SWIFT INSTITUTE

BRIEFING PAPER

DEFINING DIGITAL ASSETS

ALISTAIR MILNE

School of Business and Economics, Loughborough University

PUBLICATION DATE: APRIL 2022

Executive summary

This briefing paper examines digital assets. Examples include cryptocurrencies, stablecoins, central bank digital currencies (CBDC) and the possibility of bonds and equities held directly and exchanged through shared ledgers. It reviews the main developments and discusses what is really new about digital assets.

This discussion highlights the following points:

- The key drivers of the recent emergence of digital assets are as much social and economic as technological. The supporting technologies have been around for many years, some can be traced back more than four decades. These drivers include the 'cypherpunk' philosophy of extreme distrust of all institutions, both government and private; enthusiasm for trading new, lightly regulated crypto assets; techno-enthusiasm for new technologies and also the opportunity to address gaps in mainstream financial services provision.

- A defining feature of digital assets is that – unlike commercial bank money or securities accounts held with custodian banks – they are directly held, rather than indirectly held on the balance sheets of financial intermediaries. This means there is no need for settlement in completing the transfer or exchange of a digital asset. This is also a feature of e-monies, where transfers are 'closed loop', i.e. simply a movement from one account to another provided by the same e-money provider. Digital assets proper are based on shared cryptographically secured ledgers (also known as distributed ledgers or blockchains) with access provided by several competing intermediaries. This similarly allows closed loop transfer without settlement.

- A central distinction is between 'permissionless' and 'permissioned' digital assets. Permissionless digital assets are the 'crypto assets' held and exchanged using purely software-based architectures in line with the cypherpunk vision of fully disintermediated financial exchange. Anyone with internet access can acquire, hold and transfer them. Other digital assets, developed by regulated mainstream institutions, are permissioned in order to support, for example, confirmations of identity required by KYC regulation.

- Regulatory compliance currently limits the ability of mainstream regulated intermediaries to engage with these largely unregulated investment opportunities. How this plays out is still unclear because of uncertainty about the 'regulatory perimeter' i.e. the extent to which institutions offering transactions in permissionless crypto assets will be regulated and the requirements on regulated institutions when engaging with permissionless crypto assets. Still, it is likely that the majority of transactions in digital assets will be conducted through regulated financial intermediaries, with unregulated permissionless exchange a fringe of activity outside of the regulatory perimeter.

- The most advanced developments in permissioned regulated digital assets are various new forms of digital money. These include: e-monies; wholesale distributed ledger money supporting liquidity management by financial institutions; initial experiments with retail digital ledger money; and rapidly increasing interest of central banks in issue of central bank digital currencies with some already launched and more expected to follow. Alongside these monetary digital asset developments have been various experiments with using digital assets and their supporting distributed ledger technologies to improve operations in financial markets and financial services.

- The rise of digital assets poses challenging questions for the business models of regulated intermediaries in banking, capital markets and asset management. This is most obvious for commercial banks if a shift to holding digital asset money forces them to replace funding from core retail deposits with borrowing from money and bond markets. Similarly, a shift in capital markets to transfer of ownership of securities and foreign exchange held on distributed ledgers with trade execution followed by an immediate 'closed loop' transfer of ownership without need for subsequent settlement, challenges existing capital market business models based on delayed settlement and netting of offsetting trades. A broader challenge for all financial intermediaries is financing the investments in new systems and interfaces required to meet customer demand for holding digital assets and to benefit fully from the application of digital ledger technologies in their financial operations.

.

Introduction

This briefing paper tells the story of digital assets: where they came from, what they are now and what they may become in the future. This is a social and a human story. Digital assets are underpinned by the powerful tools of modern public key cryptography. It is not though this technology that makes digital assets so interesting. They are indeed technology-based, but what really matters about the new digital assets is their impact, now and in the future, on social, financial, business and economic relationships.

A further goal of this paper is to distinguish the main forms of digital assets. Since the appearance of cryptocurrencies, the first digital assets, there have been many subsequent innovations. These fall into three broad categories:

I. decentralised finance and crypto asset trading with minimal involvement of financial intermediaries and currently relatively little regulation
II. the emergence of new forms of digital money
III. the use of distributed ledger technologies to improve operations across financial services

An underlying question is also addressed here: what is actually new about digital assets? Financial assets have been held in digital form for many years, so to some degree the new digital assets are simply the presentation of 'old wine in new bottles'. Yet there is something genuinely novel: a shift from holding assets indirectly through financial intermediaries to direct holding on shared distributed ledgers. This can be expected to have a growing influence on mainstream finance in the years ahead.

The key points are summarised in the Executive Summary. The main body of the paper consists of four sections:

- Section 1 examines the emergence of cryptocurrencies, the first digital assets
- Section 2 considers what distinguishes digital from conventional financial assets
- Section 3 provides an overview of the principal digital asset developments
- Section 4 assesses implications for business models and regulation

A brief conclusion is followed by four annexes (Annex 1 – Annex 4) each providing further detail and discussion of material in the correspondingly numbered main section.

1. The first emergence of digital assets

The emergence of the first digital assets was as much a social as a technological movement. This social dimension is represented by the 'cypherpunk' movement. This was a loose coalition of computer scientists and coders – connected through an online mailing list – who debated politics and developed new encryption tools for defending personal privacy from government and corporate encroachment. Active participants included Eric Hughes, author of *A Cypherpunk's Manifesto,* and Julian Assange, founder of Wikileaks.

From the 1980s onward, very much in the spirit of the cypherpunks, computer scientists used the newly available tools of public key cryptography to develop a number of instruments (Digicash, Bit Gold and others) for direct online financial exchange. These were the virtual

equivalent of banknotes or coins, transferred directly from one holder to another. Underlying these architectures was an extreme concern – amounting almost to paranoia – about security. Governments and commercial institutions such as banks cannot be trusted to act honestly and reliably. Therefore, the design and operation of these new online forms of money had to be entirely software based. Moreover, this software should make it impossible for any malign actor or actors to manipulate the record of transactions to their own benefit.

Bitcoin was a breakthrough because it was the first internet money to fully achieve this goal – albeit at the cost of massive expenditure of energy on the consensus mechanism that ensures that no participants can manipulate the system. This consensus mechanism is the so called 'proof of work' or 'mining' that underpins Bitcoin and other cryptocurrency transactions (see Annex 1).

Proof of work is complicated as well as expensive. Fortunately, engaging with the new digital assets does not require understanding proof of work. This is for two reasons:

(i) As technology advances validation through proof of work will, over time, be supplanted – in the cypherpunk world of decentralised finance with no intermediaries – by other less expensive consensus mechanisms. The likely replacement is 'proof of stake', effectively a voting system based on shares of ownership in the digital asset.

(ii) There is an even stronger reason for not worrying about the details of proof of work. The cypherpunk world of decentralised finance with no intermediaries is not the mainstream future. The mainstream future of digital assets will be one in which institutions continue to play a central role. In this context validation can be carried out by a group of trusted intermediaries. Neither proof of work nor proof of stake are needed.

Alongside this mainstream adoption of digital assets, there will be a continuing fringe of direct exchange of crypto assets without intermediaries. There will also be mainstream investment in these directly exchanged decentralised crypto assets. This mainstream investment will though be closely regulated, to prevent its use for evasion of law and regulation, in turn requiring mainstream investors to rely on regulated institutional providers.

In short, for most users and investors, assurance about the validity of transactions in digital assets will ultimately be provided in the same way as for conventional financial assets, through trust in regulated institutional providers, their systems, and their employees.

2. What is new about digital assets?

Cryptocurrencies were the first digital assets. A wide range of subsequent further developments has followed, summarised in the following Section 3. Before looking at these subsequent developments, it is though helpful to address a prior question: what is really new about digital assets? The answer is that digital assets, unlike conventional financial assets, are directly rather than indirectly held.

To understand this distinction, contrast the examples of a bank account and a banknote:

- A bank account is an example of indirectly held money. It is a liability of a private institution, with legal obligations both to return money to the holder on demand and to transfer money to settle payments, when a payment is made from a customer's account to an account held with another institution.
- A central bank issued bank note, e.g. a $50 bill, is an example of directly held money. While intermediaries may be involved in transfers, for example a security company transporting banknotes from one location to another, the money itself is not the liability of any private institution.

Historically, the majority of money and financial assets were held directly and transferred as physical objects, for example: precious metal, coins, bank notes or security certificates (the latter for 'bearer securities' whose legal ownership was based on physical possession of the certificate).

In the course of the past century and a half there has a been a broad shift from direct to indirect holding, both of money – from banknotes and coin to commercial bank deposits – and of securities – from security certificates to security accounts held with custodian banks.

Now, with new powerful tools of public key cryptography, something new has emerged, the possibility of direct virtual holding of ownership claims on a shared cryptographically secured ledger. This is what digital assets are:

DEFINITION: Digital assets are virtual records of value directly held on and transferred across a shared cryptographically secured ledger.

These 'shared cryptographically secured ledgers' are what is often referred to as blockchains or distributed ledgers. These terms are more widely used than they are understood. It is helpful therefore to spell out their key features:

1. the ledger is not controlled by a single operator, rather several operators share responsibilities for validating ledger transactions
2. the ledger provides a permanent or 'immutable' record of transactions and asset holdings.
3. public-key cryptography underpins the execution of transactions on the ledger, ensuring that only owners can instruct transfers of their assets.

A shift to holding digital assets directly on distributed ledgers, instead of indirectly as liabilities of institutions such as commercial or custodian banks, changes the process of ownership transfer. A digital asset, unlike an indirectly held financial asset, is no longer fully controlled by a single intermediary. Transfers are instead first initiated through the automated verification of an asset owner's 'digital signature' and then accepted by the ledger operators.

This shift to direct holding of digital assets with transactions validated using digital signatures is a material change in the role of intermediaries. As Section 4 discusses, this has a significant impact on business models.

Although a fundamental change for financial intermediaries, in the day-to-day management of their finances and investments, holders need not necessarily see any difference between holding digital assets directly and conventional financial assets indirectly. Customer interfaces – whether online web access, mobile apps or through agents at telephone call centres -- can be much the same as the existing digital channels customers already use for accessing and transferring deposit money or in managing conventional investment portfolios.

There are though some impacts for customers from a direct holding of digital assets. These impacts depend on the form of digital asset they are acquiring:

1. For permissionless cryptoassets – cryptocurrencies and also 'stablecoins' – that have emerged directly from the cypherpunk vision of exchange of assets without intermediaries or regulation, customers are likely to hold them through a new intermediary specialising in crypto investments. Commercial banks, custodian banks and e-money providers have been looking closely at providing their customers with direct holding of cryptoassets, but regulatory approval is needed and to date only a few established mainstream institutions have been able to do this.
2. For other forms of digital assets, those being developed through co-operation between mainstream regulated institutions, regulatory approval is built in from the outset. As a result, access to these digital assets can be more easily provided by existing commercial banks, custodian banks or e-money providers. But these digital assets are still immature, at a relatively early stage in their development, and so they do not yet fully substitute for existing conventional indirectly held assets.

As an example, consider a central bank digital currency (CBDC) held by a retail customer with access provided by a commercial bank (a likely outcome for many forms of retail CBDC). Unlike a bank deposit, in excess of deposit insurance limits, there is no risk of loss of CBDC from the default of the provider. The functionality of CBDC may though be more limited than that of existing commercial bank accounts. It will be easy to transfer CBDC from one CBDC holder to another. But without substantial further investment to support interoperability with existing payment schemes, it will be difficult to provide all the familiar payment services such as batch payment processing of salaries and invoices, direct debits, card payments and direct credit transfers both to and from conventional bank deposit accounts.

3. Digital assets compared

This section compares the principal developments in digital assets, summarised in Table 1. Here the focus is on broad comparison (with fuller discussion in Annex 3). The columns, reading from the right, distinguish key features underpinning different digital assets:

- Technological design. The choices about who has access to and control of the shared ledger in which holdings of digital assets are recorded.
- Social and behavioural drivers. Digital assets are fundamentally social innovations.
- Economic value. What digital assets offer to holders that is not available from holding conventional financial assets.

Table 1: the main developments in digital assets

	Development	*Examples*	*Economic value*	*Social and behavioural drivers*	*Technological design*
DeFi (decentralised finance) and crypto	Cryptocurrencies	Bitcoin	Use in private transactions; avoiding currency controls	Cypherpunk philosophy, trading culture.	Permissionless DL
	Stablecoins	Tether, USD coin, Binance USD, DAI, PAX and others.	Facilitating crypto trading; decentralised finance without intermediaries	Cypherpunk philosophy, trading culture	Permissionless DL
	Programmable blockchain and DeFi	Ethereum	Decentralised finance without intermediaries	Cypherpunk philosophy, trading culture, techno-enthusiasm	Permissionless DL
New forms of regulated digital money	Wholesale DL money	Fnality Utility Settlement Coin	Improved liquidity management	Meeting user needs, techno-enthusiasm	Permissioned DL
	e-money	Paypal accounts, MPesa, Alipay, WeChat Pay	Addressing gaps in services	Meeting user needs	Conventional centralised databases
	Guaranteed retail DL money	Diem might have adopted this design.	Addressing gaps in services	Meeting user needs, techno-enthusiasm	Permissioned DL
	CBDC, wholesale and/or retail	e-CNY, Bahamian Sand Dollar, Digital Euro	Financial inclusion; competition in payments services	Policy goals, techno-enthusiasm	Permissioned DL Conventional centralised databases
Operations in financial markets and services	Programmable DL	Quorum, Hyperledger	Addressing gaps in services; supporting automation.	Meeting user needs, techno-enthusiasm	Permissioned DL
	DL issued securities; Fractionalised security holdings	World Bank bond-i Thai government savings bonds, BondEValue, SIX digital exchange	Facilitating direct retail bond and equity investment	Meeting user needs, techno-enthusiasm	Permissioned DL
	Automation of financial transactions	ISDA automated interest rate derivative clearing	Lowering operational costs and risks	Meeting user needs	Permissioned DL Conventional centralised databases

Notes: DL = Distributed ledgers (aka blockchains), cryptographically secured shared ledgers with many operators, contrasted with single-operator conventional centralised databases. DLT = supporting distributed ledger technologies. The double lines distinguish three main groups of developments.

The three panels in Table 1, reading from the top, distinguish three categories of digital assets:

- The largely unregulated trading in cryptoassets and DeFi (decentralised finance).
- New forms of regulated digital money.
- Applications of digital ledgers (DL) in financial operations.

There are two main choices for the technological design: (i) between a permissionless and permissioned ledger; and, for a permissioned ledger, (ii) between a shared cryptographically secured ledger i.e. a distributed ledger or a conventional database with a single operator.

The digital assets in the top panel of Table 1, those held and exchanged using purely software-based architectures and hence coming closest to the cypherpunk vision, are all permissionless. Anyone with internet access can acquire, hold and transfer them. The digital assets in the remaining two panels of Table 1 are all permissioned. These have been developed by mainstream institutions with regulatory compliance in mind. These must be permissioned to support, for example, confirmations of identity required by KYC regulation.

Permissioned assets developed by mainstream institutions face a second technology choice:– using a permissioned shared digital ledger or a conventional database. For example e-monies use conventional institutionally controlled databases. Strictly, according to the definition of Section 3, these are not digital assets. There are though many common features with digital assets proper, justifying their inclusion in the table.

A similar point applies to CBDC. Early discussions of CBDC design by the major central banks indicates that some central banks are considering issuing CBDC on a conventional centralised database with a single operator, not on a distributed ledger with many operators. This choice will depend on considerations of cost and security. For holders of CBDC or intermediaries providing CBDC services, it does not much matter if the ledger entries are validated by a single operator or by many. Some applications of digital asset technologies in financial operations, the third panel of Table 1, can also use conventional databases.

The social and behavioural drivers of digital assets vary substantially from one digital asset to another and over time. Cryptocurrencies are a good example of change over time, with the cypherpunk philosophy now largely replaced by a trading culture and speculation.

Another social driver is 'techno enthusiasm': faith in the impressive capabilities of the underlying distributed ledger technologies and expectation that they will eventually supplant conventional arrangements. This is the motivation for many experiments with digital assets, demonstrating some of the possibilities from holding financial assets on shared ledgers, conducted by banks and central banks to ensure they are abreast of the technology.

Table 1 refers to two other drivers of digital assets. One is meeting hitherto unmet user needs. Examples, labelled here as wholesale DL money. An example is Fnality Utility Settlement Coin. These provide financial institutions with a form of money that gets around constraints on holding and transferring central bank money, such as the limited opening hours for RTGS large value payments. Another driver, in the case of CBDC, are achieving policy goals including financial inclusion and competition in payments services.

Reading down the rows of Table 1 highlights four principal digital asset developments.

i. *Cryptocurrency wallets and crypto exchanges*

Interest in cryptocurrencies has spread far beyond their original cypherpunk origins and their use in private transactions to avoid regulatory scrutiny and currency controls. Increasingly, investment in cryptocurrencies is speculative, with perceived profitable short-term trading opportunities and long-term benefits, both protection against inflation and potentially substantial capital gains, compensating for the substantial short-term price volatility.

ii. *Stablecoins and decentralised finance (DeFi),*

Stablecoins, like cryptocurrencies, are permissionless traded assets traded on crypto exchanges. Unlike cryptocurrencies, market transactions are used to maintain their market value close to par against an underlying fiat currency, most often the US dollar. These market transactions can be undertaken by an institution holding reserve assets or can be purely software based. Stablecoins allow investors to rapidly take or extinguish cryptocurrency exposures. The most widely used stablecoin is Tether, but there are ongoing concerns about the opaqueness of Tether and the quantity and quality of its reserve assets.

Decentralised finance or DeFi is the rapidly growing exchange of cryptoasset exposures without any intermediaries, most actively pursued on the Ethereum blockchain. There are now a remarkably wide range of DeFi software solutions, mimicking the opportunities for leverage and exchange of risk provided by derivatives in mainstream markets.

Further support for trading of cryptocurrencies and stablecoins, and for DeFi, is coming from the increasing interest of mainstream financial institutions in crypto investments: "crypto as a new asset class". This is though not straightforward, both because of the absence of any consensus on the fundamental value of cryptocurrencies, which should determine pricing over the long-term, and the practical difficulties for regulated institutions in engaging with largely unregulated crypto wallets and crypto exchanges,

iii. *Regulated digital money and e-monies*

For mainstream institutions, it is easier to engage with other new forms of regulated digital money, those in the second panel of Table 1, developed from the outset to comply with financial regulations. These include the wholesale digital ledger money (described above) and also the various regulated non-bank e-monies. Regulation gives holders much stronger assurance than for stablecoins about the quality of the assets backing them. This in turn makes it easier to use them for day-to-day purchases and monetary transfers (though they are still different from bank money because these purchases and transactions are 'closed loop' taking place immediately on a single balance sheet without need for subsequent settlement).

The need to comply with regulation has meant that, unlike the stablecoins, these regulated forms of digital money cannot as yet be used for trading on crypto exchanges.

This distinction between stable coins and new forms of regulated digital money may well erode over time. One stablecoin, Paxos (or PAX), has focused on achieving regulatory approval allowing it to be used both for crypto trading and for day-to-day purchases and transactions.

It has been selected by Facebook as the currency of choice for an early proof of concept in international transactions for its Novi wallet. Some e-money providers – an example is Paypal – allow their customers to buy and sell cryptocurrencies.

The rapid developments in stablecoins and regulated digital money have prompted central banks, concerned amongst other things with potential loss of monetary sovereignty, to actively explore the issue of central bank digital currencies (CBDC). CBDC is new regulated digital money exchanging on the central bank balance sheet. Early examples include the e-CYN in China, the Bahamian Sand Dollar and the launch of a digital Naira in Nigeria.

iv. *Growing use of digital ledger technologies in financial operations.*

A further digital asset development has been the growing application of distributed ledger technologies to improve operations in mainstream financial services. These varied developments are not discussed in detail in this paper. Table 1 gives examples of some of the most prominent initiatives. A possibility attracting particular attention is the issue of bonds or other securities on distributed ledgers, sometimes called 'tokenisation'.

4. Intermediary business models and the regulatory perimeter.

This section completes the paper with a brief look at the challenges posed by digital assets for intermediary business models and the role of regulation. The widespread adoption of digital assets in mainstream finance offers substantial benefits, including greater cross industry standardisation of financial operations, enhanced security based on public key cryptography and avoiding the need for subsequent settlement when transferring ownership of digital money or securities. While these benefits are substantial there are also significant adoption costs. Internal systems will have to be adapted to deal with digital assets, including where required guaranteed secure management of a customer's private keys.

Digital assets pose further fundamental challenges to existing business models. This is most obvious for commercial banks. Consider a customer shift from indirect holding of money in commercial bank deposits to direct holding of digital money on distributed ledgers, e-monies or CBDC. Commercial banks will still provide customers with access to these new forms of money, either themselves or through commercial partners, but this will be fee-based servicing of digital assets held on shared distributed ledgers rather than offering fractionally reserved deposit liabilities on their own balance sheet. This in turn means that commercial banks will have to replace funding from core retail deposits with borrowing from money and bond markets. Shifting to real time settlement would be a major change to the business models used in foreign exchange and securities markets, where much of the liquidity for trading is currently based on delayed settlement and the resulting opportunity to net offsetting transactions and hence economising on capital and funding.

The emergence of digital assets also poses major challenges for regulators. Their biggest challenge is regulation of the permissionless distributed ledgers that support decentralised finance and the trading of crypto assets. Their cypherpunk origins mean that this exchange takes place virtually, outside of established legal and regulatory jurisdictions, with no identified individuals nor institutions to regulate.

This in turn creates regulatory uncertainty – how will financial regulation evolve to meet the challenges of digital assets? There are several controversies: some of the major players in crypto asset trading, for example the exchange Binance and the stablecoin provider Tether Ltd., are coming under intense regulatory scrutiny. There are also considerable differences in the attitudes of regulators – some want to encourage innovations in crypto and digital asset trading and are imposing a light touch regime on digital asset innovation; others are much more cautious and concerned to limit these activities in order to protect customers and limit prudential risks. There is also uncertainty about the legal powers of regulators to intervene in new products and services that currently fall outside of the existing regulatory perimeter. Consistency of regulation of digital assets is still a long way off.

Conclusion

This paper describes the emergence of digital assets, distinguishing three broad categories: (i) decentralised finance and crypto asset trading; (ii) new forms of digital money; and (ii) the use of digital ledger technologies to improve operations across financial services. It offers a definition of digital assets – assets directly held on a shared cryptographically-secured ledgers – reviews the main developments in digital assets and comments on the challenges they pose for intermediary business models and regulation.

Six main points emerge from this analysis, as set out in the Executive Summary.

One further concluding reflection is relevant. In one important respect digital assets are little different from conventional mainstream financial assets. Most holders will rely on regulated intermediaries for managing their ownership and exchange. This in turn means that the full commercial exploitation of the opportunities from digital assets will require several further developments: (i) industry wide adoption of shared cryptographically secured ledgers for recording and transferring digital assets holdings; (ii) the evolution of business models to support direct rather than indirect asset holdings; and (iii) a consistent approach, across institutions and jurisdictions, to the regulation of new digital asset services. These developments will not happen overnight. As a result, digital assets are still relatively immature. It will be some years yet, before their full impact on financial markets and services is clear.

Annex 1: The emergence of Digital Assets

For many, the first thing that comes to mind with the mention of digital assets are the substantial prices rises and volatility of cryptocurrencies such as Bitcoin and Ethereum. Stories of fortunes being made and lost, and "FOMO" (fear of missing out") understandably dominate the social and traditional media coverage of digital assets.

These dramas though are just the surface (some might say the froth) of fundamental financial innovation. The dramatic price increases of Bitcoin and other cryptoassets may well prove to be a bubble. Whether it is a passing fad or has a permanent place in the menu of financial assets is not so important. What is important is that aspects of the new distributed ledger technologies for holding and transferring digital assets are finding increasing application across money, banking and capital markets. Even if interest in Bitcoin disappears, and cryptofortunes evaporate, the technologies supporting Bitcoin are transforming, and will continue to transform, the way we hold financial assets and execute financial transactions.

A helpful way to understand these new assets is to dig a little bit into their history: how did we get here? It is commonplace to link the birth of digital assets to the 2008 publication of the pseudonymous white paper *Bitcoin: A Peer-to-Peer Electronic Cash System* by 'Satoshi Nakamoto' (not as far as we know a real person, but a pseudonym adopted by a computer scientist or group of computer scientists) and the subsequent 2009 release of the open-source Bitcoin software.

Impressive as this innovation was, it was simply an incremental step, building on several earlier innovations that can be traced back a further thirty years, to the military research of the 1960s and 1970s that also underpinned the development of the internet.

A major milestone in the emergence of digital assets, as these new technologies found application beyond their original military origins, was the 1977 publication of RSA (the acronym refers to the surnames of its three creators Ron Rivest, Adi Shamir and Leonard Adleman). This was the first published algorithm for public-key encryption. Public-key encryption is the foundation of internet security as well as of the new digital assets.

The basics of public-key encryption are simple. The public key is a very large number that can be used to encrypt a message or file. There is a corresponding private key, another very large number, which is required for decryption. RSA was the first publicly available algorithm for creation of pairs of public and private keys. The recipient first creates a public-private key pair. They then make the public key public, e.g. through a link on a webpage. The sender of a message or file can then securely encrypt using this public key. The outcome is that only the recipient can decrypt and read the message and file (provided have kept the private key secure). The publication of RSA and then of other related encryption algorithms of was the starting gun for the three decades of computer science research that has led us to cryptocurrencies and digital assets.

Bitcoin mining. The proof of work used in Bitcoin is known as mining. Network participants search for an unusual number that mathematically matches the most recently published transactions and links them to previous transactions. The software makes these numbers so

rare that this search requires burning large quantities of electricity i.e. work. Finding such a number confirms the addition of a new block to the Bitcoin blockchain. Successful mining is remunerated by transaction fees and the award of new Bitcoin.

How does this proof of work protect the system? To create a false, alternative transaction history based on hidden unpublished transactions, malign network participants would have to use even more electricity than the miners engaged in the legitimate proof of work search. Moreover, even if they succeeded occasionally in attaching false transactions to the Bitcoin transaction history, final confirmation requires them to do this several times in succession, so the best they can do is create one of two competing versions of history.

The legitimate miners then have a further iron-clad defence. The software resolves any discrepancy between two competing versions of transaction history through automated voting based on past legitimate mining activity. So, to break the system, the malign actors have to recruit a majority of the miners making profit out of Bitcoin to help them. In the language of economic theory, this is not "incentive compatible", because miners will not want to destroy their own source of revenues.

Annex 2: What is new about Digital Assets?

Over the centuries there has been a shifting balance between the two forms of asset holding, direct and indirect, depending on the available technology of the time. Both are found in the very earliest historical developments of money and finance, in fourth millennium BC Uruk and the other cities of ancient Mesopotamia. One of the earliest known forms of money were accounts denominated in grain held with the palace temples (an indirect holding). Another was uncoined silver (a direct holding).

Moving swiftly through five millennia of history, by the second half of the twentieth century, with the rise of computerised processing, the balance swung substantially towards indirect holding of money and other financial assets. Nowadays the large majority of both companies and household money is held with commercial banks. Similarly, since the 'paper work crisis' of the 1960s that marked the death knell of bearer securities and the subsequent dematerialisation of securities in the 1970s and 1980s, investors hold publicly traded securities such as bonds and equities indirectly through custodian banks.

The principal difference for the holder is that moving their assets from one provider to another provider is more straightforward for directly held digital assets than for indirectly held conventional financial assets. Their asset holding recorded on the distributed ledger is unchanged. Moving their directly held digital assets to a new provider means only a change in the institution responsible for managing their private keys and providing supporting account services (an issue, for which technical solutions are not yet fully developed, is the secure transfer of these keys along with historical accounting information from the old to the new account provider).

Securities could, historically, also be directly held assets in the form of bearer bond certificates. Nowadays securities are always held indirectly in accounts with custodian banks. Custodians are then in turn obliged to transfer the holding as requested by the owner for delivery against payment in settlement of security transactions.

Underpinning the direct holding of digital assets are the use of digital signatures to ensure that only asset owners can instruct asset transfers. A digital signature is a form of reverse encryption. A public key for decryption is unambiguously linked to every individual asset holding. An instruction to transfer some or all of this asset holding consists of two copies of the transfer instructions: one the original, the other encrypted using the corresponding private key. Using the public key to decrypt the encrypted message and confirming that it is the same as the original message, in turn demonstrates that the instruction has a valid digital signature. Only then does the software of the shared ledger execute the transfer.

Crypto assets like cryptocurrencies can, if the holder prefers, be exchanged directly without any intermediaries and entirely outside the framework of law and regulation (because they are held on permissionless ledgers with no real world identities or restrictions on who can buy, sell or hold). Exchange of crypto assets in this way is likely to have some enduring appeal: to devoted cypherpunks, to computer nerds, to criminals and terrorists, and also to those who wish to avoid currency controls and other state restrictions on economic exchange.

While transfers of permissionless digital assets on distributed ledgers do not necessarily require an intermediary, individuals will not typically maintain digital asset software on their own computers themselves, rather they will rely on investment institutions for their key management on their behalf and to ensure compliance with law and regulation, just as they do with conventional financial assets.

An illustration of this last point is the emergence of 'cryptocurrency wallets' as an additional wrapper to support the 'institution free' holdings of cryptocurrencies. As holding of cryptocurrencies has become more widespread, most holders do not want to manage the private keys of their cryptocurrency holdings themselves. They instead want support in doing this. There are technology based solutions that provide this service without relying on a financial intermediary – so called soft and hard wallets which support cryptocurrency key management (hard wallets are regarded as the most secure, because the keys are stored on media unconnected to the internet; soft wallets in the form of download software onto computers or mobile phones create a risk of hacking). Users could use soft or hard wallets to manage their own key software and hardware and avoid any reliance on intermediaries. In practice though the vast majority of holders of cryptocurrencies turn to an intermediary to manage their cryptocurrency keys on their behalf, either by providing soft wallet services in the form of local applications or directly holding keys on their behalf.

Institutional investors are in a similar position. They will need to use established digital asset intermediaries in order to demonstrate to their clients that they have done everything they can to ensure the safety of assets they hold for others. They are used to outsourcing the operational support for holding financial assets to custodian banks or in the case of hedge funds to prime brokers. So as crypto and other digital assets grow out of their early cypherpunk origins we can expect them to be overwhelmingly held through intermediaries.

Annex 3: Further discussion of the Table 1 comparison of digital assets

The jury remains out on the long-term importance of the various developments in digital assets. There are both enthusiasts and sceptics about these various opportunities from shared arrangements for holding and transfer based on the tools of cryptographic security. While it seems safe to assume that mainstream finance will increasingly use cryptographically secured shared databases for the simplification and automation of operations in both conventional and digital assets, the extent to which digital assets, held on shared ledgers, supplant conventional assets remains unclear.

Crypto assets and decentralised finance (DeFi)

The first category of digital assets, presented as the top panel of Table 1, are based on permissionless distributed ledgers. These were developed in line with the cypherpunk philosophy, avoiding any role for government of private sector intermediaries. Because of their origins, these are furthest removed from conventional financial assets with some features that have no parallel in mainstream finance, and transaction arrangements that continue to evolve rapidly. Still, to fully understand digital assets, it is worth some effort to understand this category of digital asset developments.

Developments in decentralised finance and trading of crypto assets have been fuelled in the past two years by the increasing interest of mainstream investors in crypto as a new investment asset class. This interest drove the most recent bull run in cryptocurrency prices in the second half of 2020, with the price of Bitcoin doubling in late 2020 to surpass its previous 2017 peak of 19,000 and rising further to around $61,000 in March 2021. Prices though have continued to be highly volatile, falling in July 2021 to below $35,000, climbing above $64,000 in Nov 2021, and then subsequently falling again in Dec 2021.

Alongside the increased interest in crypto investment has been a rapid growth of holdings of stablecoins, cryptographic money held and exchanged on unpermissioned shared ledgers, in the same way as cryptocurrencies, but designed to maintain a stable value against the $US. These stablecoins are used as the reference assets for trading on crypto exchanges (much as the $US itself is the reference asset for conventional foreign exchange market trading, currencies trading against the dollar much more than they are traded against each other). The two largest in terms of value of holdings, illustrating some of the variety of different stablecoin arrangements, are Tether and Dai.

A key feature of the stablecoins used in cryptotrading is that their values are *not* guaranteed, rather they are market determined with either an operator or software buying and selling the stablecoin against other crypto assets to maintain the value close to par (and acquiring or disposing of collateral to maintain underlying support for the value of the stablecoin). As a result, values can and do fluctuate somewhat from the stated par of 1 unit = 1 $US. The most widely used stablecoins such as Tether and DAI maintain values close to par. The price of Tether has remained within about 0.5% of par since late 2019, but did fluctuate more in earlier years. Other less actively traded stablecoins exhibit more substantial price fluctuations.

Tether, the stablecoin most widely used for crypto-trading on exchanges such as Binance, somewhat contrary to the cypherpunk philosophy, is institutionally operated by Tether

Limited which is in turn controlled by the owners of the Hong Kong based crypto exchange BitFinex. Tether Limited state that Tether is fully collateralised by underlying dollar deposits and loans (though there are continuing investor and regulator concerns about the quality of this collateral). Tether Limited redeem and issue Tether to stabilise its $US value. Two other major stablecoins, Pax dollar and USD coin issued by Circle, are similar, with a central operator and backed by a mix of commercial bank money and US Treasury bills. DAI, unlike these other stablecoins, has a more decentralised structure and is not 100% collateralised 1:1 by holdings of fiat currency. Instead it is 150% collateralised by DeFi loan contracts, in turn collateralised by holdings of cryptocurrency, with automated software that alters the interest on loan contracts to attract required collateral.

There is active round the clock trading of cryptocurrencies, and also of stablecoins on many virtual crypto exchanges, such as Binance and Coinbase. Because cryptocurrency and managed stablecoin ledgers are permissionless the servers supporting these exchanges can be established anywhere and accessed by holders of these digital assets from all around the world (Binance is well known for its claim to have no legal jurisdiction). While the details of operation vary, typically users first transfer their holdings of cryptocurrencies or stablecoins on to the exchange, from where they can directly execute trading transactions against prices offered by other exchange participants.

A related development is DeFi (short for 'decentralised finance'). This is the emergence of trading of a wide range of new crypto based financial contracts, relying on the programmability of the Ethereum or other cryptocurrency blockchains which allows automated transactions to be built into financial contracts. An example of this automation: DeFi loans are all collateralised and the software automatically terminates the loan and sells the collateral if the collateral value falls below a trigger percentage of the loan amount. Like the transactions in the underlying cryptocurrencies on which it rests, DeFi is purely software based with no institutional involvement. It provides the crypto equivalent of repo lending and borrowing, swaps, futures and options; all accompanied by its own new strange language (yield farming, oracles, perpetual swaps… to name just three).

The views of the industry on this new crypto trading remain very divided. They offer new and attractive opportunities for those with good trading skills. Some hedge funds are taking large positions. A number of payments providers – Paypal, Revolut and others – are giving their customers the opportunity to hold cryptocurrency balances and initiate payments that draw on these balances. Others, understandably, are cautious. The possibility of a market collapse cannot be ruled out. There is much internal debate within major banks about the extent and nature of their involvement in crypto, in no small part because of the associated regulatory risks. At the same time, it is difficult for institutions to avoid involvement altogether because there is client demand to hold crypto assets and a shareholder pressure to not miss out on the opportunities for earnings based on meeting this client demand.

The following comparison puts all this crypto trading activity into perspective. The global market value of the world's equity and debt markets is approximately $250trn. The market value of cryptocurrencies and the stablecoins traded on the various crypto exchanges was $2.5trn (as of end October, 2021; source Coinmarket cap) together with a further $0.14 trn

market value of stablecoins. Taking account of private equity and debt, these crypto assets, despite their stellar performance over the past year or so, still have a market value that is less than 1% of conventional financial assets.

New forms of money

The second category of digital asset developments, presented as the middle panel of Table 1, are the variety of new forms of money held on permissioned distributed ledgers or in some cases on conventional centralised databases. This category is more similar to conventional finance. All these new forms of digital money are based on permissioned ledgers (in contrast to the unpermissioned ledgers used in decentralised finance and crypto exchange).

There is a similarity between these new forms of money held on cryptographically secured shared ledgers and non-bank e-moneys also covered by Table 1. Like non-bank e-moneys (of which there are many examples including MPesa in East Africa, AliPay and WeChat Pay in China, and Paypal deposits) these new forms of money are held as entries on a single ledger and therefore can be transferred directly from one holder in a 'closed loop'. This contrasts with indirectly held bank deposit money which, if transferred from a holder in one bank to a holder in another bank, requires subsequent settlement.

All these new forms of digital money are fully reserved, not fractionally reserved like conventional commercial bank money. Some – including Alipay, WeChat Pay and Utility Settlement Coin – are fully reserved in central bank money. Others are also fully reserved but either in commercial bank money (e.g. MPesa) or by a portfolio of high quality money market and fixed income securities (e.g. PayPal). The now abandoned plans of Facebook and its partners for a digital retail currency – first Libra with its own novel unit of account based on basked of fiat currencies and then its successor Diem, intended to be offered in major fiat currencies first in US dollars – were similarly to be fully reserved with high quality money market and fixed income instruments.

A different example of a new digital money designed to meet unmet user needs is the Utility Settlement Coin, issued by Fnality, which will allow banks to make 24-7 instantaneous interbank large value monetary transfers in several currencies, thus getting around the limited opening hours and potential delays of transfer when using central bank RTGS systems and in this way supporting more efficient liquidity and collateral management in money, foreign exchange and capital markets for large international banks. For these bank users, unlike retail users of e-money, a shared ledger is required, because no major international bank will want to rely on a ledger operated by a competitor.

The distinction made in Section 3, between directly held digital assets and indirectly held conventional assets, is clear for the case of digital money fully reserved in central bank money. This distinction is less clear for digital money fully reserved in commercial bank money or in money market instruments. These are mixed cases: some transfers, those between holders, are direct without requiring settlement. But because the underlying reserves are indirectly held money, transfers out of the digital money, exchanging into other forms of money or transmitting a payment to a non-holder, require a subsequent settlement in the same way as a transfer of commercial bank money.

A feature of all these digital moneys in the Table 1 second category of digital asset development is that their values are institutionally guaranteed (though typically subject to fees when withdrawn for exchange into other forms of money). This contrasts with the stablecoins employed in crypto asset exchanges, whose values are not guaranteed. In this respect stablecoins are more like money market mutual funds, with fluctuating market values that are managed within a small range but can potentially fall below their stated par.

The boundaries between these categories are not watertight. There is interest in using stablecoins, developed for crypto asset trading (i.e. the first category of digital asset development), as new forms of retail money (i.e. the second category of digital asset development). An example is the recently announced Facebook supported Novi wallet will offer no-fee person to person payments using the managed stablecoin Pax, initially in a pilot targeting payments between the US and Guatemala. While the choice of stablecoin is unlikely to matter for initial pilots of this kind, there are obvious problems. Such a system could be difficult to scale given the risk that the value of the managed stablecoin is not guaranteed and could fall substantially below its fiat currency par value.

An open question, at this point in time, is whether there will be any successful retail stablecoin with a guaranteed value that complies fully with the Section 3 definition of a digital asset, i.e. operating on a distributed ledger. The recent decision by Facebook and its partners to terminate the Diem project illustrates that adoption of distributed ledger technology, alone, is no guarantee of success as a retail money. Other forms of digital money held on distributed ledger are not designed for retail use, either the stablecoins held on permissionless distributed ledger for crypto exchange or wholesale digital money for use by financial institutions such as Utility Settlement. In contrast, several non-bank e-money platforms such as AliPay, WeChat Pay, MPesa and Paypal have proved successful for person to person and retail purchase without being held on a distributed ledger. The use of a conventional centralised database with a commercial operator has not limited their adoption.

The final nascent example of a new form of digital money is Central Bank Digital Currency (CBDC). Before 2019 there were a number of technical experiments by central banks with issue of central bank money on shared cryptographically secured money, primarily driven by techno-enthusiasm and a need to keep abreast of these technological developments. The development of stablecoins – along with the considerable publicity surrounding the Facebook Libra now Diem project – have somewhat spooked the world's central banks, leading them to anguish about loss of monetary control. Since 2019, they have been driven to explore the development of new regimes for the regulation of stablecoins and also to a much fuller extent, to examine the launch of central bank equivalents to stablecoins i.e. CBDC.

Some central banks have already issued CBDC on a commercial scale, notably the e-CNY in China and the Bahamian Sand Dollar. The ECB is also in the forefront, leading detailed investigation by the Euro system of central banks into the potential issue of retail digital Euro (though it is unclear whether this will rely on a conventional centralised database or a permissioned distributed ledger).

Unlike crypto assets and decentralised finance, these development of new forms of digital money are primarily motivated by a desire to address previously unmet user needs. This is

true of e-moneys, which have been most widely adopted in jurisdictions where a large proportion of the population were unbanked or where banks failed to provide effective non-cash payment solutions for retail spending and person to person monetary transfers. It is also a key motivation for the introduction of CBDC and for the development of wholesale digital money such as Utility Settlement Coin.

Operations in financial markets and financial services

The third category of digital assets in Table 1 is a variety of developments employing distributed ledgers to support more efficient automated operations in security and derivative markets, in commercial and international banking, in asset management and in insurance. There are a large number of exploratory applications of this kind, usually employing shared cryptographically secured ledgers or in some cases combining cryptographic security together with conventional centralised databases. Again, as with the new forms of digital money, these are always permissioned ledgers, not the unpermissioned ledgers employed in decentralised finance and crypto asset trading.

A full list of such initiatives would be extremely long. It could also include many non-financial as well as financial applications, all cases with perceived benefits from holding agreed data on shared cryptographically secured ledgers. Table 1 is limited to a few illustrative examples.

The first of these are the commercial versions of programmable permissioned distributed ledgers, including Quorum (a permissioned version of the Ethereum blockchain employed in a number of proprietary distributed ledger financial applications for example those offered by Consenys) and HyperLedger Fabric (which supports a number of non-proprietary opensource financial and non-financial applications). Many proof of concept projects have now been developed for financial applications using these tools (the Consensys and Hyperledger Fabric webpages give many examples).

The second development under this third category included in Table 1 are some of the most prominent experiments with issue of conventional securities, such as bonds and equities, as digital assets on permissioned shared cryptographically secured ledgers. One user need that these developments meet is facilitating low cost retail bond investment, e.g. this is the objective of both the Thai government savings bonds and the Hyperledger BondEValue projects. In other examples the user need is less clear, these seem to be more based on techno-enthusiasm, examples are the World Bank bond-i issue or the creation of the Six digital exchange. The final example in Table 1 is the increasing use of cryptographic security and sharing of data to automate financial operations, even though this may often be more easily pursued employing a conventional centralised database rather than a shared cryptographically secured ledger. The example given in the table is that of ISDA automated interest rate derivative clearing, which is based on DAML, the “digital asset meta language” developed by the technology firm Digital Asset. Here the key elements that support automation are the use of public-key cryptography together with unambiguous contract description.

The potential of such digitisation of conventional financial assets is substantial, but how far and how quickly this will be pursued is unclear. Arguably this could substantially simplify operations, putting all operational systems for both trading and servicing of financial assets

on a common basis, dramatically increasing operational transparency, hence supporting substantial cost savings in asset management and in capital markets. A difficulty though, as discussed in Section 4, is that this could potentially require quite substantial changes in the business models of financial intermediaries.

Annex 4 Intermediary business models and the regulatory perimeter.

The reason that transactions in digital assets do not require clearing and settlement is because, they are directly held. The transaction execution – whether a physical transfer of a note, or the debiting of one digital asset account on the shared ledger and the crediting of another – also serves the transfer of ownership. Not only does this make settlement immediate, so a newly acquired digital asset is immediately available for re-use, it also eliminates the possibility of settlement fails, when money or securities are not delivered as promised. At times of stress in funding markets these settlement fails can spike sharply, creating systemic risks. A shift to digital assets could eliminate this systemic risk.

It would require an industry wide standardisation of transaction messaging and processing of financial assets, hence promoting near universal automation of operational processes and substantially reducing operation costs. Think ISO20022, but extended to the entire universe of finance. It would also promote much greater transparency of financial intermediaries, to the benefit of investors and customers in asset management. A further benefit, often mentioned in relation to digital assets, is moving from delayed settlement, typically T+2 in equity and foreign exchange markets, to immediate real time settlement.

There are moreover substantial additional business model challenges from any shift from the current convention of T+2 settlement in securities and foreign exchange markets to immediate instantaneous exchange without any need for subsequent settlement. Typically, a foreign exchange or security trade is settled by the beginning of the second trading day following the initial agreement to exchange. During this period trades are first netted, reducing the volume of trades that must be settled through exchange of cash and securities by up to 97% or 98%. Then participants must prepare for settlement, accessing repo and securities-lending markets as necessary, in order to position the cash and securities for exchange. Finally, settlement takes place.

Supporting all of this is a legal and regulatory framework that has developed over the course of many decades to support the required netting and ensure the predictability of contracts that commit to sale of assets that are not already owned or purchase of assets without having pre-arranged financing already in place.

These arrangements, while operationally complex, provide market participants with considerable savings of both capital and liquidity. T+2 settlement is not perfect. There is scope for contracting the cycle to T+1 providing further savings in capital and liquidity. Still, capital and liquidity committed to trading operations are already small, when compared to the value of transactions, so a contraction of the settlement cycle from T+2 to T+1 would provide only modest benefits.

In the case of custodian banks, a shift from indirect to direct holding of securities substantially changes the business models of securities lending. The loan would now have to be made from the shared ledger instead of from custodian managed security accounts. A shift from indirect to direct asset holding would also substantially change the business models of brokers, dealers and traders participating in securities and foreign exchange markets.

Despite this uncertainty it is possible to anticipate how the regulatory framework for digital assets will evolve in the years ahead. A central point is that regulation of the first digital asset development of Table 1 – DeFi and trading of crypto assets – must be very different from the regulation of the second and third digital asset developments– new forms of digital money and the use of digital ledgers to support operations in financial markets.

For DeFi and trading of crypto assets, all that regulation can do is to control the regulatory perimeter, the boundary between decentralised and mainstream finance. This is not, ultimately, a major barrier to regulation because the large majority of transactions even in crypto assets will be through regulated intermediaries. We can expect to see increasing oversight and regulation of the intermediaries that support crypto asset trading, including even the crypto asset exchanges. The tools at the regulator's disposal, should they choose to use them, are powerful. They can insist that mainstream financial institutions, handling crypto asset investment on behalf of institutional investors, transact only through adequately regulated crypto exchanges. They can police the boundary between the established payments systems – both conventional bank and card payments and the new forms of digital money – ensuring that KYC and AML obligations are met by all regulated institutions who offer. They can, if they wish, do more to promote the protection of retail customers who chose to invest in crypto assets through regulated intermediaries.

Stablecoins are a particular concern for regulators, especially their potential use outside of their original application in crypto asset trading. Like cryptocurrencies these can be used for making payments outside of the oversight of regulatory, law and tax authorities, but with the added advantage that their values are stable so they work better than cryptocurrencies as stores of value. Here the focus can be expected to be two pronged. Those stablecoins that are institutionally managed such as Tether and Pax can expect to come under increasingly close regulatory scrutiny, though this will require improved international co-ordination to be effective. At the same time there will be increased regulatory focus on mainstream financial services, for example payments wallets, that employ stablecoins as their digital money. Here regulators may require institutional guarantees, backed by the same regulations that currently cover commercial bank deposits and e-money. Reliance on stablecoins, without guarantees and not reserved in central bank money, may eventually be prohibited in retail and business payments solutions, to ensure customer protection and systemic stability.