Aaro Capital

An Introduction to Crypto's near Money Characteristics

© Aaro Capital 2019. All rights reserved.

Disclaimer

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

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

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

© Aaro Capital 2019. All rights reserved.

Acknowledgements

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

© Aaro Capital 2019. All rights reserved.

Executive Summary

In this paper, we review the underlying characteristics of money. We also cover the potentially disruptive features of Bitcoin and other cryptocurrencies in the context of money.

The question about what the "value" of a good or a service is has long eluded economists. A famous inconsistency of the classic "intrinsic theory of value" is Adam Smith's water-diamond paradox: water that is necessary for life is far less expensive than diamonds, which are of no use.

In modern economics, value is disconnected from "intrinsic values" and related to prices. Subjective value in general does not depend on any "intrinsic" property and can be shaped by social and personal values, for example art, which has no use other than enjoyment from viewing it. Ultimately, market prices are driven by the balance between supply and demand. The transaction price is set such that the quantity supplied equates to that being demanded.

Money's primary purpose is to be used as a method of payment for other goods or services. In order for money to efficiently fulfil its function as a "medium of exchange", it also needs to be a "unit of account", easing the comparison of prices across markets and products, and represent a "store of value", allowing for substitution across time.

Historically, many societies around the world moved from barter to the adoption of "commodity money", whose value was underpinned by the commodity of which it was made. These days, national currencies are pure fiat money, anchored only by trust in central governments and their ability to enforce price stability. The key property of all of these past and present forms of money is trust. That means, when one exchanges a good or service for money, one has to trust that money can be converted back into goods or services of similar value in the future.

Maintaining trust in the institutions through which money is supplied has been challenging at times. Periods of stable money supply is more an exception than the norm, and trust in institutional arrangements has often failed. History has proved that money can be fragile, regardless of whether it is supplied in a competitive and decentralized manner, namely through private means, or by a sovereign, mainly through a monopolist supplier.

The quest for solid institutional arrangements for the money supply eventually generated the emergence of today's independent central banks. Central banks, as we know them today, developed as a response to the instability originated by both a decentralized process of money supply, and the interference of governments aimed at achieving fiscal goals via monetary means.

Modern independent central banks enforce price stability via "inflation targeting" rules, usually 2% for advanced economies. Independent and credible central banks have been effective in maintaining stable prices in advanced economies. However, records of central banks are more mixed in emerging economies, where independence is often challenged by political interference, weaker institutions, and more precarious macroeconomic management. These challenges are reflected in volatile currencies, high rates of inflation, and occasional bouts of hyperinflation (as recently seen in Venezuela and Zimbabwe).

Money is supplied through a joint venture between central and private banks. Central banks issue notes and coins, while commercial banks accept deposits against the payment of interest to make loans or investments. Trust in this two-tiered system is generated through independent and accountable central banks, which back reserves through their asset holdings.

© Aaro Capital 2019. All rights reserved.

Standard money measures are:

- M0, the total of all physical currency including coinage
- M1, M0 plus the amount of demand deposits, travellers checks and other checkable deposits
- M2, M1 and “close substitutes” such as savings accounts and money market accounts
- M3, M2 plus large and long-term deposits

Different forms of money have different properties in terms of liquidity and storage of value. M0 captures currency money – an efficient medium of exchange that allows for free and anonymous transactions but is exposed to inflation, which diminishes its effectiveness as a store of value. M1, M2 and M3 are less liquid but are more effective as stores of value over longer periods of time.

The role of central banks is not limited to just building trust in the financial system. It also includes making sure that the system of payments runs smoothly, and ensuring that demand shocks are absorbed efficiently by managing the supply of reserves (i.e. ensuring the supply of money is elastic and prices remain stable).

There are different types of money with their own unique set of properties. These include commodity money, representative money, commercial bank demand deposits, privately issued money, fiat money and digital money.

Cryptocurrencies aspire to become a new, more stable form of money through three key elements:

1. A computer protocol, i.e. a set of rules, specifies how the participants in the network can transact.
2. A ledger that stores information on transactions.
3. A decentralized network of participants that updates, stores and reads the ledger of transactions following rules defined by the protocol.

Advocates of cryptocurrencies maintain that, with these three key ingredients in place, a cryptocurrency is not subject to the potentially misguided incentives of sovereign and commercial banks.

The distinguishing features of cryptocurrencies are:

- They are based on cryptographic features, aspiring to prevent counterfeiting and fraudulent transactions.
- Although “created” privately, they are no one’s liability, meaning they cannot be redeemed, and their value depends on the expectation that they will continue to be accepted by others.
- They allow for peer-to-peer exchange without the need for intermediaries.

The fact that cryptocurrencies can be exchanged on a peer-to-peer basis is what distinguishes them from other forms of digital money such as bank deposits. However, similar to fiat currencies, the value of cryptocurrencies is determined by the interaction of supply and demand.

Cryptocurrencies belong to the wider space of cryptoassets. These are commonly divided into three groups: cryptocurrencies, security tokens and utility tokens. Cryptocurrencies are designed to be used as a general means of payment for goods or services. Security tokens represent an asset that exists outside the blockchain and comply with an existing legal framework. Finally, utility tokens are needed to digitally access an application or service on a distributed ledger.

Potential challenges for a wider adoption of cryptocurrencies are:

- Lack of financial infrastructure;
- Security risks;

© Aaro Capital 2019. All rights reserved.

- Government regulations;
- Price volatility.

Important factors in the potential growth of adoption of cryptocurrency are:

- Reliability and flexibility of the Distributed Ledger Technology;
- Privacy protection in the network;
- Ease of access;
- Prospect of greater stability for economically unstable countries;
- Investor appetite.

Several of the issues that cryptocurrency markets currently face, from price volatility to market manipulation, stem from the fact that they are still very new. They lack liquidity, regulation and infrastructure. Any asset in this setting would be extremely volatile.

The infrastructure supporting payments in cryptocurrencies and hybrid (crypto/fiat) is developing rapidly. This is a crucial part of the ecosystem needed to support the diffusion and adoption of cryptocurrencies. Crypto Debit Cards and Merchant Crypto Payment Systems allow for ease of payment for goods and services across platforms and various currencies/cryptocurrencies.

Regulation is an important factor for the usability and adoption of cryptocurrencies by the wider economy. One of the common misconceptions about cryptocurrencies is that, since they are borderless, they are very hard to regulate. However, it must be noted that crypto gatekeepers and storage solutions are companies which can be indeed be regulated. This combined with the transparency and immutability of dominate cryptocurrencies can lead to a level of compliance that has not been previously attainable in traditional finance.

Stablecoins are cryptocurrencies designed to reduce the volatility inherent in the price of a cryptocurrency, by linking it to a stable asset or basket of assets. Facebook's Libra is one of the most widely discussed examples of a stablecoin in recent times. Stablecoins have the potential to take a notable role in the global payment system over the medium term, especially in international remittances and e-commerce. For example, pegging to a basket of currencies may favour increased adoption in the context of international trade, where exchange rate risks can be minimised either across currencies in a given region, or against the dominant global currency – i.e. the US dollar.

Further, ease of access and low entry costs are key advantages of distributed ledger technology. Opening a bank account can be time consuming and cumbersome in the heavily regulated banking sector, whereas only a smartphone is needed to access a crypto account. These properties are likely to be important for adoption in developed economies, where exchange and transfer fees are still needlessly high in traditional banking.

The deflationary nature of standard cryptocurrencies with a finite and fixed supply curve, such as Bitcoin, makes them potentially more suited to fulfil the "store of value" function of money, rather than a "medium of exchange" or "unit of account". With this in mind, possible markets that Bitcoin could disrupt include gold and the offshore banking industry.

However, while Bitcoin fulfils the requirement of scarcity to qualify as a "store of value", this is not the sole condition for it to be one. Value is disconnected from "intrinsic values" and related to prices and subjective utility. Ultimately, the adoption of a cryptocurrency as an asset to store value depends on the public's acceptance and willingness to adopt it. Their rate of adoption is likely to vary between generations, with older generations unlikely to ever see them as a store of value and younger generations already readily accepting that virtual assets have value. It remains to be seen if the increased level of Bitcoin engagement will be maintained in the longer term.

© Aaro Capital 2019. All rights reserved.

Contents

Disclaimer i
Acknowledgements ii
Executive Summary iii
Contents vi
1 An Overview of Money 1
1.1 What is Value? 1
1.2 What is Money? 1
1.3 A Brief History of Money 2
1.4 Trust and Modern Central Banks 2
1.5 The Creation of Money 4
1.6 Modern Payment Systems 4
1.7 Types of Money 5
2 Cryptoassets 6
2.1 Types of Cryptoassets 7
2.1.1 The Regulatory Approach 7
2.1.2 The Technical Approach 8
2.2 Challenges to Monetary and Financial Stability 9
2.3 Central Bank Digital Currency 9
2.4 Comparing Money and Cryptocurrencies 10
3 Routes to Cryptocurrency Acceptance 15
3.1 Challenges and Opportunities 15
3.2 Market Infrastructure 15
3.3 Crypto Payment Systems 16
3.3.1 Crypto Debit Cards 16
3.3.2 Merchant Crypto Payment Systems 16
3.4 Regulation 16
3.4.1 Regulation of Exchanges and Wallets Providers 16
3.4.2 Market Manipulation 17
3.5 Reducing Volatility: Stablecoins 18
3.6 Ease of Access and Low Entry Costs 18
3.7 Cryptocurrencies as a Store of Value 18

© Aaro Capital 2019. All rights reserved.

1 An Overview of Money

1.1 What is Value?

The question about what the "value" of a good or a service is has long eluded economists. A famous inconsistency of the classic "intrinsic theory of value" is Adam Smith's water-diamond paradox: water that is necessary for life is far less expensive than diamonds, which are of no use.

In modern economics, value is disconnected from "intrinsic values" and related to prices. Subjective value depends on how much utility an individual, given their preferences, can derive from a good or a service, relative to other goods or services. This can depend on consumption – or delayed consumption as for an asset – but in general does not depend on any "intrinsic" property and can be shaped by social and personal values, as for example for art, which has no use other than enjoyment from viewing it. When an exchange takes place, the value the buyer and seller place on something is revealed. Value is linked to price through the mechanism of exchange in an open and competitive market that aggregates different assessments of desirability into a transaction price.

Ultimately, market prices are driven by the balance between supply and demand. The transaction price is set such that the quantity being supplied will equates to that being demanded. These quantities are derived by the (expected) marginal utility of a good, service or asset to buyers and sellers.

In modern economies, prices are generally expressed in units of some form of money – a common unit of account and exchange. Efficient markets and stable systems of payments allow for prices to act as signals, thus allowing for the aggregation and transmission of information between buyers and sellers. Hence, efficient prices incentivise everyone to coordinate and respond to changes in supply and demand, and to allocate resources where they are most needed within an economy.

1.2 What is Money?

Money is not an object. As opposed to thinking of "money" as a noun, Nobel laureate Hayek observed that: "it would be more helpful for the explanation of monetary phenomena if 'money' were an adjective describing a property which different things could possess to varying degrees".[1]

From a legal perspective, money is anything that is used widely to exchange value in transactions. Currency refers instead to "minted" forms of money – usually taking the form of coins and banknotes. A (particular) currency refers to the specific form of money that is in general use within a country.

From an economic perspective, money is any good (or verifiable record) that is generally accepted as a method of payment for other goods or services, and potentially for taxes. However, in addition to its function as a "medium of exchange", in modern economies money has two other crucial roles: it is a "unit of account", easing the comparison of prices across markets and products, and represents a "store of value", enabling users to transfer purchasing power over time. In order to fulfil these three functions in a smooth and sustainable manner, any form of money needs to carry minimal or zero costs as a medium of exchange, be a stable unit of account across time and space and be a secure store of value.

---

[1] Hayek shared the1974 Nobel Prize in Economics with Gunnar Myrdal "for their pioneering work in the theory of money and economic fluctuations and for their penetrating analysis of the interdependence of economic, social and institutional phenomena." More information can be found at: https://en.wikipedia.org/wiki/Friedrich_Hayek.

© Aaro Capital 2019. All rights reserved.

1.3 A Brief History of Money

Historically, many societies around the world moved from barter to the adoption of "commodity money", whose value was underpinned by the commodity of which it was made. Commodity money emerged from barter when a specific good was agreed as a common unit of measure against others. Indeed, barter presents several difficulties. Firstly, both participants in a transaction need to want to trade specific goods over the same timeframe (i.e. a "coincidence of wants"). Secondly, in the absence of a standard unit of account, they need to mutually agree on the values of the goods. Finally, goods may not be divisible, making an exchange difficult.

Many different commodities have been used as money – such as metals and grains. Further items, which have limited use outside of storing and exchanging value, have also been used as commodity money. Examples of other goods that have also been thought of as having value due to their relative scarcity include metal objects, conch shells, feathers and gem stones.[2] Metals – and especially naturally scarce precious metals such as gold or silver – have often been adopted as units of account since they are durable, portable, and easily divisible.

The key property of all of these past and present forms of money is trust. That means, when one exchanges a good or service for money, one has to trust that money can be converted back into goods or services of similar value in the future.

Kings and rulers of the ancient Mediterranean and Middle East are likely to have been among the first in officially setting standards for money. The emergence of standardised metal coinage provided citizens and traders with trusted and stable means of exchange and unit of account, that could also be stored and saved for future exchanges. This system of coined metal money persists today in the coins we carry in our pockets.

Commodity money eventually evolved into a system of representative paper money first guaranteed by private banks against redeemable deposits, and then by national central banks. By the beginning of the 20th century, most countries had adopted the "gold standard", backing their legal tender notes with fixed amounts of gold. The international system was stabilised after WWII at the Bretton Woods Conference, when most countries adopted fiat money and fixed systems of exchange rates against the U.S. dollar that was, in turn, anchored to gold.

Over time, the expansion of economic activity required more convenient forms of money that could respond to increasing demand, be efficiently used in the trade of goods and services and have a stable value. This was not possible in such a fixed rate system.

In 1971, the U.S. government therefore suspended the convertibility of the U.S. dollar into gold. The national currencies across the globe became pure fiat money, untethered from gold and any commodity, and anchored only by trust in central governments and their ability to enforce acceptance and stability of currencies over time.

1.4 Trust and Modern Central Banks

Maintaining trust in the institutions through which money is supplied has been challenging at times. Periods of stable money supply are more an exception than the norm, and the trust in institutional arrangements has often failed. History has proved that money can be fragile, regardless of whether it is supplied in a competitive and decentralized manner, namely through private means, or by a sovereign, mainly through a monopolist supplier.

The quest for solid institutional arrangements for the money supply eventually generated the emergence of today's independent central banks. Central banks, as we know them today, developed as a response to the

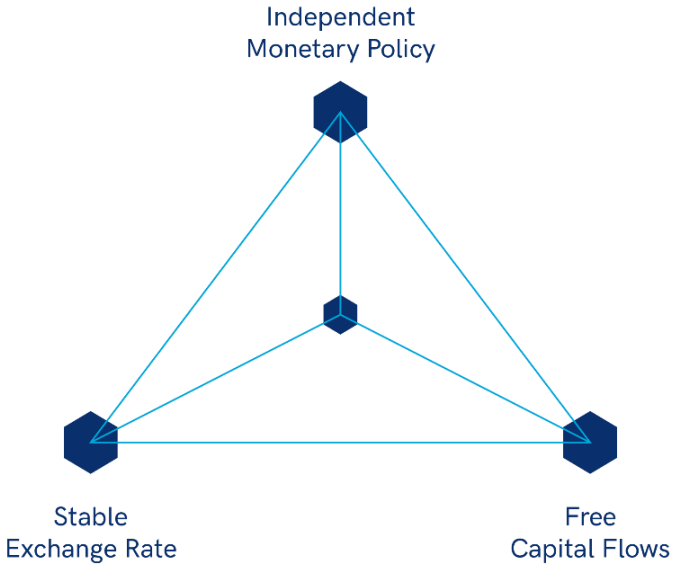
[2] An interesting read on the origins of money can be found at: https://nakamotoinstitute.org/shelling-out/.

© Aaro Capital 2019. All rights reserved.

instability originated by both a decentralized process of money supply, and the interference governments aimed at achieving fiscal goals via monetary means. Modern independent central banks enforce price stability via "inflation targeting" rules. A nominal interest rate is set by central banks to respond to changes in inflation (and other economic conditions), with the aim of ensuring that a target inflation rate is achieved, usually 2% for advanced economies. Central banks sometimes also have other macroeconomic targets. A credible inflation target guarantees prices stability over time but also preserves the function of money as a store of value, since savers can claim bank interest payments against a stable and expected inflation rate. As inflation rates are predictable and small, lenders and borrowers are able to take inflation expectations into account when drawing up contracts with a low margin of error. This limits unintended wealth transfers due to inflation.[3]

It is generally accepted that independent monetary policy can enforce stable prices and free capital flows (but not a stable exchange rate). Alternatively, a central bank can pursue stable exchange rate and free capital flows (but not an independent monetary policy), or a stable exchange rate and independent monetary policy (but no free capital flows). This is known as the trilemma or "impossible trinity".

Figure 1: The Impossible Trinity faced by Central Banks



Source: Aaro Capital Research

Independent and credible central banks have been effective in maintaining stable prices in advanced economies, even through the last financial crisis and the Great Recession.[4] However, records of central banks are more mixed in emerging economies, where independence is often challenged by political interference, weaker institutions, and more precarious macroeconomic management. These challenges are reflected in volatile currencies, high rates of inflation, and occasional bouts of hyperinflation (as recently seen in Venezuela and Zimbabwe).

---

[3] Low and stable inflation with inflation targeting prevents borrowers from inflating away their debts.

[4] In the wake of the last Financial Crisis, inflation rates in advanced economies have been stubbornly below target despite unconventional monetary policy measures such as forward guidance and quantitative easing. At the same time, the prolonged ultra-low interest rates implemented by Central Banks since the Financial Crisis have deteriorated pension fund and corporate pension scheme balance sheets, as their future liabilities have lower discounted rates. This has also had implications for savers who have longer-term savings in cash.

© Aaro Capital 2019. All rights reserved.

1.5 The Creation of Money

In almost all modern economies, money is supplied through a joint venture between central and private banks. Commercial banks accept deposits against the payment of interest and make loans or investments, while holding reserves at least equal to a mandated fraction of the bank's deposit liabilities. Reserves are held as liquid assets or currency in the bank, or as balances in the bank's accounts at the central bank.

Deposits in private banks are the ultimate means of payment between individuals, while central bank reserves are the means of payment between banks. Trust in this two-tiered system is generated through independent and accountable central banks, which back reserves through their asset holdings. In turn, trust in bank deposits is generated through a variety of means, including supervision and deposit insurance schemes as well as government regulation protecting depositors.

The money supply (or money stock) is the total value of monetary assets available in an economy at a specific time. Standard measures are:

- M0, the total of all physical currency including coinage. This is sometimes referred to as the “monetary base”, or “narrow money”.
- M1, M0 outside of the private banking system, plus the amount of demand deposits, travellers checks and other checkable deposits. Bank reserves are not included in M1.
- M2, M1 and “close substitutes”, that is M1 plus savings accounts, money market accounts, retail money market mutual funds, and small denomination time deposits.
- M3, M2 plus large and long-term deposits.

Different forms of money have different properties in terms of liquidity and storage of value. M0 captures currency money – an efficient medium of exchange that allows for free and anonymous transactions but is exposed to inflation which diminishes its effectiveness as a store of value. M1, M2 and M3 are less liquid, but more effective as stores of value over longer periods of time.

1.6 Modern Payment Systems

The role of central banks is not limited to just building trust in the financial system. It also includes making sure that the system of payments runs smoothly and ensures that economic shocks are absorbed efficiently and liquidity in the system does not dry up.[5]

Users not only need to trust money itself, but also that a payment will take place promptly and smoothly. Thanks to the direct involvement of central banks, in major economies payment systems run effectively and have achieved both scalability and safety. Safety and scalability are of particular importance as today’s economies are increasingly cashless and involves increasing volumes of trade.

A desirable property of a modern payment system is thus the certainty of transaction - that a payment correctly takes place or can be contested if it has been incorrectly executed. Hence, the system needs to be largely free

[5] For example, during the last financial crisis in 2007-2009, the Federal Reserve responded to the liquidity crisis hit the financial system injecting more than $500 billion to depository institutions that were in sound financial condition via the discount window’s primary credit program and the term auction facility. See https://www.clevelandfed.org/en/newsroom-and-events/publications/economic-commentary/2016-economic-commentaries/ec-201602-central-bank-lending-in-a-liquidity-crisis.aspx

© Aaro Capital 2019. All rights reserved.

of fraud and operational risk, both at aggregate and individual transaction levels. Strong regulatory oversight of central bank accountability helps support both the certainty and safety of transactions, and therefore trust.

Nowadays, most transactions occur through means of payment which are either directly or indirectly supported by central banks. Such means can be differentiated based on the issuer, the form, and their degree of accessibility. The issuer can be either a central or commercial bank, and its form can be physical or digital. It can be narrowly accessible, such as central bank reserves, or widely so, such as commercial bank deposits. The transfer mechanism can either be peer-to-peer (via cash) or through an intermediary, such as traditional deposits.

1.7 Types of Money

Most payment systems are currently based on fiat, nationally issued money. However, different forms of money coexist or have coexisted:

- **Commodity money** has been the prevalent form of money for a long time – first in the form of conch shells, barley, beads etc., and then as precious metals such as gold or silver. The value of the money comes from the commodity out of which it is made and can therefore fluctuate and be unstable over time.
- **Representative money** is money that consists of token coins, paper money or other record of accounts such as certificates, that can be exchanged against a fixed amount of a designated commodity (e.g. gold or silver). Hence, it differs from fiat money in that its face value can be redeemed against a specific good.
- **Demand deposits**, bank money or scriptural money are funds held in “demand deposit” accounts in commercial banks. These balances can be withdrawn at any time by check or cash withdrawal, and hence are claims against financial institutions that can be used for the purchase of goods and services.
- A **private currency** is a currency issued by a private entity, be it an individual, a commercial business, a non-profit or decentralized common enterprise. In the past, states, municipalities, private banks, railroad and other private companies have issued private currencies. If an issuer goes bankrupt the notes may be irredeemable. Private currencies were very common in the U.S. in the “Free Banking Era”, when banks were free to issue their own paper currency. These notes were a promise by the bank to pay on demand a specified amount of gold or silver currency, called “specie”. A typical requirement was for the free bank to deposit with the state banking authority one dollar’s worth of eligible bonds for each dollar’s worth of banknotes. The average lifespan for these banks was a mere 5 years.[6]
- **Fiat money** is the modern form of money. It is a currency without intrinsic value that cannot be redeemed against any good and is usually established via government regulation. Fiat money is managed by a central bank that can create new money and expand the money supply by purchasing financial assets, and that sets the policy rate at which it lends money to financial institutions. In a fractional reserve banking system, commercial banks can effectively create money by borrowing from the central bank to make loans, while holding only a fraction of central bank’s money as reserves. Money creation by commercial banks via loans is limited by capital adequacy ratios and required reserve ratios.
- **Digital money** is a form in which several different types of money can exist. For example, the money transferred between central banks and commercial banks is in electronic form, as well as most deposited money, which exists as digital currency in bank databases. Non-national digital currencies were attempted in the 1990s, but the first successful attempt was in the late 2000s. Bitcoin introduced the concept of a global, decentralised digital money in 2009.

[6] J. Lawrence Broz; The International Origins of the Federal Reserve System Cornell University Press. 1997.

© Aaro Capital 2019. All rights reserved.

2 Cryptoassets

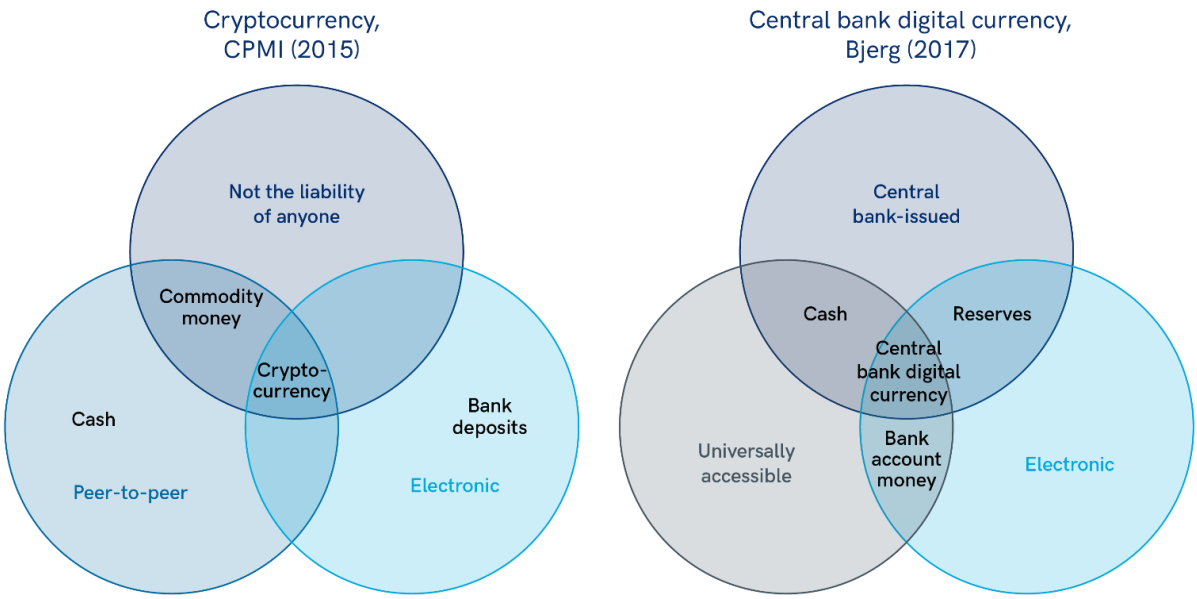
Cryptocurrencies aspire to become a new, more stable form of digital money through three key elements:

1. A computer protocol, i.e. a set of rules, specifies how the participants in the network can transact.
2. A ledger that stores transaction information.[7]
3. A decentralized network of participants that updates, stores and reads the ledger of transactions following rules defined by the protocol.

Advocates of cryptocurrencies maintain that, with these three key ingredients in place, a cryptocurrency is not subject to the potentially misguided incentives of sovereign and commercial banks.

As compared to other form of money, there are three key distinguishing features of cryptocurrencies (see Figure 2). First, they are based on cryptographic features that are designed to prevent counterfeiting and fraudulent transactions.[8] Second, although "created" privately, they are no one's liability, meaning they cannot be redeemed, and their value depends on the expectation that they will continue to be accepted by others. Finally, they allow for peer-to-peer exchange without the need of intermediaries.

Figure 2: Types of Money



Source: Bech, Garratt, "Central bank cryptocurrencies" (BIS Quarterly Review, September 2017).

The fact that cryptocurrencies can be exchanged on a peer-to-peer basis is what distinguishes them from other forms of digital money such as bank deposits. Indeed, unlike bank deposits, cryptocurrencies can be exchanged in a fully decentralized and distributed manner without the need of a third-party clearing institution to execute the exchange.

[7] Other types of data can typically be stored on public ledgers such as bitcoin.
[8] Fraudulent transactions can still be made if the fraudster has access to the private keys, but it is not possible to create an indistinguishable counterfeit of an asset secured on a distributed ledger unless the ledger has been compromised

© Aaro Capital 2019. All rights reserved.

Similar to fiat currencies, the value of cryptocurrencies is determined by the interaction of supply and demand. Unlike traditional currencies, they are neither backed by any central authority nor managed by a central bank. However, that does not imply the impossibility of implementing forms of monetary policy. In fact, monetary policy in the cryptocurrency space refers to the management of the coin/token supply by the underlying protocol, which can be fixed, expansionary, subject to a decay function or potentially more complex feedback rules. For example, Bitcoin has often been compared to gold as it has a finite supply (21 million coins) and needs to be "mined".

2.1 Types of Cryptoassets

The nature of cryptoassets is often misunderstood and overly generalised. The tendency is to define any cryptoasset as an alternative payment method, whereby it is used as a means of payment for a good or service. However, such classification is imperfect to say the least.

2.1.1 The Regulatory Approach

Different national regulators use differing terminologies and definitions. The following outlines the common understanding of these terms by the digital asset industry and the general public.

We can distinguish between three broad categories of cryptoassets: cryptocurrencies, security tokens and utility tokens. All require a distributed ledger to exist. At the time of writing, stablecoins are the only type that does not fit clearly in one of these categories (see section 3.5).

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

Security tokens represent assets that exists outside of the distributed ledger, generally within a legal framework / jurisdiction, either implicitly or explicitly. For instance, this can be stakes in a company, debt, bonds, a share in a fund, or a share in future company earnings. In the USA, the Howey's test is used to determine whether a cryptoasset is a security.[9] In the UK, security tokens are cryptoassets that have the characteristics of a Specified Investment. In Switzerland, FINMA defines asset tokens as cryptoassets that represent a claim on the issuer. Such tokens fall within the perimeter of the regulator of the jurisdiction, and often within the perimeter of the regulator of each market in which the security token is offered for sale. This holds true even if the issuer of the instrument does not explicitly refer to the jurisdiction, intentionally or not.

Utility tokens are used to digitally access (or provide) an application or a service. In the crypto industry, this term has been widely used to include tokens that meet the definition of a security token. The token is sold early on, and investors hope that, when service demand increases, the token price will rise. The regulators' definitions differ as they specifically exclude any such type of financial reward. In the UK, this includes either current or

[9] In 1946, the Supreme Court decision on the case "SEC vs Howey" created the basis for the commonly applied Howey Test which is used to determine whether a transaction is an investment contract or not. A transaction will be called an investment contract if it fulfils the following criteria: (1) It is an investment of money; (2) The investment is in a common enterprise; (3) There is an expectation of profit either from the work of the promoters or the third party. Federal courts have accepted the definition of "common enterprise" as an enterprise by which the investors pool in their money and assets to invest in a project.

© Aaro Capital 2019. All rights reserved.

prospective products, as long as the utility token does not give rights similar to security tokens above. In the USA, the SEC, as of 2019, seems to restrict utility tokens as giving access to a service already available. In Switzerland, the FINMA considers that a token can be in more than one category (i.e. a hybrid token).

2.1.2 The Technical Approach

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

Cryptocurrencies have the same meaning as above. Those who help to maintain and update the distributed ledger are rewarded by the issuance of new cryptocurrency upon the creation of each block. It is the protocol layer itself that sets the rules of issuance and allocation of the cryptocurrencies.

In contrast, tokens are issued by users on a blockchain. They are created using a specific private key, known only to the issuer of the token. What they represent is not set by the network protocol itself. Instead, it is set partly through user defined logic on-chain (so called smart contracts) and partly to services or value provided outside the distributed ledger (i.e. security tokens or utility tokens). On ZCash, user created tokens are called “User Defined Assets” (UDAs). On Bitcoin, “Colored Coins”. On Ethereum, most tokens are created using an ERC20 standard compatible smart contract.

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

Table 1: Cryptoasset Classification Frameworks

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

Source: Aaro Capital Research

© Aaro Capital 2019. All rights reserved.

2.2 Challenges to Monetary and Financial Stability

Cryptocurrencies present risks to the mandates of central banks across several areas – monetary policy, price stability, financial stability and the smooth operation of payment systems.[10]

"Currency competition" produced by cryptocurrencies could create risks to price stability by limiting, or completely driving out, government currencies. Currency competition can succeed in calming inflation and preventing the manipulation of interest rates and prices often practised by governments (Benigno, 2019).[11] However, in more extreme scenarios, it would result in central banks being unable to enforce price stability by setting short term interest rates. This could also present a great deal of risk during a liquidity crisis, as central banks often act as "lenders of the last resort" to satisfy emergency liquidity needs - a role unlikely to be assumed by any cryptocurrency protocol.

A second risk comes in the form of financial instability, should cryptocurrencies become more widely adopted and linked to the real economy via financial and fintech businesses. In such a case, cryptocurrency bubbles would pose a real threat to systemic stability, as would be the case with any other large asset class.

Finally, cryptocurrencies may create risks to the smooth running of payment systems. Users of cryptocurrencies participate directly in payment systems that are not supported by financial institutions and ultimately central banks. Hence, users face direct payment system risks (e.g. credit, liquidity, operational and legal risk), that cannot be mitigated by central banks in the case of disruption.

Given the nascent stage of crypto market development, most central banks in advanced economies estimate negligible risks to monetary and financial stability. For example, the Bank of England Financial Policy Committee in 2018 concluded that cryptocurrencies "do not currently pose a risk to monetary or financial stability in the UK. However, cryptoassets do pose risks to investors and anyone buying cryptoassets should be prepared to lose all their money."[12]

2.3 Central Bank Digital Currency

Several central banks have started experimenting with new forms of digital currencies, supported by distributed ledger technology.[13] Central Bank Digital Currencies (CBDCs) are defined as electronic forms of central bank money that can be exchanged in a decentralised manner (i.e. peer-to-peer). This distinguishes them from other existing forms of electronic central bank money, such as reserves, which are exchanged in a centralised fashion (see Figure 2 above).

Two forms of CBDCs are possible:

1. A consumer-facing payment instrument for retail transactions;

---

10 ECB, Virtual currency schemes – A further analysis https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

11 https://voxeu.org/article/monetary-policy-world-cryptocurrencies.

12 Financial Policy Committee statement from its meeting, 12 March 2018, https://www.bankofengland.co.uk/statement/fpc/2018/financial-policy-committee-statement-march-2018.

13 See discussion in Bech and Garratt, "Central Bank Cryptocurrencies" (BIS Quarterly Review, September 2017), and also Fatás, Weder di Mauro, "Cryptocurrencies' Challenge to Central Banks" (https://voxeu.org/article/cryptocurrencies-challenge-central-banks).

© Aaro Capital 2019. All rights reserved.

2. A restricted-access, digital settlement token for wholesale payment applications only.

For the consumer-facing type, the technology has the potential to provide anonymity features similar to those of cash but in digital form. If anonymity is not seen as important, then most of the benefits of a retail CBDC could be achieved by giving the public access to accounts at the central bank.

Wholesale payments today do not offer cash-like anonymity and are visible to the central operator. Hence, the case for wholesale CBDCs depends on their ability to improve efficiency and reduce settlement costs. Some central banks (for example Bank of Canada) have experimented with wholesale CBDC, but none have announced yet that they are ready to adopt this technology.

2.4 Comparing Money and Cryptocurrencies

Different forms of money offer different advantages and disadvantages for the financial system and its users. Table 2 below compares different forms of money from a user utility perspective.

Government banknotes are defined by their physical and bearer nature. This make them free and easy for everyday transactions, permissionless to access, usable 24/7, and ensures user privacy. However, its physical nature means that storage requires a physical location, it is inconvenient for large or long-distance transactions, and it does not allow for online transactions.

Electronic money held in bank accounts is defined by its electronic form, removing the need for transportation. It allows users to pay for online transactions and is better suited for large or long-distance payments compared to cash. This however comes at the cost of user freedom. Those who are highly dependent on the financial system do not have payment confidentiality, may have payment time restrictions and suffer from longer payment processing time, though this is an issue more often faced by merchants than individual users.

Gold is very much limited by its physical nature, making it hard to use in transactions and in most cases is reliant on an expensive custodian. One can hold gold directly to remove intermediaries, but this would entail risks.

The defining features of Bitcoin are that users do not need to rely on third parties for storage and usage, and it cannot easily be confiscated or stolen given that it is cryptographically secured rather than in a physical location. It is also open to all and viable for all transaction sizes and distances. On the flip side, it suffers from being an early stage technology with low liquidity, high price volatility and low acceptance.

Table 2: User Utility from Different Types of Money

	Government Bank Notes	Government Electronic Money	Gold	Bitcoin
Storage	Expensive, requires secure physical location. Can be held directly or delegated to a custodian.	Inexpensive, relies on the bank not defaulting. Requires delegation to a custodian.	Expensive, requires secure physical location. Can be held directly or delegated to a custodian.	Inexpensive, relies on secret storage of private key, either on electronic device or paper. Can be held directly or delegated to a custodian. Current storage solutions are imperfect for large amounts.

© Aaro Capital 2019. All rights reserved.

Security of Storage	Dependent of physical location of storage	Dependent on the custodian's infrastructure	Dependent on the custodian's infrastructure	Dependent on user's setup or custodian's infrastructure
Durability	Dependent on storage conditions	Dependent on institutions underpinning it	High	Dependent on the network underpinning it
Unit of Trade	E.g. USD, EUR, GBP. Orders placed in currency pairs on the forex market.	E.g. USD, EUR, GBP. Orders placed in currency pairs on the liquid forex market.	Priced per troy ounce (31 g). Markets are less liquid than forex markets.	Priced per BTC, can be almost indefinitely divided. Order placed on exchange or OTC.
Payment Acceptance	High	High	Low	Low, but crypto debit cards remove need for payment acceptance
Fungibility	High	Medium	High	Medium (due to its transparent history)
Confidentiality of Transactions	High	Medium	Can be high	Pseudonymous
Traceability	Low	High	Low	High
Unit Transaction Cost	Free	Low (fees often charged to venders)	Low	Low
Transaction Settling Time	Instant	Hours to days	Days	Approx. 1 hour (or instant on the lightning network)
Ease of Payment for Micro Transactions	High	Low, fees can prevent micro-transactions being viable	Low	High via Lighting Network
Ease of Payment for Large Transactions	Low	Medium	Low	High

© Aaro Capital 2019. All rights reserved.

Ease of Payment over Large Distances	Low	Medium	Low	High
Censorship Resistant	Yes	No	Yes	Yes
Online Transactions	No	Yes	No	Yes
24/7 Usage	Yes	Out-of-hours and limited weekend usage. Possible downtime as systems upgraded.	Limited out-of-hours and weekend usage	Yes
Rely on Intermediaries to Process Transactions	No	Yes	Usually	No
Price Volatility	Variable by currency and government.	Variable by currency and government.	Medium	High

Source: Aaro Capital Research, Imperial College London[14], Bitmex[15]

Table 3 below compares different forms of money from a macro perspective.

Banknotes are a form of money that central banks have direct control over. It fulfils the role of money within a given country but is not Know Your Customer and Anti-Money Laundering compliant.

Electronic money that, for example, can be created by a commercial bank when crediting a loan in a current account, is managed by the central bank via price incentives (i.e. policy interest rates) and regulatory limits. Central banks in advanced economies must carefully manage their policy tools to achieve price stability while allowing money supply to adjust to absorb demand and supply shocks.

Gold has an inelastic supply curve making its price much more volatile. It has limited usability as a general form of money, beyond a longer-term store of value. It is also not necessarily Know Your Customer and Anti-money Laundering compliant.

Bitcoin supply is currently totally inelastic. This, together with limited supporting infrastructure, very much limits its current usability as money. Saying that, there are currently many interesting developments which may aid

[14] https://www.imperial.ac.uk/media/imperial-college/research-centres-and-groups/ic3re/CRYPTOCURRENCIES--OVERCOMING-BARRIERS-TO-TRUST-AND-ADOPTION.pdf.
[15] https://blog.bitmex.com/wp-content/uploads/2018/05/2018.05.30-Bitcoin-economics.pdf.

© Aaro Capital 2019. All rights reserved.

Bitcoin's usability as a form of money.[16] In terms of Know Your Customer and Anti-Money Laundering, once key parties in the ecosystem become compliant, so does the underlying asset.

Table 3: Macro Comparison of Different Types of Money

	Government Bank Notes	Government Electronic Money	Gold	Bitcoin
Production Mechanism	Issued by central banks following central bank limits	Issued by commercial banks following central bank limits	Mineral mining using physical extraction and processing	Digital block mining
Maximum Supply	Unlimited, USD had an average 3.26% inflation rate from 1914 to 2019.	Unlimited, USD had an average 3.26% inflation rate from 1914 to 2019.	Finite but unknown, annual production has been ~1.5% for the past 100 years.	21 million units, current inflation rate of 3-4% and will drop down to 1.8% in 2020.
Supply Elasticity	Yes	Yes, and a good mechanism to match supply with demand	Limited	No
Store of Value	Yes in most countries	Yes in most countries	Yes but has some volatility	To be determined, highly volatile at the moment
Medium of Exchange	Yes within a given country	Yes within a given country	No	Limited
Unit of Account	Yes	Yes	No	No
Price Stability During Exogenous Shocks	Supply elasticity means that it can absorb economic shocks	Supply elasticity means that it can absorb economic shocks, but stressing the system can cause rapid unwinding of leverage	No	No
KYC/AML compliance	Low	High	Medium	Once fiat on- and off-ramps are compliant, compliance is extremely high

Source: Aaro Capital Research, Imperial College London[17], Bitmex[18]

[16] This includes the development of crypto microlending companies, which can increase circulating supply when demand increases.

[17] https://www.imperial.ac.uk/media/imperial-college/research-centres-and-groups/ic3re/CRYPTOCURRENCIES--OVERCOMING-BARRIERS-TO-TRUST-AND-ADOPTION.pdf.

[18] https://blog.bitmex.com/wp-content/uploads/2018/05/2018.05.30-Bitcoin-economics.pdf.

© Aaro Capital 2019. All rights reserved.

An important characteristic of Bitcoin (and several other cryptocurrencies) is its fixed supply curve. This makes it an intrinsically deflationary currency and means that the price of goods in Bitcoin should decrease over time due to its scarcity relative to an expanding economy. In modern economic thinking, this is a highly undesirable quality for a currency – precisely the reason why central banks in advanced economies target low inflation rates at or below 2%. There are two major issues of a deflationary currency. First, it restricts its function as a medium of exchange as users tend to hoard it for investment purposes, having a negative impact on the economy.[19] Second, deflation increases the value of debt in real terms over time, putting a strain on individuals. This may amplify recessions by making harder than necessary to deleverage during market downturns.

A final point that is worth considering is that cryptocurrencies are global by their very nature – they are not linked to any national economy. While this may encourage many to dream of the birth of a decentralised and universally adopted global currency, in practice this is highly unlikely. Economic theory tells us that for an economic region to be an optimal currency area[20] – i.e. for a common currency to maximize economic efficiency in the region – at least four criteria have to be fulfilled: (i) labour mobility; (ii) a risk sharing system possibly in the form of fiscal transfers; (iii) synchronised business cycles; (iv) capital mobility and price flexibility across the region. These four criteria guarantee that economies in the region expand and contract together, thus creating scope for a common monetary policy. They also ensure that when asymmetric shocks happen, the system is able to re-equilibrate itself by the action of market forces and fiscal risk sharing, without the need of exchange rate devaluation. The difficulties experienced in the Euro Area during the last financial crisis are a clear example of the tensions that can appear when these criteria are not fully met. In light of these observations, it seems unlikely that any global currency will supersede national/regional currencies.

[19] https://www.bloomberg.com/news/articles/2018-03-29/the-ancient-history-of-bitcoin.
[20] Mundell, R. A. (1961). "A Theory of Optimum Currency Areas". American Economic Review. 51 (4): 657–665.

© Aaro Capital 2019. All rights reserved.

3 Routes to Cryptocurrency Acceptance

Cryptocurrencies captured widespread attention after displaying significant, rapid growth in 2017. It is therefore only natural to ask whether they can become an accepted means of payment or store of value in the near future.

It is important to note that this is a very early stage technology with little of the supporting infrastructure in place for which it requires to become a universally adopted mean of exchange. Further, one should not make the mistake of predicting how Bitcoin may function within an economy that is 100% Bitcoin-based. However, a generally accepted scenario is one in which digital currencies complement and compete with the existing sovereign fiat currencies.

3.1 Challenges and Opportunities

From an economic perspective, cryptocurrencies currently do not fully meet the three functions of money defined in economic literature: (i) medium of exchange (ii) store of value, and (iii) unit of account.

At the moment, cryptocurrencies have limited function as a medium of exchange due to their very low level of acceptance amongst the public. The high volatility of their exchange rates to currencies also hamper their role as a store of value. These two properties make them unsuitable as a unit of account.

Indeed, potential challenges for a wider adoption of cryptocurrencies are:

- Lack of financial infrastructure;
- Security risks;
- Government regulations;
- Price volatility.

However, the growing interest in cryptocurrencies and growing size of the industry are potentially indicators of longer-term trends. Important factors in the potential growth of adoption of cryptocurrency are:

- Reliability and flexibility of the Distributed Ledger Technology;
- Privacy protection in the network;
- Ease of access;
- Prospect of greater stability for economically unstable countries;
- Investor appetite.

In the following sections, we discuss some of the challenges and opportunities in the cryptocurrency space.

3.2 Market Infrastructure

Several of the issues that cryptocurrency markets currently face, from price volatility to market manipulation stem from the fact that they are still very new. They lack liquidity, regulation, infrastructure and established valuation models.

Financial institutions are not yet fully engaged, and therefore the optimal allocation of funds to the best crypto use cases is still lacking. Basic financial infrastructure is absent, such as depositories and institutional-grade exchange trading. Currently, the cryptocurrency market is highly fragmented, with many exchanges not always offering the best execution price. Moreover, there is geographical segmentation, as investors are not necessarily

© Aaro Capital 2019. All rights reserved.

allowed to transfer funds between exchanges of different jurisdictions. Any new asset with a level of infrastructure as basic as this would be volatile and inefficient.[21]

However, given time and as adoption grows, cryptocurrencies can become more mainstream and settle prices in a much more efficient manner. This would lead to higher liquidity within the market and a continued decline in volatility.[22]

3.3 Crypto Payment Systems

The ecosystem supporting payments in cryptocurrencies and hybrid (crypto/fiat) is developing rapidly in a number of exciting directions. This is a crucial part of the infrastructure needed to support the diffusion and adoption of cryptocurrencies.

3.3.1 Crypto Debit Cards

Several Fintech companies have created debit cards linked to flexible crypto wallets/fiat accounts.[23] These allow for ease of payment for goods and services across platforms and in various currencies/cryptocurrencies. The cards instantly exchange the currency chosen by the buyer into the currency choses by the seller at close to market rates. This removes the need for double coincidence of wants and overcomes the “chicken and egg” issue which forms the largest hurdle faced by any emerging medium of exchange.[24]

3.3.2 Merchant Crypto Payment Systems

Card payment systems also allow for merchants to accept crypto payments and then instantly convert to their chosen currency (or fraction of the payment to their chosen currency).[25] This again helps solve the double coincidence of wants issue faced by mediums of exchange.

3.4 Regulation

Regulation is an important factor required for the usability and adoption of cryptocurrencies by the wider economy. One of the common misconceptions about cryptocurrencies is that, since they are borderless, they are very hard to regulate. However, it must be noted that crypto gatekeepers and storage solutions providers are companies which can indeed be regulated. This, combined with the transparency and immutability of dominate cryptocurrencies, can lead to a level of compliance that has not been previously attainable in traditional finance.[26]

3.4.1 Regulation of Exchanges and Wallets Providers

A recent example of a regulatory effort are the Financial Services Agency of Japan’s guidelines on cryptoassets that aim to strengthen the protection of crypto exchanges against hacking.[27] One requirement is that exchanges

---

[21] The lack of established valuation models is also a major driver behind the volatility of this asset class.
[22] For more analysis on the decline of volatility, see: https://coinmetrics.substack.com.
[23] Examples of crypto debit cards include: https://www.crypto.com/, https://www.coinbase.com/card, https://tenx.tech/en/.
[24] However, this change of currency does undermine the medium of exchange function of a cryptocurrency in the short run.
[25] Examples of crypto payment systems include: https://bitpay.com/, https://commerce.coinbase.com/, https://flexa.network/, https://elipay.com/business.
[26] There are privacy cryptocurrencies such as Monaro which are not compliance friendly.
[27] For more information on the regulatory guidelines currently present in Japan, see: https://www.loc.gov/law/help/cryptocurrency/japan.php#_ftnref12.

© Aaro Capital 2019. All rights reserved.

should have sufficient funds in order to repay investors in the case of hacking. Another meaningful measure is to force companies that run crypto exchanges to be registered.

There are also efforts to regulate wallet providers, in order to prevent money laundering but also to protect the consumers who use them. A recent report by the European Banking Authority advises the European Commission on the regulatory steps that need to be undertaken with respect to cryptoassets, wallet providers and crypto exchanges.[28] The result is that several crypto exchanges and wallet providers are now already compliant in terms of Know Your Customer and Anti-Money Laundering standards. Regulators have already started to prosecute crypto exchanges that do not comply, for example the U.S. Securities and Exchange Commission against the founders of EtherDelta.[29]

3.4.2 Market Manipulation

The relative immaturity, lack of depth, and pseudonymity of the cryptocurrency market have provided a fertile ground for malicious participants, who try to manipulate prices and, in the process, generate large profits. The most common way of achieving this is through "Pump-and-Dump" schemes.

A Pump-and-Dump scheme involves a group that usually organises itself through Telegram, which provides encrypted messaging services. The organiser informs the inner group about the timing of the attack, the exact coin that should be traded, and the crypto exchanges where it will take place. All participants prepare by depositing sufficient funds and ensuring that they are able to perform numerous transactions in a short period of time, often involving bots. A few seconds before the attack, the name of the coin is announced, and the pumping stage begins. The participants buy and hold the coin, thus artificially inflating its price. A few minutes later, the first decline of the price is observed, providing the signal for all members of the inner circle to start dumping. Although the organisers will reap most of the profits, other traders are willing to participate, because they believe that they can find "greater fools", who will buy at artificially higher prices.

These schemes typically last only for a few minutes, as compared to months for Pump-and-Dump schemes in more traditional markets, such as the stock market. Moreover, they are not triggered by any information or news about the specific cryptocurrency, which usually happens with traditional Pump-and-Dump schemes. A recent study calculated that average returns can be as high as 18%, whereas the trading volume can increase by 13% in the first 10 minutes of an attack.[30]

These activities, however, have not been unnoticed by regulators. In February 2018, the Commodity Futures Trading Commission issued warnings to consumers about the possibility of Pump-and-Dump schemes and has vowed to aggressively focus on cracking down manipulation in cryptocurrency markets.[31] The main crypto exchanges act to prevent such schemes, although less reputable exchanges still participate in them.

---

[28] For more information on the report for the European Common, see: https://eba.europa.eu/-/eba-reports-on-crypto-assets.
[29] For more information on the enforcement action against EtherDelta, see: https://www.sec.gov/news/press-release/2018-258.
[30] Li, Shing and Wang (2018) "Cryptocurrency Pump-and-Dump Schemes" (Working Paper).
[31] For more information on the crackdown against crypto market manipulation, see: https://www.cftc.gov/PressRoom/PressReleases/pr7697-18, https://www.crowdfundinsider.com/2018/11/141377-cftc-enforcement-director-addresses-crypto-fraud-in-speech/.

© Aaro Capital 2019. All rights reserved.

3.5 Reducing Volatility: Stablecoins

Stablecoins are cryptocurrencies designed to reduce the volatility inherent in the price of a cryptocurrency, by linking it to a stable asset or basket of assets. A stablecoin can be pegged to:

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

When pegged to another currencies, they can be thought of as a form of "private currency". Stablecoins backed by currencies or commodities are said to be "centralised", while those linked to other cryptocurrencies are said "decentralized". The upside of the peg is the reduced volatility of the cryptocurrency, while on the downside there is the implicit link to the monetary policy of a given country. The main challenges relate to the intrinsic costs of DLT, hacking risks, and counterparty risks (as is the general case for private currencies).

Stablecoins have the potential to take a notable role in the global payment system over the medium term, especially in international remittances and e-commerce. For example, pegging to a basket of currencies may favour increased adoption in the context of international trade, where exchange rate risks can be minimised either across currencies in a given region, or against the dominant global currency – i.e. the US dollar.

Libra, the electronic currency proposed by Facebook, technically qualifies as a stablecoin.[32] While not pegged to one specific currency, Libra is to be pegged to a group of "low-volatility assets, including bank deposits and government securities" in multiple currencies (the Libra Reserve). However, this is not a hard peg – enforcing a constant value vis-à-vis a currency, but rather a soft peg with reserves guaranteeing some lower bound to Libra's values.

3.6 Ease of Access and Low Entry Costs

Ease of access and low entry costs are key advantages of distributed ledger technology. Opening a bank account can be time consuming and cumbersome in the heavily regulated banking sector, whereas only a smartphone is needed to access a crypto account.

These properties are likely to be important for adoption in developed economies, where exchange and transfer fees are still needlessly high in traditional banking.

DLT payment systems are also particularly appealing for emerging and developing economies where there is great appetite for financial inclusion and more effective platforms for payment.[33] This is important in countries where the banking system suffers from low trust, high cost and erratic changes in regulation - private property may not be well protected, and institutional frameworks may be weak due to volatile political regimes.

3.7 Cryptocurrencies as a Store of Value

The deflationary nature of standard cryptocurrencies with a finite and fixed supply, such as Bitcoin, makes them inherently more suited to fulfil the "store of value" function of money rather than direct substitute of currencies.

With this in mind, possible store of value markets Bitcoin could disrupt include gold and offshore banking.

---

[32] For more information on Libra, see https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf.
[33] An example of a platform promoting financial inclusion is https://omisego.network/.

© Aaro Capital 2019. All rights reserved.

- Gold has an established history as a store of value and is considered in many cultures a safe haven asset.
- Offshore banking industry, while often related to tax evasion, has also provided opportunity to individuals and organisations to shield their wealth from corrupt governments and rapacious institutions, where property rights are not safeguarded.

Bitcoin has potentially numerous advantages over gold and offshore bank accounts as outlined in Table 2 above, but the key differentiator is accessibility. Up until now, protecting one's wealth against the adverse actions of a government was only accessible to wealthy individuals or large firms. Bitcoin aims to offer the same level of protection to all individuals, irrespective of wealth or country of residence.[34]

An important challenge for Bitcoin to become a commonly adopted asset as store of value is presented by its volatility as compared, for example, to gold. Interestingly the volatility of gold was much higher in the 70's after the end of the gold standard. In 1974, the gold price rose 73%, to then fell 24% in 1975. In 1981, gold lost 33% of its value, after climbing 121% in the two previous years.[35] This is evidently a normal pattern for an asset emerging as store of value: increasing value and decreasing volatility over time. However, while Bitcoin meets the requirement of scarcity to qualify as a store of value, this is not the sole condition for it to be one. As outlined in section 1.1, value is disconnected from "intrinsic values" and related to prices and subjective utility. Ultimately, the adoption of a cryptocurrency as an asset to store value depends on the public's acceptance and willingness to adopt it.

Importantly, the adoption of a cryptocurrency as a store of value is likely to vary between generations. Currently, older generations are unlikely to ever see cryptocurrencies as a store of value. On the other hand, younger generations readily accept that virtual assets have value, as evidenced by their use of digital greetings cards, virtual flowers and in-video-game items. For example, last year the videogame Fortnite generated $2.4 billion in revenues on the back of in-game sales of virtual products.[36] Data suggests that whilst the perception towards, and engagement with, Bitcoin is improving, both are heavily negatively correlated with age.[37] It remains to be seen if these positive trends will be maintained in the longer term.

[34] The blockchain is not more effective than an offshore account in helping individuals protect their money. However in moving assets outside of the country, it is not as easy for a government to confiscate them or erode them through inflation. If a government wants to go after a specific individual, it can do so both in the case of an offshore account and in the case of a distributed ledger. However, anyone can use distributed ledger, whereas not everyone can open an offshore account or buy gold. For example, a middle-class individual in Venezuela would benefit from buying BTC, whereas they often would not be able to open an offshore account.

[35] See, for example: https://www.forbes.com/sites/matthougan/2018/05/23/what-golds-history-teaches-us-about-bitcoin-as-a-store-of-value/.

[36] See: https://www.telegraph.co.uk/gaming/news/fortnite-earned-annual-revenue-game-history-2018/.

[37] For more information, see: https://medium.com/blockchain-capital-blog/bitcoin-is-a-demographic-mega-trend-data-analysis-160d2f7731e5, https://coin.dance/stats/age.

© Aaro Capital 2019. All rights reserved.

Aaro Capital

© Aaro Capital 2019. All rights reserved.

Authors:

Dr. Giovanni Ricco
giovanni.ricco@aaro.capital

Peter Habermacher
peter.habermacher@aaro.capital

Contact Information:

Peter Habermacher
peter.habermacher@aaro.capital

Ankush Jain
ankush.jain@aaro.capital

Sebastien Jardon
sebastien.jardon@aaro.capital

aaro.capital