



CRYPTOCURRENCES: OVERCOMING BARRIERS TO TRUST AND ADOPTION

Dr Zeynep Gurguc and Prof William Knottenbelt,
Imperial College London

**Imperial College
London**
Consultants

Contents

01	Foreword	02
02	Executive summary	04
03	Introduction	06
04	Key blockchain concepts	07
05	Evolution of money	11
06	Challenges and solutions	17
07	Conclusions and conjectures	21
08	Glossary of terms	23
09	Acknowledgements	24

01 Foreword



The Internet started out with the simple use case of email (digital communications) and the aim to decentralise communications. The Blockchain, in a similar vein, started out to decentralise 'value'. The first use case being cryptocurrencies like Bitcoin (digital money).

As the Internet scaled so did the use cases. The Internet facilitated e-commerce, social networks, gaming and so on. In the same way, the Blockchain has increased its use cases, away from much talked about cryptocurrencies like Bitcoin and Litecoin to other cryptoassets, such as cryptocommodities like Ethereum and cryptotokens like Steem. New use cases will continue to emerge and other segments such as cryptosecurities will start to appear.

Just as communication underpins almost all applications across the Internet, value will do the same on the Blockchain. This concept of value and in turn money is what we seek to review in this report.

Traditionally, money needed to fulfil three fundamental roles: a store of value, a medium of exchange and a unit of account. If Bitcoin or cryptocurrencies are to become the 'new money' there are several questions we need to address:

- Does it need to fulfil all of the aforementioned roles?
- Has money and its definition evolved?
- Does money have to be 'real'?

At the same time, we have to ask, what does this really mean for the everyday consumer?

Conversation tends to focus on whether individuals should invest in cryptocurrencies. But if cryptocurrencies are to fulfil their intended use case - and become a

globally accepted form of money - we should also be asking when buying the weekly shop with them will be commonplace.

As our findings make clear, the notion that cryptocurrencies have to fit in with old-world financial models is flawed. Money has always evolved. Its uses and social status have changed and will keep changing. Why should we measure cryptocurrencies with the same yardstick used for traditional payment and currency systems? Would you really judge email with the same criteria as the written letter?

The report supports our conviction that cryptocurrencies will gain global mainstream adoption within the next decade.

If the Internet changed the way we communicate, starting off with a simple application (email), that led to a transformation in the way we do global business, imagine what the Blockchain could do. If we change the way we transfer value and think about money by using a simple application like Bitcoin, what could that do for global commerce?

It could be a long journey, but it is one well worth exploring.

Iqbal V. Gandham
UK Managing Director at eToro

A handwritten signature in black ink, appearing to read 'I. Gandham'.

The background is a dark blue-grey field filled with glowing digital elements. Streams of binary code (0s and 1s) flow diagonally across the frame. Interspersed among the code are small, colorful squares in shades of blue, green, and red, resembling data points or pixels. The overall effect is one of high-tech digital connectivity and data processing.

**“...Bitcoin
and Blockchain
technology could
do to banks what
cell phones did to
telephone poles.”**

Chris Burniske and Jack Tatar, *Cryptoassets*, 2017

02 Executive Summary

Blockchain – and Distributed Ledger Technology (DLT) in general – has become one of the most hyped technological innovations since the Internet and the focus of both public and private sector stakeholders. One of its applications, namely cryptocurrencies, and, in particular, Bitcoin, has attracted enormous attention; however, Bitcoin and other cryptocurrencies – and the overall concept of Blockchain – are often misunderstood.

Our goal is to analyse cryptocurrencies, in particular Bitcoin, by looking into the evolution of money and assessing which particular aspects of cryptocurrencies are different from government backed fiat money, if any. We also explore further potential applications of the emergent DLT concept, and expand to the larger context of tokens and the potential of DLT business models.

By looking at the evolution of money, we explore how cryptocurrencies can transition into mainstream use and become globally accepted by fulfilling the three main roles of traditional fiat money, namely:


1. Medium of exchange
2. Unit of account
3. Store of value

We believe that cryptocurrencies and cryptoassets are already utilised as a store of value, yet cryptocurrencies still have to satisfy the first two functions of traditional fiat money to overcome the barriers to becoming globally accepted and adopted payment instruments. Fulfilling the functions of a medium of exchange and unit of account are highly dependent on governmental and other ecosystem actors.

We argue that cryptocurrencies can become units of account only if there is a friendly and conducive regulatory environment. We conjecture that this could then allow businesses to accept cryptocurrencies as payment systems in a broader context.

Furthermore, we argue that technical and economic challenges such as scalability, privacy and volatility need to be overcome in parallel. Finally, DLT businesses, cryptocurrencies and cryptoassets need to invest in design thinking as user-friendly design is at the core of any successfully adopted technology. Only then could we expect a continuation of the exponential growth of adoption seen in the technology's early phases.

We acknowledge that new payment systems (or asset classes) do not emerge overnight; and, there are many more challenges that DLTs in general are destined to face. However, it is also worth noting that the concept of money itself has evolved greatly in our lifetime from cash to plastic via use of debit/credit cards and even more so through the current use of contactless payments. The wider use of cryptocurrencies is the next natural step in reducing friction in the global economy, supported by the adoption of tokens in local contexts, be they specific to geographies or industry-sectors.



**“Cryptocurrencies
can become units of
account only if there
is a friendly and
conducive regulatory
environment...”**

Dr Zeynep Gurguc and Prof William Knottenbelt

03 Introduction

Blockchain – and more generally DLT – has attracted significant interest due to its potential to reshape industries, organisational and governance structures, and disrupt traditional business models. Industrial, academic and state actors are simultaneously cooperating and competing to create practical applications for Blockchain – and DLTs – in multiple domains.

In this report, our goal is to examine how cryptocurrencies and cryptoassets can transition into mainstream use. To explore this, we investigate the capabilities of the emergent Blockchain concept, its ecosystem and the barriers it faces with respect to wider adoption.

We start by discussing key concepts in this field and examining cryptocurrencies, in particular Bitcoin, before expanding to the wider context of smart contracts and token economies. We outline the functions and evolution of money throughout history and provide a comparative analysis of fiat money vs. cryptocurrencies.

Finally, we explore the short-, medium- and longer-term challenges that these concepts and cryptoassets need to overcome in order to realise their potential to decrease the local, global and industry-specific economic and digital frictions that we currently experience.

04 Key Blockchain Concepts

a. Distributed Ledger Technology

A distributed ledger is an immutable database that is governed by a predetermined set of rules, consensually shared and synchronised across multiple sites, institutions or geographies. It enables untrusting parties with common goals to co-create a permanent, immutable and transparent record of exchange and processing, while making the database more secure and resilient.

We can categorise DLTs according to certain characteristics. First, the ledger may be publicly available or not; namely, public versus private. Second, they can differ in terms of which set of verifiers are authorised to validate transactions; namely, permissionless versus permissioned¹.

Public and permissionless DLTs are systems where an open set of participants are allowed to submit transactions to the ledger as well as validate them. These public and permissionless systems are potentially the most impactful in terms of changing organisational and governance structures as they do not rely on a centralised authority for trust but rather a large number of network participants. These systems offer the scope for a foundational shift in business models and optimal allocation mechanisms. However, they can be computationally expensive and currently face scalability issues.

Public and permissioned DLTs only allow an authorised set of participants to be validators and hence require permission to become a node; however, all transactions are publicly viewable.

Finally private and permissioned DLTs are more appropriate for highly controlled and regulated environments where all participants need to be known, hence lack the pseudo-anonymity and decentralisation of authority associated with permissionless ledgers but offer higher transaction rates, and settlement times at lower costs than current public permissionless systems.

b. Cryptocurrency

Cryptocurrencies such as Bitcoin consist of a peer-to-peer network of nodes which jointly maintain a common tamper-resistant record of historical transactions without relying on a central authority or trusted third party. The key innovation is a novel transaction-recording mechanism known as the blockchain. The latter is made up of blocks – that is, batches of validated transactions – which are chained together – that is, logically linked or tied to each other in such a way that any attempt to edit or otherwise corrupt the historical record is either prohibitively expensive or becomes immediately evident. Therefore, a DLT such as Bitcoin, enables its participants to co-create an irrefutable record of transactions.

Cryptocurrencies have popularly been used as a catch-all synonym for what is actually a broader term, namely cryptoassets. Cryptoassets include any digital asset that utilises cryptography. Three subclasses of cryptoassets have been identified in the recent literature: cryptocurrencies, cryptocommodities, and cryptotokens (Burniske and Tatar, 2017). Cryptocurrencies (e.g. Bitcoin, Litecoin, Monero) are digital coins designed to fulfil the traditional role of real-world currencies but in the digital space, i.e. to act as a global medium of exchange. Cryptocommodities (e.g. Gas in the Ethereum network) are the computing, storage and networking resources which power blockchain ecosystems, just as physical commodities like oil provide the fuel for real-world economies. Cryptotokens, known as tokens in the DLT sphere, embody tradeable assets, or value exchange and/or creation mechanisms for goods or services, often in an industry- or domain-specific context, and will be discussed further in section 4.e. Cryptotokens include tokenised investment assets, namely cryptosecurities, a term that is currently drawing more attention.² The relatively recent term 'cryptoconsumable' refers to a cryptotoken that is constructed to decrease in value over time using a decay or burn function to influence token velocity (Outlier Ventures 2018)³.

¹ For a good graphical representation please refer to Mulligan, Catherine, Jennifer Zhu Scott, Sheila Warren and JP. Rangaswami. World Economic Forum. Blockchain Beyond the Hype:

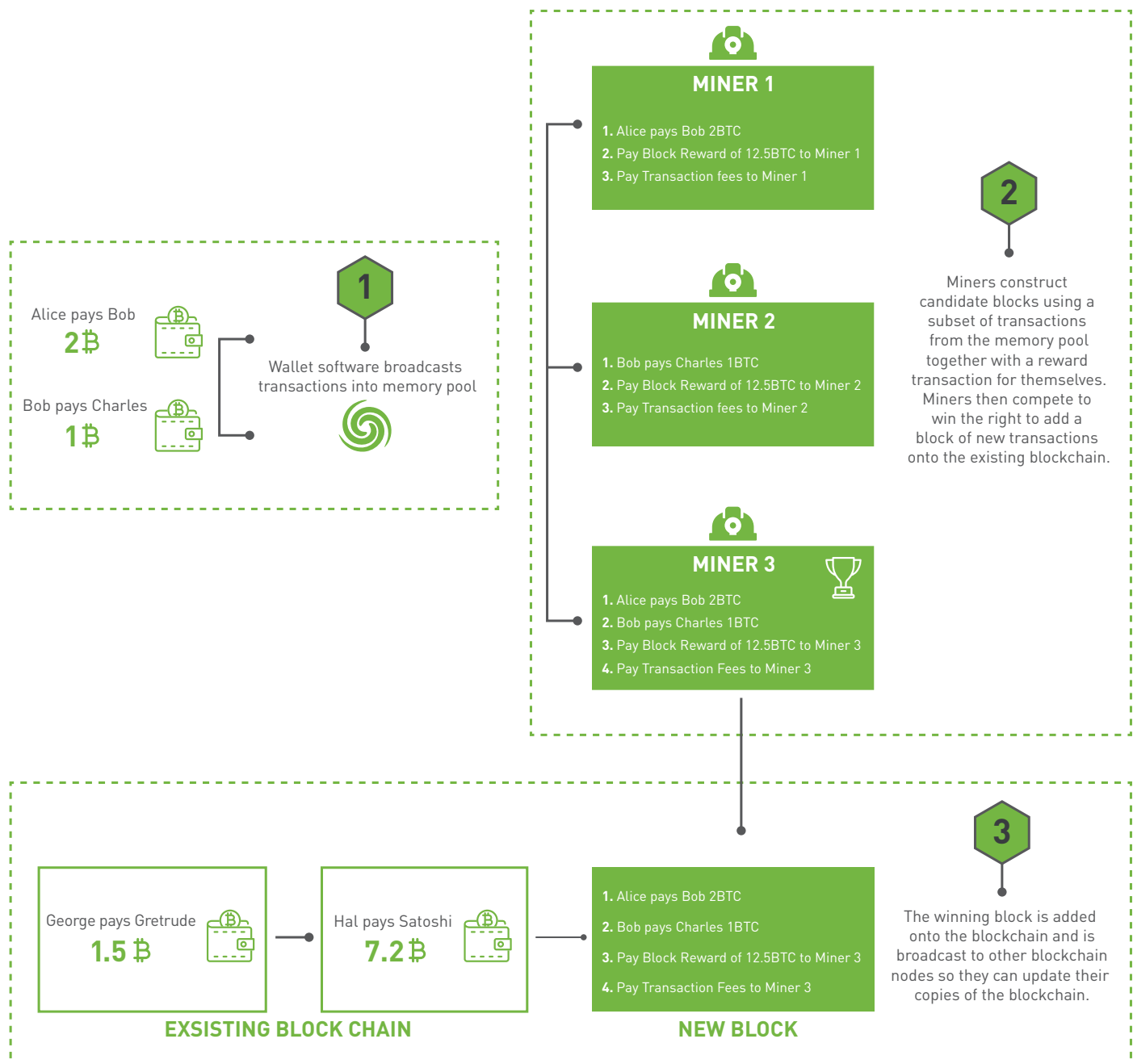
A Practical Framework for Business Leaders. 2018

² <https://news.bitcoin.com/coinbase-acquires-investment-firms-regulated-crypto-securities/>

c. Bitcoin

Bitcoin (BTC), without relying on a central authority, uses a peer-to-peer network of nodes which jointly maintain a common tamper-resistant record of historical transactions. A transaction entering the Bitcoin network at one of its constituent nodes does not immediately join the blockchain. Instead, it is validated⁴ and inserted

into a waiting area known as the memory pool⁵. It is then broadcast 'gossip'-style to other nodes. Every node that receives the transaction repeats the validate-insert-broadcast cycle. In this way, the transaction is rapidly propagated around the world, but it is not yet part of the blockchain.



³ Outlier Ventures. The Convergence Ecosystem. Technical Report, March 2018. Available at https://outlier Ventures.io/wp-content/uploads/2018/03/The_Convergence_Ecosystem_Report_Outlier_Ventures_2018.pdf

⁴ For example, assessing whether the transaction is cryptographically signed by the sender and verifying that the transaction does not spend funds that are not available or create funds out of thin air

⁵ See <https://blockchain.info/unconfirmed-transactions>

Special nodes, known as miners, then build up a block of transactions they wish to publish (thereby adding a block to the blockchain) by selecting transactions from the memory pool. To win the right to publish their block, a mining node must solve a cryptographic puzzle that is a function of both the most recently published block in the blockchain and the present one. It is in principle so hard to solve this puzzle that the only way to do so is to repeatedly guess solutions in a brute force manner - this is the process of *mining* with each guess known as a *hash*. It is, however, very simple to verify that the correct solution has been found, so that anyone can immediately verify that the correct answer has been found without repeating the same brute-force process. The amount of work expended to solve the puzzle proves the miner has invested in securing the system, and their reward is the permission to publish the next block of transactions. Publishing the block thereby orders the transactions in time and prevents double spending.

The incentive for the nodes to participate in the mining process entails the right to include a transaction rewarding themselves with the block reward of a certain number of new bitcoins (the so-called 'coinbase' transaction) plus the transaction fees for all transactions included in the block. The Bitcoin software running on network nodes controls the supply of new bitcoins, by regulating the difficulty of the puzzle from time to time so that blocks should be published on average once every 10 minutes. (Footnote: As of 3 March 2018, the chances of guessing a valid solution to the mining puzzle with a single hash is truly minuscule - approximately one in 13 sextillion (13×10^{21}).) Given that the blocksize is fixed, the limit on the rate at which blocks are published has the side-effect of limiting transactions throughout the Bitcoin network as a whole.

Once a valid block has been found by a mining node, it is broadcast to other nodes, which validate the block and (if it passes validation) add it to their local copy of the blockchain. At this point the transaction has been embedded in the blockchain and is said to be confirmed. The deeper a transaction is embedded in the blockchain the more certain it is that it cannot be edited without an extraordinary amount of computing power (or, alternatively, the ability to solve the mining puzzle in a much more efficient way than guessing).

At certain points there may be competing versions of the block(s) to be added (because different miners discover publishable blocks at nearly the same time for example); in which case the chain is said to have forked.

This is usually resolved in relatively short order by nodes choosing to add new blocks to whichever branch is the first to become the longest chain. Community disagreements can lead to forks of a much more serious and more persistent nature. For example, Bitcoin Cash is a fork of Bitcoin with much larger block sizes, which emerged following the inability of the community to agree on whether or not an increased block size was the most effective solution for the congestion being experienced in the Bitcoin network. Ethereum is actually a fork of the Ethereum Classic network, with added state changes to reverse the effect of a large smart-contract-related hack in June 2016.

Without precautions, forks can lead to unintended chaos - e.g. transactions can be replayed from one fork into another, and miner hashing power can swing dramatically between forks, destabilising their block publishing rates and security.

d. Smart contracts

Smart contracts⁶ are programmed rules that are self-executed or verified by computer code; that is, when some predefined rules in a contract are met, a set of predefined actions are executed without an enforcement authority/mechanism other than computer code. More traditionally, a contract may be defined as an agreement, a legally enforceable promise or an instrument that allows the designer to plan for possible contingencies.

In economics, the main challenges with respect to contracting are 'asymmetric information', which occurs when parties involved in a contractual relationship do not possess the same level of relevant information; and, 'bounded rationality', which occurs due to the fact that not all contingencies in a contractual relationship can be defined or accounted for⁷. Accordingly, the principal goal of any contract is to minimise asymmetric information, particularly moral hazard, where some parties involved in a contractual relationship may be tempted to exhibit 'opportunistic behaviour' and affect the other parties' values of the contract negatively.

Arguably, by making use of new digital tools and protocols, smart contracts could offer an improvement over traditional contractual relationships by increasing traceability, accountability, enforceability and trust even among strangers while decreasing the costs that would have to be borne running these processes in a traditionally bureaucratic analogue system.

⁶ The term was coined by Nick Szabo in 1996.

⁷ Either simply because some events are unforeseeable, because of costly calculations or our cognitive limitations.

e. Tokens

Tokens in the context of blockchain, in other words cryptotokens, are value exchange/creation mechanisms that allow a community or network participants to govern and manage the system. Two broad sub-categories of cryptotokens are security tokens and utility tokens. Security tokens, that is cryptosecurities, are comparable to equity held in a firm and are subject to general securities regulations. Utility tokens, on the other hand, provide access to the services provided by DLT companies; and have started to play an important role in ensuring that the incentives of network participants are properly aligned and the underlying decentralised protocols are robust. Currently, some tokens can be considered as a hybrid between the two since, on the one hand, they stipulate some predetermined utility for their own ecosystem; on the other hand, investors use them as a way to store value.

Accordingly, the terms cryptoeconomics, tokenomics and token engineering refer to the alignment of participants' incentives in the blockchain ecosystem for two main purposes; first, for nodes to sustain the network, and second, for participants of a certain ecosystem/market to exchange value in a seamless manner. In addition to cryptography, cryptoeconomic modeling relies on the proper use of game theory, mechanism design and behavioural economics, which has finally started to gain popular attention in the DLT environment⁷.

Utility tokens conceivably have a wide range of applications varying from exchange of data or data services, granting licenses, verification of credentials/ownership rights, to reputation management among others. If they are utilised to enhance coordination of resources and network participants, they can potentially allow markets to become more accessible, open and efficient.

For example, the Aventus protocol governed by the ERC20⁹ compatible Aventus token (AVT) regulates rules around the ticketing supply chain. The Golem token (GNT) helps the governance of a computing power sharing economy. Storj, governed by the STORJ token, allows users to store their data in a decentralised way by making use of a payment system based on the blockchain.

f. Ethereum and beyond

While Bitcoin can support some classes of simple smart contract, it is overwhelmingly focused on the peer-to-

peer transfer of value in the form of a single class of token (BTC). Ethereum, on the other hand, is a powerful general-purpose blockchain platform for decentralised computation that was designed from its conception to support the deployment of smart contracts. Ethereum's rapid block time (an average of 15 seconds vs an average of 10 minutes for Bitcoin) means that changes in the state of smart contracts can be reflected in the blockchain record in a much more timely fashion than would be possible in Bitcoin. Ethereum features a native token (Ether or ETH) which can be used to pay for the cost of executing smart contracts and transaction fees. It is also a popular platform for the creation of new digital token ecosystems - particularly via the ERC20 token standard, which defines common operations and interfaces that must be provided by compliant tokens. At the time of writing there are over 290 such tokens, each with a market capitalisation in excess of \$10m¹⁰.

The safety, correctness and security of currently deployed smart contracts is highly variable, and it is often the case that smart contract code of apparently good quality can conceal subtle unforeseen bugs. One recent academic study found thousands of live Ethereum smart contracts that could be exploited to lock up funds on an indefinite basis, leak funds to arbitrary users, or be terminated by arbitrary users¹¹.

Several blockchain platforms that aspire to compete with, and perhaps ultimately even supplant, Ethereum as the pre-eminent platform for smart contracts and the foundation of new digital token ecosystems are under active development, most notably Cardano, EOS and NEO (sometimes referred to as the 'Chinese Ethereum'). Other platforms, most notably Stellar, make less use of flexible smart contracts, with an eye to boosting security, which is an important consideration in its targeted use case of financial environments. Other platforms seek to move away from the linear transaction recording structures traditionally associated with blockchains and classical cryptocurrency mining. IOTA, for example, uses a directed-acyclic-graph (DAG) or Tangle in which transactions are validated by other users who are seeking to make transactions.

It should be noted that factors such as the state of platform development, the range of actually-deployed applications and the degree to which security properties have been rigorously verified, varies a great deal across all of the aforementioned platforms.

⁷ Either simply because some events are unforeseeable, because of costly calculations or our cognitive limitations.

⁸ See e.g. the blog post "A Crash Course in Mechanism Design for Cryptoeconomic Applications" by Alex Evans.

⁹ A standard for Ethereum tokens which will be further discussed in Section 4.f

¹⁰ Source: <https://etherscan.io/tokens>

¹¹ See <https://arxiv.org/pdf/1802.06038.pdf>

05 Evolution of money

Cryptocurrencies are virtual, and do not possess a physical form, which often leads to the key misconception that they 'do not exist'. This view is based on a fundamental misunderstanding of how money gets its value and is used day-to-day. Therefore, before delving into cryptocurrencies and offering a comparative analysis of cryptocurrencies versus fiat money, we provide a summary of the functions of money as well as an historical overview. We investigate the barriers that cryptocurrencies currently face and explore how they need to evolve in order to transition into mainstream use.

a. What is money?

In legal terms, fiat money is defined as a legal tender¹² by order of a government, which is legally recognised as a medium of exchange for the payment of debts but doesn't have an intrinsic value. Instead, economists, fascinated with the concept of money for a long time, usually define money as anything that serves the functions of: (i) medium of exchange, (ii) unit of account, and (iii) store of value. Money acts as a medium of exchange by eliminating the need for double coincidence of wants, which is necessary for a barter economy to function; thereby increasing efficiency in the process of exchanging goods and services. Money is a unit of account as it acts as a measure of value in the economic system. Finally, it also acts as a store of value as it allows individuals to make intertemporal choices on when to spend their purchasing power.

In economics literature, money can be modeled as a bubble, where it yields no future payoff and holds no intrinsic worth but is valued for what it will provide in exchange. These are valid assumptions for fiat money as it is not backed by a physical commodity such as gold or silver. In a sense, the value of money is determined by a coordination game among the participants of its ecosystem. Professor Morris Perlman very wisely stated: **"Money is like a myth that requires only imagination for its creation, but faith for its effectiveness"** Morris Perlman, Macroeconomics (3rd edition), 1999

b. Evolution of money and the emergence of cryptocurrencies


Throughout history, we observe that many cultural, political and economic actualities caused money's form to change. In 7th century BC, the Lydian empire, in what is now Turkey, was the first civilisation to use minted silver or gold coins. However, from the very beginning of trade relations, individuals have used some sort of payment method first in the shape of bartered goods, and eventually money that held many forms varying from cowrie shells and cattle, to beads from precious metals, and even salt.

The first fiat currency was used in China and dates back to 1000 AD, but fiat money became prevalent only after the decoupling of the US dollar from gold in 1971, which effectively brought the end of the Bretton Woods system. Until then, most money was convertible to precious metals (which was called the gold standard in the 20th century). Under the Bretton Woods system, currencies of the member states held a fixed exchange rate regime, maintained within 1 percent, with respect to US dollars, which was in turn convertible¹³ to gold. These commodity-backed monetary systems of the past could be costly and inefficient; however, they offered stability. In contrast, current non-convertible systems offer freedom to governments in shaping monetary policy but sacrifice price stability and may result in inflation.



More recently, advances in computing facilitated the evolution of money into 'centralised' electronic money which is broadly defined by the European Central Bank as "an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer". It also allowed the creation of 'centralised' virtual currencies, used particularly in multi-player computer games. However, previous attempts to replace fiat money by 'centralised' virtual currencies largely failed on account of this centralisation, because this offered a single system for hackers to attack, or company to close in the case of regulatory misadventure.

¹² For a good discussion on what a legal tender is, please refer to <http://edu.bankofengland.co.uk/knowledgebank/what-is-legal-tender/>

¹³ Convertible directly, meaning backed by gold (currently currencies are exchangeable to gold, according to prices determined by the markets, like in any other commodity, not backed by gold.)



“Money is like a myth that requires only imagination for its creation, but faith for its effectiveness.”



Morris Perlman, Macroeconomics (3rd edition), 1999



Bitcoin and other cryptocurrencies are in a unique position in that their decentralised architecture provides no single point of control at which they can technically be regulated or shut down. Moreover, with ever-expanding digital technologies and the current rise in computing resources in terms of both capacity and efficiency, it is easier than ever before to become a network validator. Nevertheless, to become widely adopted as a payment system decentralised currency structures face a new set of technical, legal, and economic and social challenges; which will be discussed in detail in Sections 6 (challenges and solutions) and 7 (conclusions).

A simple comparison between fiat money and cryptocurrency shows us that the value of both fiat money and cryptocurrency is derived from the interaction of supply and demand. The difference is that fiat money is backed by a central government and allows central banks to conduct monetary policy, whereas cryptocurrency is a digital asset that operates independently of a central bank. Traditionally, monetary and fiscal policy complement each other and allow governments to manage a nation's economy. The central bank of a nation conducts monetary policy to reach macroeconomic targets by managing the money supply and the interest rate; whereas the government uses tax policies and government spending to carry out fiscal policy.

Similarly, monetary policy in the crypto-space refers to the management of coin/token supply, which can be fixed, expansionary or subject to a decay function. Other measures, such as discounts on certain services in DLT business models, subsidies offered to some network participants, or partitioning of tokens among the stakeholders in the ecosystem in a particular way, can be considered as fiscal policy measures that are available in a token economy.¹⁴ These tools affect token velocity, which has important implications for the volatility, scalability and overall health of the token economy and sustainability of any DLT based business model/market.¹⁵

Bitcoin, the most famous decentralised cryptocurrency, has an interesting set-up. It is often compared to gold as it has a finite supply (of 21 million BTC) and needs to be mined. In this respect it shares some features with gold.

Table 1 (page 14) presents a more detailed comparison of gold, Bitcoin and government money. It is important to note that individual units of Bitcoin are highly divisible (each Bitcoin being made up of 100 million Satoshis), so there are plenty of currency units to support a full range of economic activities irrespective of the unit price of Bitcoin. Indeed, as the price of Bitcoin has risen in US dollar terms over the years it has become customary to trade in mBTC (milli-Bitcoins or 1/1000 of a BTC). Should the price continue to rise then it is expected that µBTC (micro-Bitcoins or 1/1000000 of a BTC), and perhaps eventually even the Satoshi itself will become the preferred unit of trading.

¹⁴ A good discussion on monetary and fiscal policy in the context of tokens can be found at <https://medium.com/@avtarsehra/economics-of-initial-coin-offerings-c083311e53ec>

¹⁵ Good resources on token velocity are <https://medium.com/newtown-partners/velocity-of-tokens-26b313303b77> and <https://medium.com/outlier-ventures-io/why-token-velocity-matters-1ad459435e33>

	Gold	Bitcoin	Government money
Production mechanism	Mineral mining using electrically-powered extraction device. Electricity in, physical commodity out.	Cryptocurrency mining using electrically-powered extraction device. Electricity in, digital commodity out.	Physical notes are printed but most money is created electronically. Typically issued by commercial and central banks of nation states.
Maximum supply	Finite (but unknown). Supply has consistently increased at a rate of c. 1.5% p.a. for more than 100 years.	Finite (and known). Supply currently increasing at c. 4% p.a. but rate of increase from year to year is always decreasing and will drop to 0 by 2140.	Theoretically unlimited. Supply has increased at an average rate of c. 11.5% p.a. over the last 40 years ¹⁶ .
Concentration of resource	Varies by geography but is fixed within specific locations. Independent of global mining power deployed.	Dynamic concentration, dependent on global mining power deployed, and adjusted every 2016 blocks (+/- 2 weeks).	Dynamic, dependent on government and central bank policies.
Storage	Expensive. Requires secure physical location. Can be held directly or via nominee.	Inexpensive. Requires secure storage for private keys, which can be offline or online. Can be held directly or via nominee.	Usually inexpensive. Requires wallet, secure physical storage or bank account. Can be held directly or via nominee.
Unit of trade	Priced per Troy Ounce (31.1g). Typically available in quantities ranging from 0.5g (+/- \$30) to 1kg (+/- \$40000).	Priced per BTC. Typically available in quantities ranging from 1 mBTC (+/- \$7.60) to 100 BTC (+/- \$760000) ¹⁷	USD, EUR, GBP, etc. which are further subdivided into 100 units (cents/pence).
Licensing requirements for production	Typically requires a mineral extraction licence issued by government.	Typically none although certain jurisdictions have imposed moratoriums on new commercial operations.	Production rights for physical representation are exclusive to government.
Price volatility	Moderate	Extreme	Variable depending on currency and government
Environmental impact of production process	Typically viewed as negative	Typically viewed as negative	Neutral

¹⁶ Source: <http://positivemoney.org/how-money-works/how-banks-create-money/>

¹⁷ Exchange rates prevailing on 6 June 2018

Bitcoin has so far experienced three main phases in the public eye (according to Tasca et al. 2018)¹⁸: (a) cyberlibertarian experiment (c. 2009-2012), (b) 'sin'-enterprise promoter (especially gambling, dark markets) (c. 2012-2014), (c) enabler of legitimate enterprises and a sought-after exchange asset (2015-), all the while gaining traction and adoption. Indeed, some might argue that Bitcoin already partially fulfills all three of the functions of money - medium of exchange; unit of account and store of value.

First, it is used as a medium of exchange to buy certain goods and services. Unfortunately, it is currently facing limitations with respect to this function due to high transaction costs, but by the end of 2017 more than 11,000 businesses had accepted Bitcoin as a form of payment, a figure that has grown at an average quarterly compound growth rate of around 10%.¹⁹

Second, it is used as a unit of account in its own ecosystem. Cryptocurrency exchanges list prices and analyse other coins and tokens not only in terms of dollars but also with respect to the value of a Bitcoin. However, to become widely adopted it should be accepted as a unit of account not only in its own ecosystem but by a wider global audience.

Third, and perhaps most importantly, Bitcoin fulfills the function of a store of value. Due to its finite supply, no central authority or single entity can debase the value of a Bitcoin, which is why it was so appealing to early adopters and was perceived as a wealth-preserver and believed to eventually be a wealth-expander. Its exponential growth in terms of adoption and finite supply has resulted in a lot of volatility in its value, which is currently creating a hindrance to its store of value function.

A renowned expert from the Bitcoin community states: "It is fiat money that is the greatest social experiment on the human race; Bitcoin is merely a techno-reaction to that." An interesting question that follows is: "If cryptoassets [more specifically, cryptocurrencies] are supposed to replace fiat... why do we measure their health in the exact 'means of exchange' they're trying to replace?"²⁰

Bitcoin and other cryptocurrencies have been criticised and referred to as 'Ponzi schemes' (for example by Agustin Carstens from the Bank of International Settlements and the ex-governor of the Mexican Central Bank for being a "combination of a bubble, a Ponzi scheme and an environmental disaster."), but let's note that fiat money itself has no inherent value, is still perceived by the general public as an asset to store wealth, and can in fact be modelled as a 'bubble'.

Henry Ford stated: **"Those who believe that the people are so easily led that they would permit printing presses to run off money like milk tickets do not understand them. It is the innate conservatism of the people that has kept our money good in spite of the fantastic tricks which the financiers play — and which they cover up with high technical terms. The people are on the side of sound money. They are so unalterably on the side of sound money that it is a serious question how they would regard the system under which they live, if they once knew what the initiated can do with it."** (My Life and Work, p. 179)

Finally, it is worth noting that certain problems in current financial markets are indeed very similar to challenges cryptocurrencies face. For example, what happens during financial crises, when the uncoordinated systemic money demand of the whole public results in bank runs which are not easily met by the traditional financial system, is similar to what happens in exchanges in the crypto-world. More recently, some officials have argued that regulating and understanding the realities of the current global system would be a better approach. For example, Bank of England Governor, Mark Carney stated: "A better path would be to regulate elements of the crypto-asset ecosystem to combat illicit activities, promote market integrity, and protect the safety and soundness of the financial system".²¹

¹⁸ Tasca, Paolo, Adam Hayes, and Shaowen Liu. "The evolution of the bitcoin economy: extracting and analyzing the network of payment relationships." The Journal of Risk Finance 19.2 (2018): 94-126. Available at <https://doi.org/10.1108/JRF-03-2017-0059>

¹⁹ <https://cointelegraph.com/news/bitcoin-adoption-by-businesses-in-2017>

²⁰ <https://twitter.com/boborado/status/975752100427718656>

²¹ Scottish Economics Conference at Edinburgh University in 2 March 2018



“It is fiat money that is the greatest social experiment on the human race, Bitcoin is merely a techno-reaction to that.”

Renowned Bitcoin expert

06 Challenges and Solutions

A number of challenges remain to cryptocurrencies becoming more widely adopted as a method of payment. Many of these challenges are linked to the underlying technology but also include legal, economic and social factors. The promised outcomes of DLTs may be the optimal allocation of resources and a reorganisation of society to make it more efficient; however, we are still at the early stages of their emergence and whether these systems will lead to a foundational transformation of social and economic structures is yet to be seen and will depend in the long run on how DLTs respond to the challenges we outline below. The sustainability and success of DLTs and the associated business models will require building trust, usability, transparency, and consequently legitimacy in the medium term.

a. Regulation vs reputation

Reputation and trust are particularly important in the DLT ecosystem and business models. A good reputation system employed by the network makes the system resilient to manipulation and gaming; and creates a safe environment for network participants to interact and reveal their preferences truthfully. Additionally, a firm's good reputation and its ability to ensure trust in the ecosystem determines the firm's ability to signal good quality. This is essential for attracting investors, eventually increasing user engagement and securing financial longevity. Moreover, the bad reputation of certain DLT ecosystem participants can create a negative externality for 'good' actors and prevent the overall ecosystem from growing.²² Regulation plays an important role in correcting informational asymmetries and negative externalities when a market is susceptible to potential deficiencies²³.

In the DLT context, a friendly regulatory environment plays an important role in increasing adoption,

but the global and cross-border characteristics of cryptocurrencies and DLT business models create problems for the traditional regulatory measures available to nation states. This implies the necessity of a global regulatory framework or perhaps a self-governance model in which regulation is largely replaced by good reputation mechanisms.

Currently, the regulations being defined and implemented and governance around cryptocurrencies and initial coin offerings (ICOs) vary greatly across different nations. For example, Switzerland²⁴, Gibraltar and Australia have taken a proactive and positive approach towards ICOs; Japan has legitimised Bitcoin by declaring it a legal currency, and allowed Ripple to develop an app to speed up intra-bank transactions, but China took a hard line and banned all ICOs, in addition to cryptocurrency trading and mining in 2017.²⁵

b. Privacy and trust

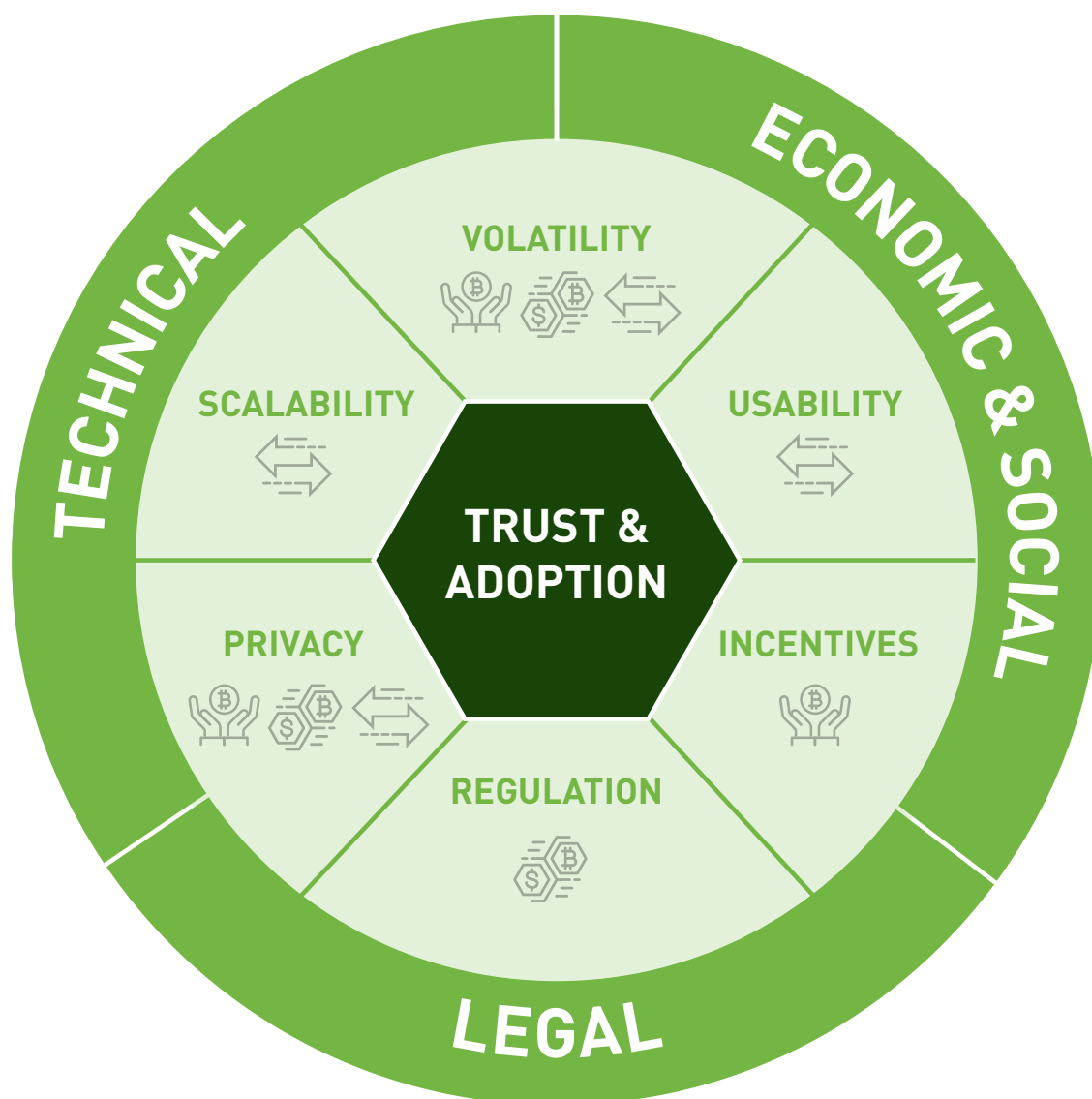
While it is intuitively appealing to use blockchains to provide a transparent single source of truth, it is often desirable for there to be different levels of privacy available to stakeholders when it comes to accessing details of specific transactions, smart contracts or personal data. This is a particular challenge for public permissionless blockchains like Bitcoin and Ethereum which expose all transactions, smart contract code and state, thus potentially enabling privacy erosion and forms of industrial espionage based on blockchain analysis. A variety of novel public permissionless blockchains have been designed to address this problem. Monero, an inherently private blockchain technology based on ring-signatures which make it difficult to definitively identify the originator of a transaction, features the concept of a 'view key', which can be used to view (but not authorise) the transactions associated with a Monero address. zCash

²² For example failed/fake ICO launches can cause problems for those that are completely legitimate and affect the credibility of solid projects.

uses the concept of a 'zero-knowledge proof', that is a logical proof that transactions are valid which does not reveal details like the sender, the receiver, or the amount of the transaction.

However, anonymity resulting from such technology may also result in concerns regarding the legal environment. A common criticism of such cryptocurrencies is that, like cash transactions, they can be easily used to fund

criminal activity due to our inability to track exchanges. Indeed, Japanese regulators are reported to be actively discouraging cryptocurrency exchanges from listing high-privacy coins such as Monero, Dash and zCash.²⁶ In some jurisdictions, however, progress is being made in the opposite direction. For example, New York state recently formally approved the trading of zCash on the Gemini cryptocurrency exchange.²⁷



- TYPE OF CHALLENGE
- CHALLENGES
- AIM

FUNCTIONS OF MONEY



Store of value



Unit of account



Medium of exchange

²³ For example, general public with no formal investment experience may be more prone to manipulation and gaming

²⁴ <https://www.ft.com/content/c2098ef6-ff84-11e7-9650-9c0ad2d7c5b5>

²⁵ <https://cointelegraph.com/news/from-gibraltar-to-australia-how-countries-approach-icos>

²⁶ See <https://themerkl.com/japans-fsa-wants-to-get-monero-dash-and-zcash-removed-from-all-domestic-exchanges/>

²⁷ See <https://dailyhodl.com/2018/06/08/crypto-breakthrough-new-york-state-approves-privacy-coin-trading/>

c. Volatility

Volatility can be both a technical and an economic challenge, and is currently a major hindrance to cryptocurrencies becoming a widely adopted payment system as it creates difficulties relating to all three functions of money, but especially the function of store of value. Even though problems faced in traditional financial systems such as 'bank runs' are relatively similar to those being faced by crypto-exchanges, the very high volatility of cryptoassets has the potential to negatively affect perceptions and hamper their use in all kinds of long-duration transactions. There have been some attempts to address the volatility issue through the creation of so-called stable-coins which are digital tokens with values intended to be pegged to those of fiat currencies. Tether (USDT) is the most well-known example. Every USDT token issued is in theory backed by a US dollar deposited with a custodian by the private company Tether Ltd. However, the financial and operational transparency of the scheme is limited and token holders must place their trust in, amongst other factors, the solvency and integrity of Tether Ltd and their custodian.

By contrast, Dai is an ERC20 stable-coin pegged to the US dollar developed by Maker (<https://makerdao.com>) which does not rely on trusted third parties. Instead, it makes use of smart contracts on the Ethereum network to issue Dai coins overcollateralised by a locked deposit of Ether (ETH). When the Dai is repaid, the Ether deposit is unlocked. An associated utility coin MKR is intended to be generated and sold as a recapitalisation mechanism in case a drop in the ETH/USD exchange rate leads to the system becoming under collateralised, although it is not clear that the system could withstand a sudden, drastic and unexpected crash in the ETH/USD exchange rate. Circle's CENTRE project (<https://centre.io>) aims to facilitate interoperability between different payment providers and stablecoins using their own fiat-collateralised tokens as a bridge.

d. Scalability

Issues relating to scalability could delay/prevent blockchain's capability to transform businesses, economics and governance (Yli-Huumo et al., 2016). Many foundational public permissionless blockchain protocols do not scale to high transaction volumes on account of being limited in terms of transaction throughput by design. This is because many of these protocols feature restrictions on block size or transaction complexity, and deliberately regulate the rate at which blocks are published (via regulation of the difficulty of the mining process) in order to control the rate at which new tokens are produced. This can lead to poor transaction response times and very high transaction fees. For example in December 2017 Bitcoin transaction fees were of the order of \$30 while in October 2017 costs of deploying even relatively straightforward smart contracts on the Ethereum network rose as high as \$48²⁸.

Entire classes of application use cases, especially those based around micropayments, are rendered economically unsound by higher transaction fees, forcing businesses based on those use cases to migrate to other technologies. One approach being explored to address this issue is the development of '(micro)payment channel' technologies which enable a virtually unlimited number of off-chain micropayment transactions between parties that agree to set up a collateralised payment channel with very low fees. Subsequently, far fewer on-chain transactions have to be made to reflect the updated state of the payment channel. The Lightning network (<https://lightning.network>) is the preeminent example of such an approach for Bitcoin, while off-chain solutions for Ethereum such as the Liquidity Network (<https://liquidity.network>) and Raiden (<https://raiden.network>) are also being developed. Others believe that the solution to the scaling problems lies in blockchain interlinking, e.g. through the use of cross-chain atomic swaps which allow parties on two different cryptocurrency blockchains to swap assets without the need for an intermediary. This is the vision of platforms such as Komodo (<https://komodoplatfrom.com>), Polkadot (<https://polkadot.network>), and Cosmos (<https://cosmos.network>), amongst others.

²⁸ See e.g. https://medium.com/@makoto_inoue/the-history-of-deploying-smart-contracts-on-ethereum-mainnet-10-times-7a4fdd5b065

e. Incentives

Incentives are crucial to sustain any economic or contractual relationship, since they induce people to act in a particular way in an economic or business situation. The design of the right incentives allows us to achieve mutual gains when parties involved in a relationship have differing goals and possess varying degrees of knowledge.

In traditional economic ecosystems, strategic interactions between network participants need to be well-managed and coordinated through use of incentive-compatible mechanisms. In other contexts, a central authority, such as a designated firm, institution or cooperative may coordinate services to the system (Cusumano & Gawer, 2002; Iansiti & Levien, 2004a; Li, 2009; Pierce, 2009, Autio & Thomas, 2018²⁹)³⁰. However, DLTs offer a new avenue for ecosystems to self manage and coordinate without the need of a central authority. In this context, the fields of game theory, mechanism design and behavioural economics are particularly useful tools and offer unique insights into designing incentives that will ensure the sustainability and growth of an ecosystem and the associated business models.

f. Usability and adoption

DLT businesses, cryptocurrencies and cryptoassets need to invest in 'design thinking' as user-friendly design is at the core of any successfully adopted technology. This facilitates the engagement of two main audiences - individual users and bigger organisations.

For adoption to grow beyond technically-savvy audiences and include a broader base of individual users, accessibility of blockchain-related technologies plays a crucial role. For example, wallet technologies that allow users to transport cryptoassets often require the understanding of highly technical concepts such as addresses and public-private key encryption.

Additionally, not only users but also operators of exchange platforms often face difficulties interacting with traditional fiat-money-based banking facilities in the process of conversion of cryptocurrencies/assets to fiat currency. Nevertheless, institutions such as banks, central banks and governmental organisations are considering adopting DLT in various contexts ranging from increasing intra-bank transaction speed and cost-effectiveness to helping ensure the transparency of overseas aid programmes.

²⁹ Autio, Erkko and Llewellyn D. W. Thomas. "Tilting the Playing Field: Towards an Endogenous Strategic Action Theory of Ecosystem Creation." World Scientific Reference on Innovation Volume 3: Open Innovation, Ecosystems and Entrepreneurship: Issues and Perspectives. Ed. Satish Nambisan. World Scientific Publishing Co. Pte. Ltd., 2018, 111-140.

³⁰ sometimes shared platforms such as eBay or Android help coordination or regulation of the ecosystem.

07 Conclusions and Conjectures

In this report, we have assessed whether cryptocurrencies can potentially transition into mainstream use and be adopted by a wider global audience, while considering the challenges faced by cryptocurrencies and the overall DLT ecosystem and business models. The wider use of cryptocurrencies is the next natural step in reducing friction in the global economy, supported by the adoption of tokens in local contexts, be they specific to geographies or industry-sectors.

An interesting question remains as to whether we will ever reach a point in which the value and health of cryptocurrencies, or cryptoassets in general, is no longer measured in terms of fiat money. This can only happen if cryptocurrencies start being used in daily transactions and evolve from their present-day use cases such as being a reserve currency which acts as insurance against political distrust, a means to preserve financial privacy and a tool to overcome capital controls. The question is now to consider the steps required for cryptocurrency to make the transition to becoming a 'real-world' payment system.

From section 5.b., it is easy to note that the concept of money itself has greatly evolved in our lifetime - from cash to plastic via the use of debit/credit cards and again through the current use of contactless payments. Despite this technological evolution, the three core functions of money have remained the same. Some cryptocurrencies are beginning to satisfy these functions; however, we find that there are technical, legal, economic and social challenges currently restricting the degree to which cryptocurrencies are fulfilling the three traditional functions of money:

- 1. Medium of exchange**
- 2. Unit of account**
- 3. Store of value**

More specifically, the 6 issues listed below and discussed in detail throughout the report, hold the key to the adoption process and improving trust:


- 1. Scalability**
- 2. Privacy**
- 3. Volatility**
- 4. Regulation**
- 5. Incentives**
- 6. Usability/Design thinking**

Trust scales very poorly in our society and one of the main purposes of cryptoassets is to make trust scale up in a world of ambiguity. Any form of money needs to be easy to transact with, easily recognisable or verifiable by users, and easy to carry for it to work well as a payment system. Many commodities that are currently utilised to store wealth are not easy to carry or transfer; Bitcoin (or a more evolved cryptocurrency) offers a new alternative.

Monetary policy is a powerful tool for national governments to achieve their economic goals and some countries will continue to pursue active monetary measures. However, the finite supply of Bitcoin can render itself as a resilient and useful alternative for economies that prefer to have a passive monetary policy³¹. Adoption of cryptocurrencies with a fixed or finite supply may be plausible for countries with vulnerable economic conditions, as many cryptocurrencies are not predisposed to issues such as hyperinflation in the way that fiat currencies are. Some governments with currencies susceptible to high volatility in traditional financial markets, who therefore prefer passive monetary policies, may indeed decide to separate themselves entirely from monetary policy tools by adopting cryptocurrencies. Potentially, we could even see bitcoinisation/ cryptonisation of certain economies, in a manner similar to dollarisation.

It is also worth noting that the potential of Blockchain and DLT goes well beyond merely creating new forms of money to compete with existing fiat currencies. This foundational technology has the potential to reshape industries, as well as disrupt traditional business models, organisational and governance structures. It encompasses designing entirely new ecosystems and allocation mechanisms based around token economics. This is a multidisciplinary mechanism design challenge that requires an understanding of technology, economics, business, finance, law, psychology, geo-politics, and history among others.

³¹ See e.g. <http://bitcoinist.com/bitcoin-ideal-countries-adopting-passive-monetary-policy/>



“Getting a global society to agree something has value and can be used as a currency without government support and without a physical form is one of the most significant accomplishments in monetary history.”

Chris Burniske and Jack Tatar, *Cryptoassets*, 2017

08 Glossary of terms³²

Bitcoin: A decentralised digital currency that uses a peer-to-peer network of nodes which jointly maintain a common tamper-resistant record of historical transactions, independent of a central authority.

Bitcoin Cash (aka Bitcoin ABC):

A cryptocurrency that resulted from a fork in the Bitcoin protocol August 2017 to allow more transactions to be processed by increasing the size of blocks.

Blockchain: A novel transaction-recording mechanism that comprises of batches of validated transactions called blocks which are chained together in a way that ensures a very high level of data integrity.

Bretton Woods System: An international monetary and exchange rate management system established in 1944, whereby participating currencies were pegged to the price of gold and US dollar acted as reserve currency linked to the price of gold. The Bretton Woods Agreement also marked the creation of the World Bank and IMF.

Cryptocurrency: A digital currency that uses cryptography for security.

Cryptoasset: Digital assets that utilise cryptography.

Cryptocommodity: Computing, storage and networking resources which power blockchain ecosystems.

Cryptoeconomics: The design of the economic incentives within a system that uses cryptography.

Cryptotoken/token: Value exchange mechanisms that allow a community, or network's participants, to access, govern and manage the system.

Distributed Ledger (Technology): An immutable database that is governed by a predetermined set of rules, consensually shared and synchronised across network spread across multiple sites, institutions or geographies.

Ethereum: A decentralised software platform first released in July 2015 that enables the deployment of smart contracts and Decentralised Applications (dApps) with a wide range of applications and an associated cryptocurrency called Ether.

EOS: A blockchain-based platform currently under development that aspires to enable the development, hosting, and execution of commercial-scale dApps.

Fiat Money: A legally-recognised medium of payment without an intrinsic value that can be used for the settlement of debts.

Fork: A divergence in the state of a blockchain caused by a disagreement amongst blockchain nodes. Can be temporary (e.g. a fork due to two miners finding competing blocks at nearly the same time) or permanent (e.g. a fork due to a subset of nodes introducing new rules for the validation of transactions).

Game Theory: The study of multi-person decision problems and resulting outcomes taking into account strategic interaction among participants given a set of rules.

Legal tender: Any official medium of payment recognized by law that can be used to extinguish a public or private debt, or meet a financial obligation.

Miner: Special blockchain nodes that build up a block of transactions they wish to publish by selecting groups of ordered transactions.

NEO: A blockchain-based platform designed to build a scalable network of dApps and associated cryptocurrency.

Node: A computer running blockchain software that is connected to a network, and which maintains a copy of a blockchain. So-called "full" nodes validate all incoming blocks and transactions. "Lightweight" nodes trust other nodes to do this on their behalf.

Satoshi: The smallest fraction of a Bitcoin that can be transacted named after the pseudonym of the Bitcoin creator.

Smart Contract: Programmed rules that are self-executed or verified by computer code.

Tokenomics: The design of the economic incentives governed by tokens in a blockchain.

Token Engineering: The theory, practice and tools to analyse, design and verify tokenised ecosystems.³³

³²We rely on our own but also definitions provided by investopedia.com, techpedia.com and dictionary.com in this section.

³³<https://blog.oceanprotocol.com/towards-a-practice-of-token-engineering-b02feeff7ca>

09 Acknowledgements

At eToro we believe we will see the tokenisation of all assets in the coming years. This is a significant, long-term change – revolution, rather than evolution – and cryptoassets are the first such asset in this transformation.

As a result, we commissioned Dr Zeynep Gurguc and Prof William Knottenbelt of Imperial College London to research the trajectory for one of the most discussed subsets of cryptoassets – cryptocurrencies – with a focus on barriers to mainstream adoption. We'd like to thank them for their valuable, insightful contribution to this debate.

The authors themselves would also like to thank Robert Learney and Ioana Surpateanu for their comments on earlier drafts of this report.

About eToro

eToro empowers people to invest on their own terms. The platform enables people to invest in the assets they want, from stocks, to cryptocurrencies to commodities. eToro is a global community of more than ten million people who share their investment strategies; and anyone can follow the approaches of those who have been the most successful. Users can easily buy, hold and sell assets, monitor their portfolio in real time, and transact whenever they want.

eToro is regulated in Europe by Cyprus Securities and Exchange Commission and regulated in the UK by the Financial Conduct Authority.

Disclaimer: The views presented in this report are those of the authors and do not necessarily represent the views of Imperial College London.