, security tokens need to implement some form of inherent linkage with real-world identity for ownership verification and prevention of accidental loss of assets. Using a similar technique to the stop-gap explained above, bearer security tokens can be secured by a custodian who then issues non-bearer, tradable replications of these assets.[58]

Securitisation is the process of using financial engineering to make illiquid assets more liquid and suitable for trading. Tokenisation could be considered an evolution of securitisation. Not only do tokens and tokenised assets enable fast and easy ownership transfer like securities do, but they can also encapsulate logic and data. Tokens can be programmed to be accessible only to individuals who qualify, such as those who are certified as meeting the professional or sophisticated investor criteria. Tokens can expire, split, convert, distribute profits, accumulate interest and store data, all in programmatic ways that can be fully automated. The potential of tokens to enhance

[56] For more information on the Stuttgart Stock Exchange's blockchain plans, see: https://www.presseportal.de/pm/80210/4229254.

[57] For more information on the Australian Stock Exchange's blockchain plans, see: https://www.asx.com.au/services/chess-replacement.htm.

[58] An example of a company offering a stop-gap solution for cryptoassets is Koine, see: https://www.koine.com/.

financial engineering is clear, but practical applications are still in their early stages. It is likely that the flexibility of programmable financial instruments could pave the way for very complex investment dependencies and also have a reduced total cost profile versus traditional securities.

3.3.1 Equity Tokens

Equity tokens allows investors to hold traditional equity, but in the form of DLT tokens. Investors have the right to vote at annual general meetings, receive dividends, and are subject to the usual palette of corporate actions such as accounting splits and mergers. Nivaura and Securitize offer regulated equity token platforms and the London Stock Exchange has worked with Nivaura to issue an equity token for a start-up financial services company.[59,60]

Equity tokens can offer more features than traditional equity instruments, given that they rely on software. Their pay-outs are automated, meaning there are no accounting errors, such as deducting too much withholding tax or skipping certain holders during the dividend distribution process. Voting may also be carried out securely via the distributed ledger.

3.3.2 Debt Tokens

Debt tokens exist in the same technological and regulatory niche as equity tokens, with the difference being that they follow the rules of debt rather than equity instruments.

The par value, maturity date, coupon sizes and payment dates are all pre-scripted and fixed in the smart contract behind the token. Whoever holds the debt token at the time of any coupon payment date will receive the interest to their ledger address automatically, without having to fill in a transfer form and notify custodians of their bank account details.

Hybrid securities such as convertible bonds can also be replicated using tokens. It is possible there will be a surge in the next few years of innovative structured financial products which would have been difficult to facilitate in the past.

3.3.3 Asset Backed Tokens

For centuries, businesspeople have been bundling assets up into pools and issuing IOUs, certificates of deposit, shares and other liens to investors. Asset backed tokens can be considered the next technological step in this area. Many physical assets are valuable but ill-suited for use in markets, and especially digital markets, simply due to their mass or fragility.

Fractional ownership of companies is an old idea, but thanks to tokens this concept has spread to asset classes which have not traditionally been fractionalised. For example, high value art works are being tokenised by segregating ownership from custody and selling the ownership in many pieces as tokens.

The commodities trading world is accustomed to using derivative contracts to trade the ownership of metals and food crops repeatedly while the assets themselves sit motionless in a warehouse. By moving this activity into token form, the flexibility and scope increases further still.

[59] For more information on Nivaura, see https://www.nivaura.com/.
[60] For more information on Securitize, see: https://www.securitize.io/.

3.4 Stable Coins

Stablecoins are designed to reduce price volatility relative to a reference asset, either by directly linking to it, or by providing a hedging mechanism. A stablecoin can be pegged to:

- A currency or basket of currencies;
- Exchange traded commodities (such as precious metals or industrial metals);
- Other cryptocurrencies.

When pegged to other currencies, stablecoins can be thought of as a form of “private currency”. Stablecoins backed by assets held by trusted third parties (such as currencies, metals and cryptocurrencies) are said to be “centralised”, while those linked to other cryptocurrencies via smart contracts are “decentralised”. The benefit of the peg is the reduced volatility of the stablecoin, which is contrasted with the price volatility of more well-known cryptocurrencies, such as BTC and ETH. However, if a stablecoin is pegged to a currency of a specific country, there is the drawback of the implicit link to its monetary policy. For example, if a developing country predominantly uses a stablecoin pegged to the USD, it will also “import” US monetary policy, which may be incompatible with its own economy. Other challenges relate to the intrinsic costs of DLT, hacking risks, and counterparty risks (as is the general case for private currencies).

Stablecoins have the potential to take a notable role in the global payment system over the medium term, especially in international remittances and e-commerce. For example, pegging to a basket of currencies may favour increased adoption in the context of international trade, where exchange rate risks can be minimised either across currencies in a given region, or against the dominant global currency – the US dollar. Compared to other forms of electronic money, such as PayPal, their advantage is that information about transactions is not captured by a trusted intermediary, who can then abuse it. Price stability can be achieved quite easily by fully collateralising tokens with the assets they represent.

Case Study: Tether

Tether is the most widely used stablecoin. It is simply a corporate issued token by a firm with a USD bank account. Customers deposit USD to Tether’s bank account and in return Tether will mint some tokens, one for each dollar deposited, and send them to the buyer. Tether is therefore a form of representational money with good price stability. Note that its price does vary from its dollar peg within a few percent due to natural fluctuations in supply and demand and relative market inefficiencies. Occasionally, there are more significant shocks to the price, when the market’s trust in Tether’s ability to repay all liabilities is eroded. Therein lies the major risk that Tether investors must accept in return for their dollar peg – credit risk. Credit risk aside, users of Tether tokens have a special flavour of the USD, which has some of the traits of a cryptocurrency like bitcoin in that it is borderless and censorship resistant in its transactions.

Case Study: Libra

Libra, the electronic currency proposed by Facebook, technically qualifies as a stablecoin. Libra is not pegged to one specific currency, but to a group of “low-volatility assets, including bank deposits and government securities” in multiple currencies (the Libra Reserve). However, this is not a hard peg enforcing a constant value vis-à-vis a currency, but rather a soft peg with reserves guaranteeing some lower bound to Libra’s values.

The aforementioned stablecoins still require a trusted intermediary in order to safeguard the collateral, and possibly even another intermediary to verify that the collateral is indeed safeguarded. It is an interesting challenge therefore to design a decentralised stablecoin, which is non-volatile and fully censorship resistant, or trustless. Such coins generally implement some form of algorithmic monetary policy, which reduces supply of the stablecoin when its price increases and increases it when its price decreases.

Case Study: Dai

Dai (from MakerDAO) is a decentralised stablecoin implemented as a smart contract using the ERC-20 Ethereum standard. Price stability is achieved using a two-token system, consisting of Dai, which targets a value of $1, and Maker (MKR), which is used to pay interest on Dai loans and grants voting rights on the system.

To explain the mechanism, consider the following example. Suppose that the price of 1 ETH is $100. A borrower places 1 ETH as collateral in order to borrow Dai. The ETH is put in a Collateralized Debt Position, which is essentially a smart contract that locks the ETH until the loan is repaid. This contract specifies a collateralization ratio, which determines how many Dai are created as a loan from 1 ETH. If the ratio is 150%, for instance, then 66 Dai are loaned to the individual. These Dai are newly created and will be destroyed when the loan is repaid. Effectively, if 1 Dai is worth $1, the individual has borrowed $66 worth of Dai, placing $100 worth of ETH collateral. He can now use Dai for transactions, just like with any other cryptocurrency. When the loan is repaid, the 66 Dai are destroyed and he receives his collateral of 1 Ether. Additionally, he pays an interest (called the stability fee) in MKR.

Since the Dai is freely traded, its price can fluctuate. However, when the price drops below $1, someone with an open Collateralized Debt Position is incentivised to buy more Dai and repay his loan at a lower cost. For example, if the price of Dai is $0.5 and the price of 1 ETH is still $100, it makes sense for the aforementioned individual to buy 66 Dai in the open market at the price of $33 and repay his loan of $66, so that 66 Dai are destroyed. This increase in the demand for Dai and decrease in its supply results in a price increase.

When the price rises above $1, there is an incentive to open more Collateralized Debt Positions in order to receive Dai that are worth more. For example, if the price of 1 ETH is still $100 but the price of 1 Dai is $2, then with the same collateralization ratio of 150% an individual can borrow 66 Dai, worth $132. By selling them in the open market and never repaying the loan (hence forfeiting the ETH collateral worth of $100), he makes a profit of $32. As more Collateralized Debt Positions are opened, new Dai are created and this increase in supply leads to a decrease in its price.

The collateralization ratio protects the borrower from a large decrease in the price of ETH. If the individual does not repay the loan and the value of the collateral (ETH) drops dangerously close to the value of the Dai that it is backing, the smart contract liquidates the collateral and auctions it off to the highest bidder. The 150% collateralization ratio effectively allows for a drop of up to 33% to the price of Ether, before it is worth less than the 66 Dai that are borrowed, in the case that the price of 1 Dai is $1. In practice, the liquidation occurs much earlier.

If a very big depreciation of the collateral occurs suddenly because the price of ETH suddenly crashes, there is the danger that loans are not repaid on time (or more collateral is injected), and the Collateralized Debt Positions are not auctioned off. In that case, a process called global settlement takes place. It simultaneously liquidates all open Collateralized Debt Positions and returns them to the borrowers, destroying all Dai. This process is triggered centrally by a group of active participants in the Maker network, who hold the token MKR, thus creating a centralization element to the network.

4 Fundraising

The emergence of the crypto ecosystem has given rise to new tools which projects and companies can use to raise capital from investors. These include initial coin offerings (ICOs), security token offerings (STOs) and initial exchange offerings (IEOs).[61] These new mechanisms give rise to an interesting new dynamic of liquid venture capital investing, where investors can potentially benefit from exchange traded secondary markets for early stage investments in token form.[62]

4.1 ICOs

Initial coin offerings (ICOs) draw on ideas from the initial public offerings (IPOs) model of the corporate equity market. Unlike IPOs, they are directly accessible to individuals without the need for financial intermediaries. DLT, typically Ethereum, is used as a decentralised and permissionless intermediary between fundraisers and investors.

To raise capital, fundraisers issue a dedicated token to investors. During the development phase of a project the tokens act as IOUs which can be traded on public secondary markets. Once the project has an active product or service, these tokens provide utility to their holders. For example, Binance Coin tokens give holders discount on exchange fees, and 25% of Binance's profits are used to buy back tokens.[63] Projects raising via ICOs will usually accept investment in cryptocurrency, which gives them access to a global pool of investors. Others may choose to accept fiat currency.

ICOs can be viewed as a proof-of-concept for large-scale private market investment. The private equity and private market investment universe makes up a large portion of global wealth. They are, however, by definition not accessible to most people. ICOs enable private enterprises to issue tokens to a global audience and, while laws will continue to shape who can have access, this technology ultimately expands the potential reach.

The practices around ICOs has matured and general norms have been established. ICOs tend to launch with a marketing document, a whitepaper. This can be thought of as the equivalent of a prospectus for an IPO, although there is still work to be done on standardisation and regulatory compliance. In the whitepaper, founders lay out their vision, the capital required and timeline. Some projects have prototypes ready by this stage, but many in the ICO bubble of 2017 still raised capital with nothing more than a whitepaper. Fundraises typically limit the number of tokens either with a fixed price offered on a first come first served basis, or with some variable price based on an auction. A soft-cap is the minimum amount of funding needed to deliver the project, and a hard-cap is the fundraising limit. If the soft cap is not reached, investors have their capital returned. Most ICOs are now issued via ICO platforms which offer a more structured framework for issuing tokens to investors.

An advantage of the ICO model is that it can deliver a user base for a project from the day it launches. Projects often try to design their ICO process to capture a wide base of investors interested in using their product, rather

[61] We do not cover IEOs as the underlying economics is very similar to ICOs. The key difference is that issuance is via an exchange, who then provide instant liquidity to investors.
[62] There is an OTC secondary market for VC equity investments, which is illiquid relative to publicity traded markets, particularly for early stage investments. Note that any publicly traded market for early stage investments will still likely be very thin, as demonstrated by existing early stage tokens.
[63] For more information on binance coin, see: https://info.binance.com/en/currencies/binance-coin.

than just speculators only interested in selling on their stake for a profit. Some combination of both groups usually achieves the best funding and diversity ratio.

Even with the use of DLT to carry the tokens, the capital at risk very much depends on the integrity, talent and luck of the founders. A report by Status Group identified that over 80% of ICOs conducted in 2017 were scams, with only 70% of capital raised going to genuinely high-quality projects.[64] The secondary market may have limited liquidity, leaving investors with limited avenues to exit their positions. Smart contracts and DLT platforms which carry the tokens can also suffer from design flaws and bugs.

As the technology develops, smart contract standards can be established and made more robust through repetitive use. This can result in routines that are even more secure than traditional stake tracking technologies such as bilateral private paper contracts or central registries. Countries such as Malta and France are also building regulatory frameworks for ICOs.[65,66] Alternatives to the traditional ICO model, such as DAICOs, have been designed with the aim of protecting investors and incentivising good project management.[67]

4.2 STOs

Security token offerings (STOs) stand in contrast to ICOs specifically in their regulatory status. STOs may be considered a sub-class of ICOs, which have been given approval or exemption by the local regulator within the traditional regulatory framework. STOs, partly by convention and partly by necessity, contain explicit rights and obligations. As discussed in section 3.3, equity and debt tokens are designed to replicate and extend the features of these familiar security classes.

Most current security token projects operate within the exemption rules of securities regulators which tend to restrict their availability only to accredited and professional investors. Due to their inherent programmability, security tokens lend themselves well to legal compliance by auto-enforcing the rules under which they operate.

4.3 Liquid Venture Capital[68]

Venture capital (VC) funds, being part of the private equity fund universe, are subject to the J-curve effect.[69] Investments in start-up companies are private, illiquid and take many years to garner a positive return. Funds tend to have negative returns in early years (the down swing in the 'J') whilst their portfolio companies draw down on capital. In later years when revenue is generated, the portfolio can return positive cash flows. VC funds usually

[64] For more information, see: https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ.

[65] Malta was the first country to establish a regulatory framework for ICOs in 2018. This framework does leave areas to be desired from a financial regulatory framework, but is a step in the right direction. More information can be found at: https://icomalta.com/ico-regulation/.

[66] France's financial watchdog is set to launch a more sophisticated ICO framework. For more information see: https://www.reuters.com/article/us-crypto-currencies-regulation-france/france-to-approve-first-crypto-issuers-as-new-rules-loom-idUSKCN1UB18P?feedType=RSS&feedName=technologyNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FtechnologyNews+%28Reuters+Technology+News%29.

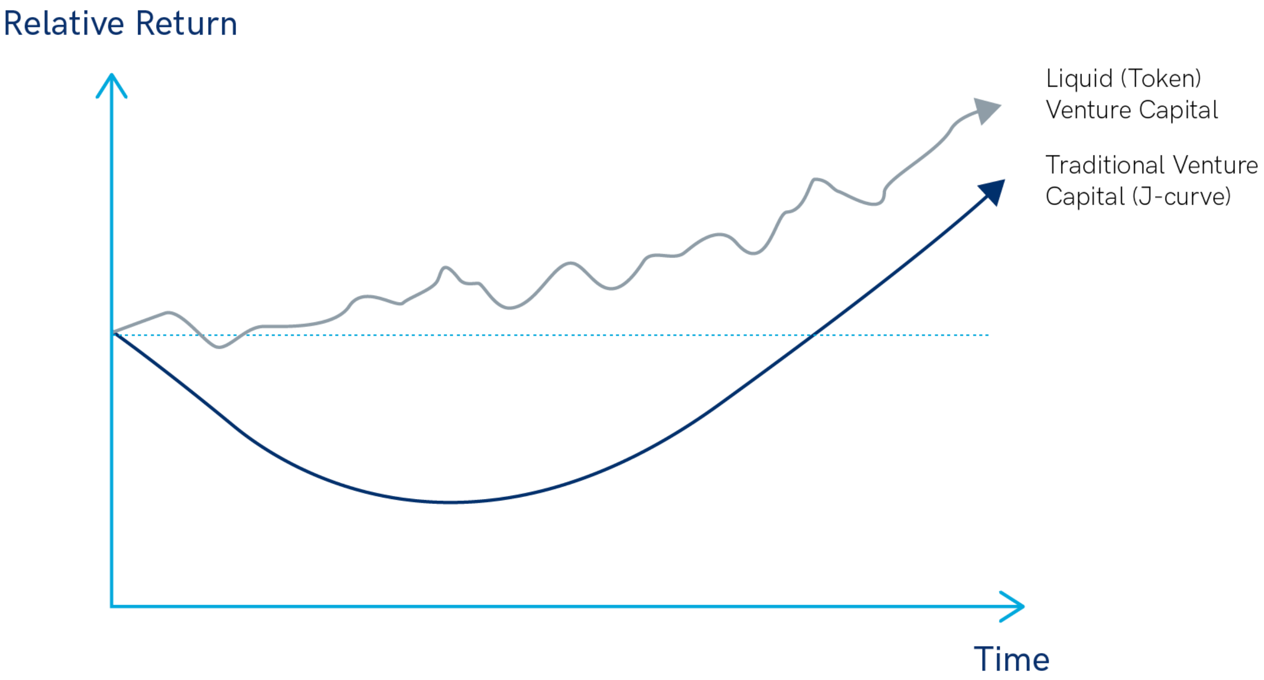
[67] For more information on DAICOs, see: https://ethresear.ch/t/explanation-of-daicos/465.

[68] A discussion of liquid venture capital is also available here: https://multicoin.capital/2017/08/15/venture-capital-economics-with-public-market-liquidity/

[69] For more information on the J-curve, see: https://en.wikipedia.org/wiki/J_curve#Private_equity.

realise the bulk of their returns by exiting the investment in a bulk sale to another private investor, an equity buyback by the start-up, or through an IPO.[70] This process typically takes between 7 and 13 years.

Figure 7: Return Profile for Traditional vs Token Venture Capital

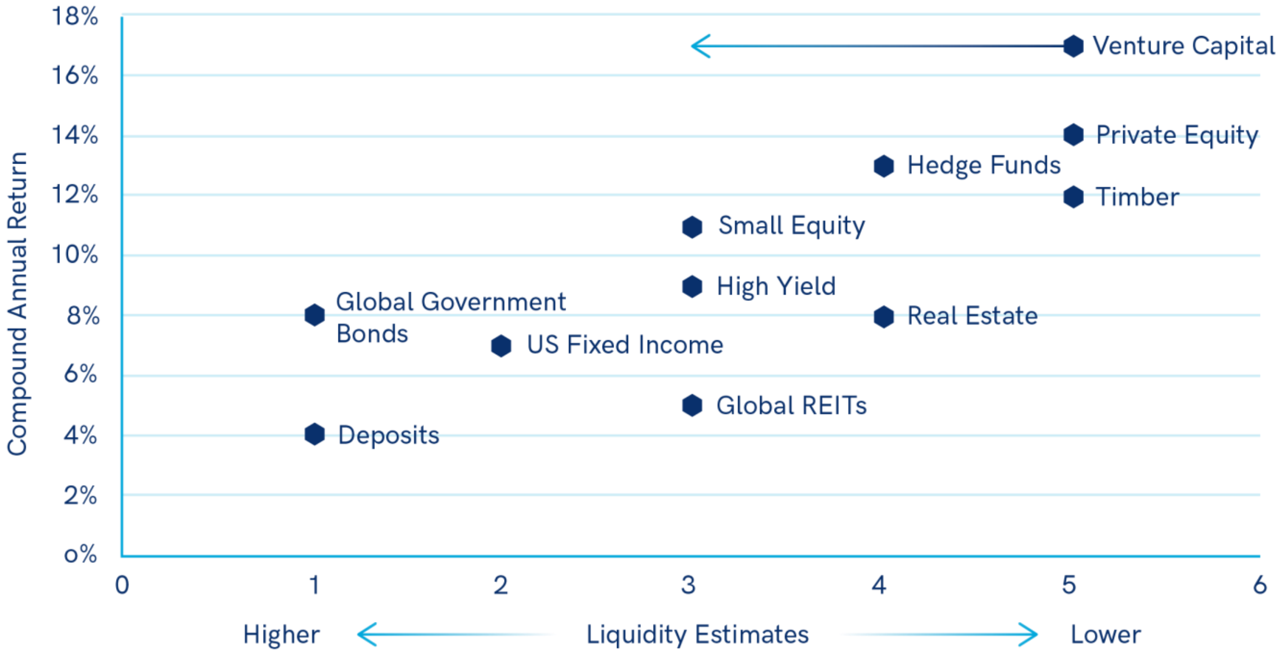


Source: Aaro Capital Research

Token venture capital funds invest in tokens issued by start-ups. By building a portfolio of tokens rather than private shares, they are relatively insulated from the J-curve effect as the tokens tend to reflect some book value or premium for the project they represent through the development lifecycle. Figure 8 plots traditional VC against other asset classes in terms of its relative liquidity and expected return. The arrow indicates the aim of liquid venture capital. Increased liquidity also allows funds to adjust holdings depending on progress of the project or diversify risk by buying into competitors.

[70] There is an OTC secondary market for VC equity investments, which is illiquid relative to publicity traded markets, and especially illiquid for early stage investments.

Figure 8: Expected Asset Class Returns vs Liquidity



Source: "Expected Returns", by Antti Ilmanen, 2011. Scatter plot of average asset returns 1990-2009 on (subjective) illiquidity estimates; Bloomberg, MSCI Barra, Ken French's website, Citigroup, Barclays Capital, J.P. Morgan, Bank of America Merrill Lynch, S&P GSCI, MIT-CRE, FTSE, Global Property Research, UBS, NCREIF, Hedge Fund Research, Cambridge Associates. For illustrative purposes only. Actual future results may differ materially from expectations.

A key consideration for liquid venture capital managers is whether the value of the project will be transferred to the token they are buying. For security tokens, there will be a clear value transfer mechanism. For utility tokens, this mechanism needs to be clearly defined (e.g. via token buy-back programmes).

Such liquidity also brings risk. Traditional VC investment only offers price information when a new round of fundraising is completed, which can be a very occasional event. In an actively traded market, prices become more volatile, introducing the issues of human sociology around trading. Rather than simply focusing on maximising returns in the long-run, liquid VCs contend with volatile prices and therefore the validity of the portfolio's value becomes a factor they must manage. As these assets are now liquid, investors typically demand increased access to their capital, forcing managers into an open-ended hedge fund structure. This has disadvantages in terms of increased administrative distractions and incentive misalignment, as performance fees are paid out more regularly and cut into long-term returns.

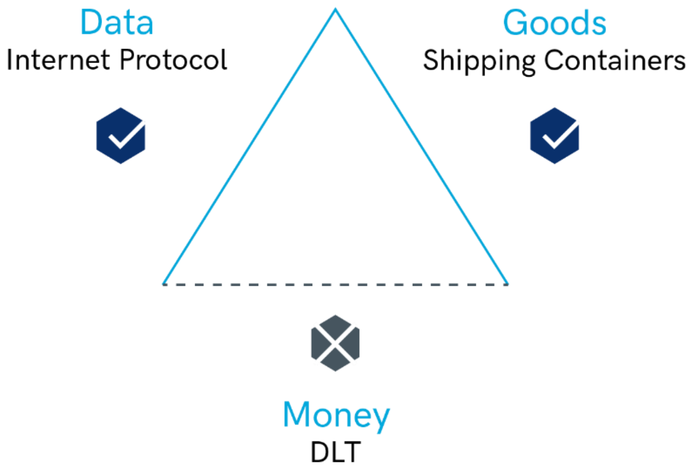
It can be argued that the illiquidity of venture investments is not necessarily something to be fixed. Many start-ups are looking not only for investment, but also experienced stakeholders who bring more value than just capital to the project. In such an arrangement, an investor may not transfer their holding without materially affecting a project’s chance of success and so explicit contractual restrictions are placed on liquidity.

5 Internet of Value: Integrating the Financial and Information Layers of the Internet

The two key technological tools underpinning the modern economy - the Internet and the digital payments infrastructure - currently utilise different technology stacks and achieve different outcomes in terms of user experience and cost. Using the Internet, users can video call in real-time across the world from a mobile phone and send large files almost instantly for free. In contrast, to transfer 10,000 EUR between the UK and the Eurozone, it is typically both quicker and cheaper to fly with the cash than to transfer electronically. For Internet card payments, merchants are typically charged around 2% per transaction and wait weeks for final settlement.

The Web's designers envisaged a payment technology layer which would interact with the Web, enabling users to quickly and cheaply pay for goods and services. They created the HTTP code 402 to handle errors from such a payment layer. However, the digital payment infrastructure continued to be developed by the financial system largely independent of the Internet, and '402' therefore enjoys little usage at present. The current digital payment system remains highly fragmented relative to the Internet.

Figure 9: The Internet has been a force for globalisation, and cryptocurrencies can be expected to reinforce that pattern



Source: Blockwall Management GmbH

Interbank payments and transfers are largely a national affair with ACH in the US, Faster Payments in the UK and TARGET2 in the Eurozone. As payment systems move money issued by central banks and commercial banks, the systems are often closely tied to the national jurisdiction.

Even within a single jurisdiction, payments are fragmented across multiple independent systems. The UK has at least three: BACS, CHAPS and Faster Payments. They differ in speed, cost, transaction limits, access, and security/finality. Some payment systems have multiple layers of security and enable transaction reversal, while others will always guarantee execution and finality (see Table 8 below). Not all bank accounts are connected to all three systems.

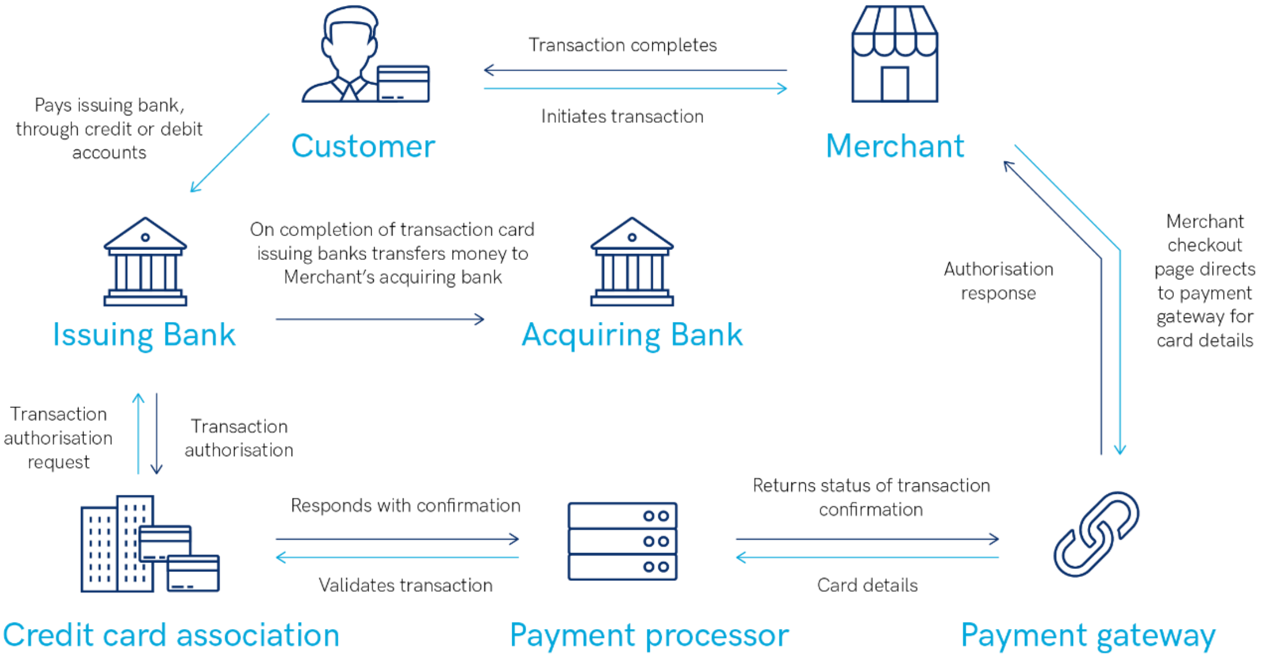
Table 8: Characteristics of the UK’s Payment Systems

	Limits	Cost	Speed
Contactless	30 GBP/transaction	Free for the end user	Up to 4 days
Faster Payments	250,000 GBP/day		Minutes or hours
BACS		Low cost	Several days
CHAPS		20-30 GBP	Within 3 hours

Source: Aaro Capital Research

Since the Web was created, many associated payment systems experienced high growth and became very popular. These include Visa and MasterCard credit and debit cards and PayPal. Each of these private services can disconnect any user or merchant at their discretion, have high fees, slow settlement and high fraud risks. This fragmentation has created a market opportunity for aggregators such as Square and Braintree, at a cost to merchants and thus retail users.[71,72] Figure 10 below outlines the many financial intermediaries and steps currently involved in processing an online payment.

Figure 10: Traditional payment systems diagram


Customer
Transaction completes
Initiates transaction
Merchant
Pays issuing bank, through credit or debit accounts
On completion of transaction card issuing banks transfers money to Merchant’s acquiring bank
Issuing Bank
Acquiring Bank
Authorisation response
Merchant checkout page directs to payment gateway for card details
Transaction authorisation request
Transaction authorisation
Responds with confirmation
Validates transaction
Returns status of transaction confirmation
Card details
Credit card association
Payment processor
Payment gateway

Source: Aaro Capital Research

[71] For more information on Square, see: https://squareup.com.
[72] For more information on Braintree, see: https://www.braintreepayments.com.

The large electronic payment and international bank transfer market is almost exclusively controlled by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).[73] It connects more than 11,000 financial institutions in 200 countries. The first SWIFT message was sent in 1977, and its technology was upgraded in 2005 to SWIFTNet using IP instead of X.25. The SWIFT network however is not as secure as might be expected given its importance:

- The 2015-2016 hacks of banks in Bangladesh, Vietnam and Ecuador led to the theft of 100 million USD. [74] SWIFT messages were sent but local records (PDF and print) were modified to look unsuspicious.
- In early 2018, two junior employees at Punjab National Bank, India, stole 1.8 billion USD by sending illegal letters and deleting transaction records in the internal system.[75]

While this globally unique method of identifying bank accounts and routing information has largely been a great success, settlement still takes days, end user fees are a minimum of 25 USD, and security is not a core consideration to the system. SWIFT is also often caught in geopolitical pressures to disconnect entire countries.[76]

5.1 Integration of the Information and Payment Layers of the Internet

For fully digital services such as social media, where information itself is the value, distributed ledgers are a natural building block for combining payments with the service provision. Facebook's Libra project is a step in this direction.[77] When purchasing a virtual product, users exchange one piece of data for another, where one piece is the product and the other is electronic money. It thus makes little sense to keep the information and payment layers of the digital world separate.

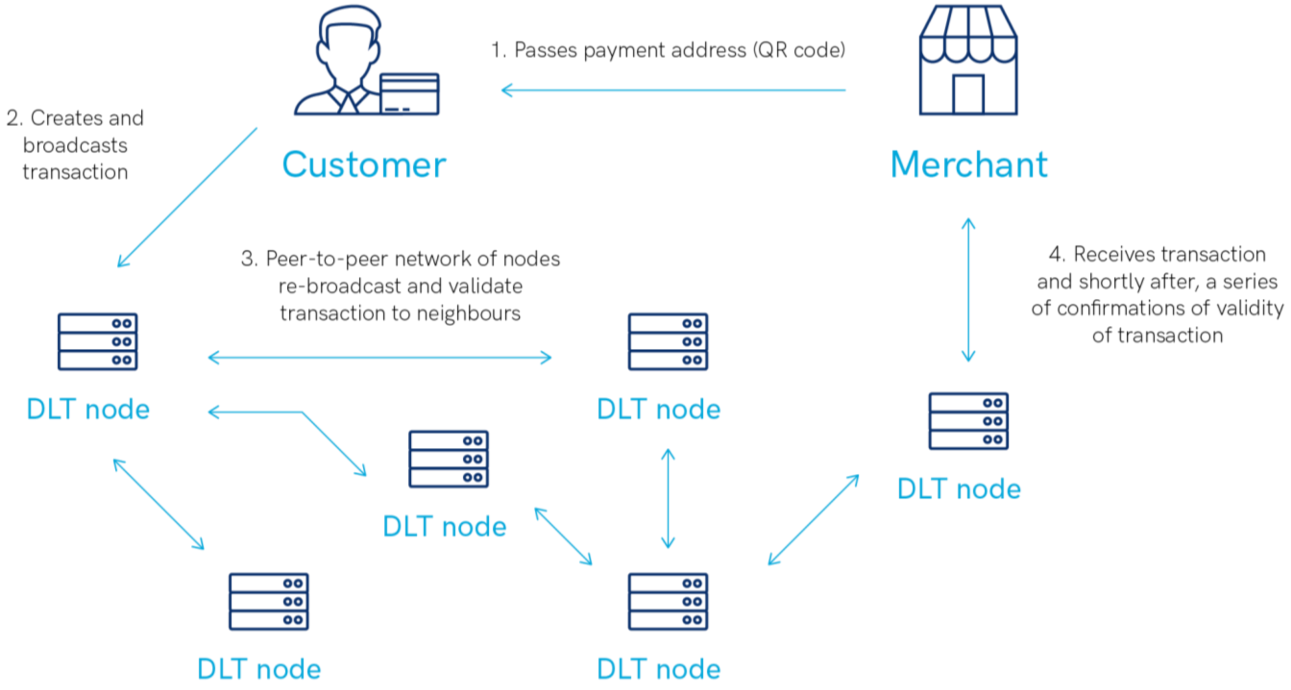
Micropayments may be a viable alternative to advertising as a source of funding for online content creation. Under the traditional payments model, micropayments have struggled to find a role due to poor integration with the Web and relatively high cost of transaction. Web 3.0 is a natural home for micropayments where iterative content delivery can be conditional on iterative debits with virtually no overhead. Such payments can be ad hoc, pay per use and not require any account set up or subscription agreement. In addition, the content may be protected from unlicensed re-distribution by means of digital rights management being tightly integrated into the same architecture handling the delivery and payment.[78] Project Mycelia by the musician Imogen Heap is an example of such a system in which the copyright owner of the music is paid their fee in real time through a smart contract.[79]

One key difference between traditional and DLT-based payments is transaction finality. For most forms of distributed ledgers, especially permissionless ledgers, finality increases over time but never reaches 100% - a trait known as probabilistic finality.[80]

[73] For more information on SWIFT, see: https://www.swift.com/.
[74] For more information on these SWIFT hacks, see: https://www.bankinfosecurity.com/another-swift-hack-stole-12-million-a-9121.
[75] For more information on the Punjab National Bank theft, see: https://qz.com/india/1208266/the-1-8-billion-punjab-national-bank-nirav-modi-fraud-explained
[76] For more information on SWIFT's non-impartiality, see: https://www.rt.com/business/441904-iran-swift-mnuchin-sanctions
[77] For more information on the Libra project, see https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf.
[78] DLT for the first time allows for digital scarcity as it is no possible to create an indistinguishable copy. It also allows for sellers maintain ongoing digital rights management after sale.
[79] For more information, see: myceliaformusic.org/
[80] For a more detailed treatment of probabilistic finality please refer to the paper "*An Introduction to Distributed Ledger Technology*"

Figure 11 below outlines how an online payment via DLT works.

Figure 11: DLT payment systems diagram


1. Passes payment address (QR code)
2. Creates and broadcasts transaction
Customer
Merchant
3. Peer-to-peer network of nodes re-broadcast and validate transaction to neighbours
4. Receives transaction and shortly after, a series of confirmations of validity of transaction
DLT node
DLT node
DLT node
DLT node
DLT node
DLT node

Source: Aaro Capital Research

5.2 Regulation of Web 3.0 Payment Systems

Barriers to entry are high despite the multiple payment systems currently in play, so much so that the EU passed the Payments Services Directive to force incumbents to open their platforms and their customer ownership in an attempt to level the playing field.[81] Payment systems in Web 3.0 would be inherently open to competition both in development efforts and via the diversity of alternative schemes. However, increased innovation could pose risks in the form of software bugs and the handling of accountability. Regulators will naturally be inclined to impose a framework on commercial users, such as merchants, to ensure minimum standards.

Regulatory requirements in the distributed ledger services field so far have focused on streamlining Know Your Customer (KYC) and Anti-Money Laundering (AML) rules. On public DLT networks, we are observing the potential for a partition of assets into a set of KYC compliant coins and a set of coins which do not have a complete KYC record. There are bridges between these two partitions though. US government agencies, for instance, have seized cryptocurrency proceeds from crime which are later sold at auction, thus porting them over to the 'KYC partition'.[82] Protocol developers are researching techniques to prevent partitions from occurring for any such reason as they might be deemed to harm the value of a cryptocurrency.[83]

[81] For more information on the Payments Services Directive, see: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en.
[82] For an example of a cryptocurrency auction, see https://www.usmarshals.gov/assets/2018/bitcoinauction/
[83] For more information, see: https://bitcoinmagazine.com/articles/taproot-coming-what-it-and-how-it-will-benefit-bitcoin

6 Benefits of Decentralised Markets

Distributed ledger technology offers several interesting features for marketplaces: trust minimisation, open data, reduced fraud and embedded logic in cryptoassets. Decentralised marketplaces can operate without the need of a legal entity, as profits can be generated and distributed without the requirement of a bank account or any other specific third party. They have no single server or data centre and therefore can operate reliably around the clock and be accessible globally. They can also make use of smart contract-based escrows to keep parties safe while physical goods are shipped, and thus maintain trust.

6.1 Reduce Payment Administrative Costs

Reconciliation of in-house and external records is a laborious and costly overhead for any business. By referencing a shared external ledger, businesses can all but do away with reconciliation. Auditing of historical accounts is also made easier due to the reduced risk of errors and abuse.

6.2 Trust Minimisation and Fraud Reduction

For cryptoassets, controlling the key that moves the asset implies ownership of the asset. As cryptoassets can be placed under the framework of a smart contract, what can happen to that asset is clearly defined and the rules are known and verifiable, thus greatly reducing the opportunity for fraud. Consumers are less dependent on a regulator to ensure fair practices and there is reduced need for legal infrastructure in resolving disputes.

While distributed ledgers are good at forming an 'internal truth' such as the correct ordering of transactions, they are less adept at identifying 'external truths' such as the amount of rainfall last week in Ohio. Inaccurate data entered on the ledger about a product or event could lead to a loss of faith in decentralised markets. Identity rating systems and particularly stake-secured reputation systems will help consumers identify safer trading counterparties and also disincentivise fraudulent data entry. The increased auditability of DLT-based market platforms could deter fraud, tampering and increase the integrity of any associated physical delivery service through staked collateral and escrow of payment. Supply chain tracking on distributed ledgers can be highly automated by means of 'internet of things' (IoT) class devices including electronic seals and tamper resistant sensors. Where such devices can add their own entries to ledgers is opportunity for high scale automation and verification cost saving. While trust will always be required to some degree when interfacing with the physical world, the DLT layer allows a trustless shared infrastructure to be built mutually and improve on existing database controlled processes.[84]

6.3 Data Sharing and Ownership

Raw data held on distributed ledgers and storage networks is publicly available, making such assets and relationships available via multiple portals and interfaces.

This openness allows consumers to easily compare functionality and costs (if any) between portals and they will not need to create new user accounts and relationships for each. To some extent, this function is available and undertaken in the current web by data aggregators such as Skyscanner and Momondo in the air travel business. Such services however do have non-trivial costs and require proprietary databanks. Open data allow start-ups

[84] A more detailed discussion on cost savings of verification via DLT can be found at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598.

to more readily identify market opportunities or create competing services, again increasing diversity and potentially lowering prices for consumers.[85]

6.4 Examples of Early Decentralised Markets

6.4.1 Open Finance

The tokenisation of funding has greatly reduced the setup and operating costs of financial services, and has broadened the addressable market globally. For middle classes in emerging markets such as Brazil and Russia, ICOs have been popular, easily accessed and offer higher risk/reward investments. Traditionally, access to global financial markets has been limited and expensive for retail investors in many countries.

Open finance creates new investment opportunities including cryptocurrencies, utility, security and asset backed tokens. Tokens make independent fundraising and investing possible anywhere the internet reaches, from hyper local to hyper global markets.

6.4.2 Prediction Markets

Prediction markets are a means of crowdsourcing sensible opinion about the probability of a specified outcome of some event, such as an election. They work by allowing participants to place bets on either their agreement or disagreement with the stated question, by means of taking either a long or short position on some 'shares' in the market. Thus each bet changes the odds or market price through supply and demand for the shares. The value of these prediction markets is based on the statistical phenomenon "Wisdom of the Crowd", where on average a crowd of people can collectively more accurately estimate the probability of an outcome than any individual.[86] Prediction markets have a long history from politics to corporate strategy and gambling. Due to gambling laws, prediction markets played with real money are illegal in the US, with some exceptions operated under certain restrictions. An additional moral and legal issue with these markets is their creation of incentives to harm others for financial gain. Nevertheless, the benefits are compelling and, in some cases, there may be no likely downside.

An innovative use case is Liquidity Health, which helps to predict the spread of epidemic diseases.[87] Augur is also a decentralised prediction market protocol and runs on the Ethereum blockchain as a set of smart contracts.[88] It is currently most popular for predicting the future prices of cryptocurrency in USD or the successful outcome of ICO funded projects. Using a reward incentive could attract data scientists to enhance prediction models. While the current applications are niche, they are gradually proving the scope, accuracy and profitability of a decentralised prediction market.

6.4.3 Online Gambling

Gambling has been a very popular activity within cryptocurrencies, almost since their inception. The SatoshiDice start-up was a bitcoin lottery game from 2012, sold in 2013 for 11.5 million USD.[89] The game was notable for its 'provably fair' mechanism where all players can see the actual pot at stake, how much of it goes to the house,

[85] See https://www.mydayta.io for an example of project championing this paradigm.
[86] For more information on Wisdom of the Crowd, see: https://www.investopedia.com/terms/w/wisdom-crowds.asp.
[87] For more information on Liquidity Health, see: https://twitter.com/liquidityhealth.
[88] For more information on Augur, see: https://www.augur.net/.
[89] For more information on SatoshiDice, see: https://en.wikipedia.org/wiki/SatoshiDice.

and also that the winner-selection algorithm is not biased or corruptible. More recently, Ethereum has enabled a more ambitious gambling protocol, FunFair, which has similar 'provably fair' mechanism to SatoshiDice using a pseudo random number generator but supporting an increasing number of different games such as blackjack and virtual slot machines.[90]

6.4.4 Labour Marketplaces

Researchers in the DLT industry are investigating novel ways of organising work: universal basic income, helping businesses find talent and build teams, rewarding people in unusual ways, and reinventing management processes. Among others, Aragon, The DAO (a decentralised autonomous organisation), Colony and Dash have demonstrated unique approaches.

Colony was started in 2014 with the aim of enabling organisations in which decisions are taken openly and transparently.[91] Colony sees itself as the infrastructure of collective work whether that is through a non-profit organisation or company.

Dash is a successful fork of the Bitcoin codebase, designed to facilitate a decentralised middle tier service platform distinct from the miners, run by entities called masternodes.[92] One can see Dash as a decentralised labour and governance marketplace for a cryptocurrency. Dash miners get 45% of block rewards and 45% goes to the masternodes. One of the main services offered by masternodes is 'InstantSend' which is a method of fast-tracking payment confirmation. The remaining 10% of the miner reward goes to the decentralised Dash development budget which is allocated through democratic voting by the masternodes.

Aragon is a decentralised system for voting, governance, administration and identity.[93] The team behind Aragon envision three waves of users: first, blockchain projects looking for a governance solution; second, open source projects, which want to pay volunteer developers using tokens; and third, distributed companies willing to pay their developers in tokens.

[90] For more information on FunFair, see: https://funfair.io/.
[91] For more information on Colony, see: https://colony.io/
[92] For more information on Dash, see: https://www.dash.org/.
[93] For more information on Aragon, see: https://aragon.one/.

Aaro Capital

Authors:

Oscar Pacey
oscar@tranquilitynode.com

Peter Habermacher
peter.habermacher@aaro.capital

Contact Information:

Peter Habermacher
peter.habermacher@aaro.capital

Ankush Jain
ankush.jain@aaro.capital

Sebastien Jardon
sebastien.jardon@aaro.capital

aaro.capital