2017
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

Risks and Vulnerabilities of Virtual Currency

Cryptocurrency as a Payment Method

Cryptocurrency as a Payment Method

Team

Team Champion:	Everette J., Department of the US Treasury
Team Members:	Kyle Bartrem, Leidos
	Jessica Curtis, Maryland Coordination and Analysis Center
	Julia Dorosz, Wisconsin Department of Justice
	Hannah Hein, Haystax
	Sarah L., Federal Bureau of Investigation
	Steve Landes, Citibank
	Jim Lippard, American Express
	Greg Mandile, Fidelity Investments
	Kaivan Rahbari, Fidelity National Information Services
	Annalise S., Federal Bureau of Investigation
	Christine Wondra, First National Bank

Cryptocurrency as a Payment Method

Key Insights

- The world of cryptocurrency is rapidly changing and evolving. Innovators and entrepreneurs are constantly introducing new cryptocurrencies, each promising new and varying characteristics to attract investors and users.
- The cryptocurrency payments market remains small, despite the regular introduction of new cryptocurrencies. Cryptocurrency users are slowly growing and evolving, however, widespread adoption of cryptocurrencies by the general public remains unlikely in the near future.
- Each of the user groups explored in this paper--illicit actors, consumers, the official sector, and financial institutions--have preferred cryptocurrency features that would need to be satisfied in order to generate widespread adoption. We conclude that no one cryptocurrency currently available addresses all the desired cryptocurrency features.
- Bitcoin historically may have been the cryptocurrency of choice for illicit actors, most likely due to its acceptance on the Dark Web, however, this trend may be changing as new analytic tools allow regulators and law enforcement to trace Bitcoin transactions. Cryptocurrencies offering a higher degree of anonymity are gaining in popularity.
- No evidence was found to indicate that consumers will begin to use cryptocurrency as a primary means of payment for their purchases in the near future.
- Global official sector reaction to cryptocurrencies varies as the decentralized technology does not fit easily into existing regulatory definitions and structures. This sector will likely continue to be cautious as it monitors the risks to financial integrity, consumer protection, financial stability, tax evasion and treatment, and monetary policy. Leaders in regulation, like Japan, are likely to set the standard for the rest of the world in a scenario where the borderless nature of cryptocurrencies requires a cohesive and collaborative effort.
- Financial institutions are monitoring the rise in cryptocurrencies and have invested significantly in cryptocurrency-based technologies; however, active involvement in the use of cryptocurrencies as a method of payment remains low.

Contents

Introduction and Scope Note

Cryptocurrencies have many different features. They are a peer-to-peer network, a distributed public database (i.e., the blockchain), an Internet protocol, a software client, and a digital asset (i.e., token) which you can own and transfer to another party. The use cases for cryptocurrencies may be grouped into four major categories: (a) speculative digital asset/investment; (b) medium of exchange; (c) payment rail; and (d) non-monetary use cases. (1) The simple payments and money transfer use case for cryptocurrency first captured the public's imagination when Bitcoin, the first cryptocurrency, was introduced in 2009.

The emergence of cryptocurrencies as a new method of payment has broad implications for illicit actors, consumers, the official sector, and financial institutions. There are significant risks and challenges that must be overcome before these users adopt and accept cryptocurrencies to conduct financial transactions on a large scale. This adoption will require adaptation of the cryptocurrency protocols to meet the requirements of each of these perspectives.

In this paper, we will explore the risks and challenges for the use of cryptocurrencies as an alternative to traditional currencies for illicit actors, consumers, the official sector, and financial institutions. Through exploring the cryptocurrency needs and requirements for each of these groups, readers can better understand which actors are most likely to navigate to specific cryptocurrencies, and then develop an appropriate response.

For example, if financial institutions know that legitimate customers are more likely to utilize cryptocurrency A over cryptocurrency B, then they can begin to develop ways to incorporate cryptocurrency A into their operating environment, while ensuring federal and state regulation requirements are met. If illicit actors are more likely to navigate to cryptocurrency C, then financial institutions can make an informed decision as to whether to or not they should attempt to work with this cryptocurrency. Additionally, the official sector can then focus on cryptocurrency C to develop methods to limit the flow of illicit funds through this cryptocurrency.

State of Cryptocurrencies Used as a Payment Method

Market and Acceptance

Bitcoin, since its inception in 2009, has achieved its goal of establishing a digital currency capable of recording transactions and preventing double spending without a centralized, trusted third party such as commercial or central banks. Bitcoin, and other cryptocurrencies established since, have introduced new consensus mechanisms (e.g., proof-of-stake) and enhanced their underlying protocols to provide additional functionality and enable non-monetary use cases. (1) Some of these innovations were constructed to address disadvantages in cryptocurrency systems including: (a) a rigid currency supply, (b) lack of scalability in the sense that they can only handle low transaction volumes (for example, Visa can process several thousand transactions per second versus Bitcoin's 7), (c) high volatility in part because they are not tied to a sovereign currency, and (d) tendency to suffer from incentive problems as the network size increases. (2)

Despite these advancements, cryptocurrencies have failed to rival fiat currencies like the US dollar, Euro, and Yen in terms of price stability and acceptance as a form of payment. As of early August 2017, the crypto market for the top 100 cryptocurrencies is just above $121 billion and approximately 25th of 1 percent of the $200 trillion in gold, cash, stocks, and bonds. (3) (4) This is up from $27 billion less than six months ago, at the time of the Cambridge Centre for Alternative Finance's Global Cryptocurrency Benchmarking Study. (1) In market capitalization, Bitcoin dominates the currencies field, followed by Ethereum, Ripple, Bitcoin Cash, and Litecoin. As of March 2017, Bitcoin was the most widely used cryptocurrency in terms of the average number of daily transactions, followed by a distant second-place Ethereum, which has been gaining traction over the last 8 months – even surpassing Bitcoin in daily transaction volume for a short period. There is a general trend towards rising transaction volumes for an analyzed subset of cryptocurrencies since Q4 2016, with Monero and Dash transaction volumes growing the fastest. Bitcoin is the cryptocurrency that is supported and used by the overwhelming majority of wallets, exchanges, and payment service providers that participated in the Cambridge cryptocurrency benchmarking study. (1)

Estimates for the use of cryptocurrency for payments varies significantly across sources. A recent study estimates that as of late 2013, the legitimate use of bitcoin has exceeded potential criminal activity. (5) In 2016, The Boston Federal Reserve estimated that 75% of US consumers who own cryptocurrencies have used them for payments within a 12 month period, while a major US cryptocurrency exchange business indicated that 46% of its users use bitcoin as a 'transactional medium.' Consumers appear to not have adopted cryptocurrencies as a primary medium of exchange for daily purchase, although a growing number of merchants worldwide are accepting cryptocurrency as a payment method. This is due to several factors, including price volatility and the lack of a 'closed loop' cryptocurrency economy, in which people or businesses would get paid in cryptocurrency and then use cryptocurrency as a primary payment method for everyday expenses. (1)

Global Regulation

Cryptocurrencies, due to their decentralized nature, do not fit easily into existing regulatory definitions and structures. The borderless nature of cryptocurrencies and the absence of an identifiable "issuer" of the instrument pose challenges to regulators; worldwide regulators have been both highly reactive and cautious in regulating cryptocurrencies. Regulatory responses have ranged from providing no guidance

or regulation, to issuing warnings, prohibiting banks from buying and selling cryptocurrencies, regulating certain actors in the cryptocurrency ecosystem (e.g., wallet providers and exchangers), and banning cryptocurrencies altogether (Bangladesh, Bolivia, Ecuador, Kyrgyzstan, and Saudi Arabia). (6) The Financial Action Task Force—the global anti-money laundering (AML) standards setting body—in 2015 provided its members with guidance for a risk-based approach to virtual currencies which clarifies the application of FATF AML Recommendations to convertible virtual currency exchanges and helps national authorities develop regulatory responses. (7)

Risks, Challenges, and Protocol Preferences

The below section explores the risks and challenges posed by the use of cryptocurrencies as an alternative to traditional currencies for the official sector, financial institutions, consumers, and illicit actors. Not all the risks or challenges are applicable to every cryptocurrency in every situation and they will increase or decrease based on the level of adoption.

Illicit Actors

Challenges and risks

As the availability and adoption of cryptocurrencies increases, US federal officers, analysts, academics, and researchers have expressed concerns regarding illicit actors utilizing this capability to move funds through the international arena. These funds, used for activities such as financing day-to-day operations and attacks,[a] and the movement of trafficked individuals and drugs, then have the potential to find their way into the legitimate international financial system through cryptocurrency exchange platforms and other laundering techniques.

To date, law enforcement and researchers monitoring the adoption of cryptocurrencies by illicit actors have yet to reach an agreement on the current breadth and scope of cryptocurrencies being utilized for such activities. Bitcoin remains the transactional medium of choice for 'Dark Markets' (online black markets existing on the Dark Web) such as the infamous Silk Road and its numerous successors. In 2014, the top 6 Dark Markets grossed $650,000 worth of sales in bitcoin. (61).

While Bitcoin has been, and continues to be, utilized by buyers and consumers of illicit goods on the Dark Web, concerns surrounding the prospect of criminal organizations or Islamic terrorist groups engaging in Bitcoin seem to remain unsubstantiated. A May 2017 report from CNAS "*Terrorist Use of Virtual Currencies: Containing the Potential Threat*" reports:

> …there is no more than anecdotal evidence that terrorist groups have used virtual currencies to support themselves. Terrorists in the Gaza Strip have used virtual currencies to fund operations, and Islamic State in Iraq and Syria (ISIS) members and supporters have been particularly receptive to the new technology, with recorded used in Indonesia and the United States.

It is important to note that while criminal organizations and Islamic terrorist groups are not currently embracing cryptocurrencies to process funds or purchase materials, a substantial loss, or abrupt loss, of physical territory may limit their access to traditional financing systems. If this occurs, it will likely become difficult for these groups to move substantial amounts of cash across widespread geographic areas and through borders, potentially enticing these groups to explore the ability to move funds through cryptocurrencies.

Desired Features

While illicit actors may not fully embrace cryptocurrencies, certain features of cryptocurrencies appeal to these groups. Additionally, as new cryptocurrencies are developed and embrace these desirable features, enhanced adoption by these groups may occur. It is possible that a potential "tipping" point

[a] For example, in January 2017, Indonesia's financial transactions agency announces Bitcoin and online payment services were used by Islamic State militants in the Middle East to fund terrorist activities in Indonesia. (53)

may be on the horizon, in which illicit actors begin to turn to cryptocurrencies as a reliable and desirable method to conduct financing operations throughout the international arena.

Illicit actors utilize cryptocurrencies for a variety of reasons, to include buying and selling drugs, weapons, and illicit services available on the Dark Web, as well as simply moving money in a pseudonymous fashion. Terrorist organizations have also been known to request funding donations through cryptocurrencies, and cyber criminals have begun using Bitcoin as a form of ransom payment (see 'Ransomware'). The pseudonymity of Bitcoin, Monero, and Zcash make those cryptocurrencies especially attractive to criminals, since one account can generate many Bitcoin public keys or addresses, or Monero or Zcash addresses which are not visible on their respective blockchains, making it difficult to establish chain of custody.

For Bitcoin, services such as Bitcoin Tumblers and Mixers (and, potentially in the future, aggregation of off-chain transactions using Lightning Networks) (8) can further obfuscate transactions. A tumbler, for example, would take money from several wallets and combine it into one "pot", and then pull randomly from that "pot" of money to pay the transactions. So, although Person A may be making a payment to Person C, the money for the transaction may actually be coming from Person B. However, these features of Bitcoin do not guarantee a lack of traceability, which may lead illicit actors to shift to Monero, Zcash, or other cryptocurrencies that offer better privacy protections.

Below is an overview of those characteristics that, if available in a cryptocurrency, may attract more illicit actors into embracing cryptocurrencies on a large scale.

1. **Ease of Use**: Currently, the ability to purchase, buy, sell, and trade with cryptocurrencies requires a technical background. As user friendly interfaces are developed and implemented, it will become easier for unsophisticated illicit actors to use cryptocurrencies to their advantage. Ease of use for cryptocurrency purchase by the average user is a primary constraint on the success of the ransomware business model. (9) Illicit actors also desire the ability to create automated, scalable payment interfaces which can be incorporated into ransomware and other crimeware. (10) The more legitimate users a cryptocurrency has, and the more legitimate transactions which are made using that cryptocurrency, the more opportunities there are for an illicit actor to build a criminal business model on obtaining cryptocurrency payments from those users as victims and the greater the opportunity to hide illicit transactions in a larger sea of legitimate transactions.

2. **Independence from Controls of Legitimate Financial System:** As banks and other financial institutions continue to work on a risk averse structure due to enhanced regulations and financial transaction monitoring, these groups may seek alternative methods to move funds outside of the legitimate financial system, while still desiring connections to the legitimate financial system in order for customers or victims to move money into cryptocurrencies, and to cash out from cryptocurrencies with the proceeds. In the event of wider adoption of cryptocurrencies, the need for a connection back into fiat currencies for cashing out becomes less important, and the need for aiding customers and potential victims to enter the system declines.

3. **Increased Anonymity:** As cryptocurrency developers continue to advance from pseudonymity to more near-complete anonymity of transactions, illicit actors may find such transactional capabilities appealing. This feature is the converse of Transparent Customer Info and Transparent Transactions; to date, there has apparently been more demand for a lack of

Transparent Customer Info than for a lack of Transparent Transactions, as evidenced by the use of Bitcoin for ransomware payments, cashing out through the BTC-e cryptocurrency exchange which did not comply with Know Your Customer laws.[b] Now that the operator of that exchange has been arrested and two Dark Web marketplaces which engaged in Bitcoin transactions have been taken down by law enforcement, (11) there may be increasing demand for cryptocurrencies which have privacy for transactions in addition to mere pseudonymity of parties to transactions. (12)

4. **Dark Web Access:** As additional cryptocurrencies (beyond Bitcoin) are adopted as methods of payment for illicit sites on the Dark Web, it is likely certain groups will adopt those cryptocurrencies to transact on these sites. Features such as multi-signature transactions[c] and smart contracts to support decentralized escrow and remove the need for trust between illicit actors who do not know each other are also likely to support adoption.

Cryptocurrencies that Closely Align to Desired Features

Bitcoin: The Bitcoin blockchain is a distributed and decentralized digital money system. It is decentralized in the sense that there is no central authority responsible for regulating or taxing the money system. As Bitcoins are mined and transactions are verified via peer-to-peer cryptographic proof-of-work, there is no need for such an authority. The Bitcoin blockchain is also distributed – meaning every node on the network retains a complete copy of the digital ledger, which prevents tampering, while ensuring full transparency. Additional features that make Bitcoin particularly appealing to illicit actors are its low-friction, high-speed transaction protocols (which enable transactions to be executed at extremely low costs while reducing the possibility of arbitrage or other exploitation) and its pseudonymous nature. Because participants are represented via 'shell' addresses (public keys), it is difficult to link an actor to a Bitcoin Address. This enables illicit actors and groups to conduct financial operations while avoiding detection by law enforcement.

Bitcoin can be used by anyone who creates a Bitcoin wallet either online or through a mobile application. Once the user has created a wallet, they can purchase Bitcoins through a US Currency Exchange service, by charging a credit card for the amount, or by paying a third-party vendor in cash. Once the wallet has funds, users can begin making purchases and payments. Bitcoin works by implementing two pieces of data, or keys; one public, and the other private. The public key or Bitcoin address, is what other users are provided with when they would like to make a payment. The private key is specific to each individual wallet, serving as a signature on the transaction and verification that the funds have been sent from the owner of that wallet. The private key also prevents the transaction from being altered by anyone once it has been issued, making all transactions irreversible. Each transaction is logged in the block chain, showing a dated timestamp of the two public keys or addresses in the transaction and the transaction amount. (13)

Ethereum: Ethereum is an open-source, public, blockchain-based distributed computing platform featuring smart contracts. Having taken #2 in the virtual currency market since its launch in 2015, Ethereum's focus on smart contracts – contracts able to self-verify their own conditions using both blockchain and external data – utilizes a tamper resistant means for criminals to expand the crime-as-a-

[b] The BTC-e cryptocurrency exchange was used for cashing out 95% of ransomware victim payments according to a recent Black Hat Briefings presentation. (63)

[c] DeepDotWeb's Dark Web Marketplace comparison chart includes multisig transactions as a desirable characteristic. (61) This is also noted in a recent RAND report on dark web transactions for firearms, explosives, and ammunition sales. (62)

service model. (14) The use of Ethereum within the dark web has caused significant impacts, forcing the use of two separate blockchains in response to the theft of a third of Ethereum's reserves. However, Ethereum is not solely the focus of criminals; JP Morgan Chase and the Royal Bank of Scotland have both built upon its platform to engage in virtual currency and payment systems.

Monero: Monero is an open-source, freely available, secure, private, and untraceable cryptocurrency. Originally created in April 2014, Monero adoption has increased significantly over the last few years, with its value reportedly increasing by 2,760 percent in 2016. (15) While many new cryptocurrencies are viewed as derivatives of Bitcoin, Monero is hailed as a new form of cryptocurrency, possessing unique privacy and decentralization properties, resulting in full anonymity and an inability to trace.[d] Monero uses a process coined "stealth addresses" in which the user can retrieve sent funds, but all addresses are encrypted, meaning the stealth address cannot be traced back to an owner. Additionally, Monero combines multiple non-related transactions together, making it even more difficult to trace the origination of funds.

Zcash: Zcash is marketed as a permissionless cryptocurrency that can fully protect the privacy of transactions using zero-knowledge cryptography. (16) Zcash also enables users to send public payments similar to Bitcoin. With the support for both shielded and transparent addresses, users can choose to send Zcash privately or publicly. Zcash payments sent from a shielded address to a transparent address reveal the received balance, while payments from a transparent address to a shielded address hide the value received. (17) While the Bitcoin blockchain contains records of the participants in a transaction, as well as the amount involved, Zcash's blockchain shows only that a transaction took place, not who was involved or the amount. (18)

[d] There appear to be significant limits to the effectiveness of Monero's measures in this regard. (67) (68)

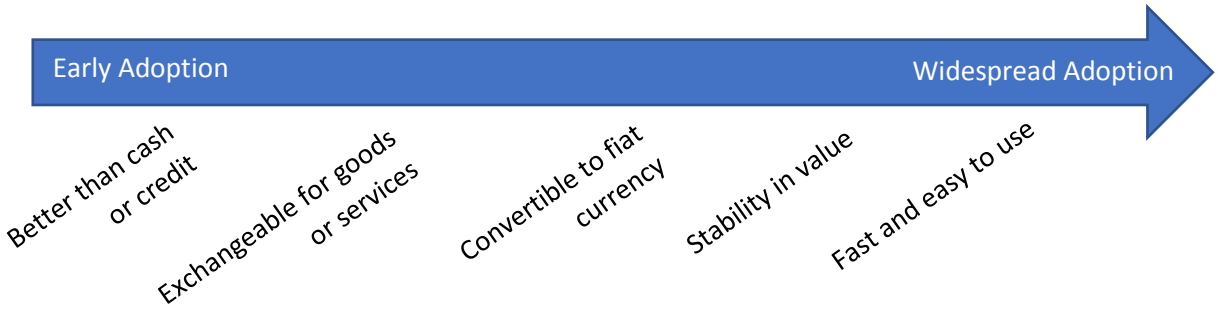
Consumers

Challenges and Risks

Widespread consumer adoption of cryptocurrencies faces many challenges beyond those posed by directly by features of the cryptocurrencies themselves. These include a lack of merchant acceptance, the risk of loss due to hacking of cryptocurrency exchanges or the loss of private keys, the learning curve associated with understanding the technical complexity to a level of comfort, fears that particular cryptocurrencies may be scams or may go defunct, and concerns about legality and tax implications of use. The association of cryptocurrencies with illicit activity and its origins in anti-government rhetoric which have encouraged adoption in some circles have also played a part in discouraging widespread use. Wild fluctuations in value have encouraged more speculative investment than use as a form of payment.

Desired Features

Cryptocurrencies, to achieve widespread adoption of consumers, must possess these functions: a store of value, unit of account, and medium of exchange. (19 p. 278) (20) Identified below are five protocols that would make a cryptocurrency more attractive to consumers for legitimate, non-illicit transactions and exhibit the three functions of money for use. These features range in criticality to a cryptocurrency's success, but to be widely adopted, they must be present to some degree. Additionally, not all features must be present at inception for the cryptocurrency to be adopted, just the possibility and promise that someday these features could be developed.



1. **Better than Cash or Credit:** It seems obvious, but it is worth mentioning that for a cryptocurrency to be successful with any consumer there must be something that sets it apart from the current systems: credit and cash. Cash is anonymous but inconvenient and credit is convenient but there are strings. If a cryptocurrency is to survive the first hurdle, it must present a consumer with something that solves a problem that credit or cash creates for them as users.

2. **Exchangeable for Goods or Services:** Consumers want to be able to use money to purchase goods and services from merchants as well as to transact with other individuals. In the former case, merchants would make a change to how they accept payment for one of two reasons, either there is a financial incentive to the switch (i.e. significantly lower fees associated with each transaction or more rapid settlement of transactions) or there is a market demand to switch (e.g., customer demand for cryptocurrency payments, loss of confidence in prevalent fiat

currency or other forms of electronic payment).[e] Cryptocurrency transaction costs would need to remain below the three percent charge associated with credit card payments to lure merchants in developed economies[f] or would need to be more stable and reliable than the sovereign currency to lure consumers.

For example, First Blood is a blockchain, decentralized system designed for user-to-user interactions in the eSports world. Their currency is FirstBlood Token ("1ST") and the goal is to provide eSports players a way to make money without the "fear of losing what is theirs" or relying on third parties to validate. Uses of the currency include playing matches, witnessing matches and voting on the jury, hosting tournaments, and claiming rewards from referrals. (21)

Arguably, the most successful merchant-to-user transactions are done in Bitcoin. Third party providers have attempted to facilitate Bitcoin purchases on Amazon which allowed consumers to transfer any dollar amount of Bitcoin to use for purchases on Amazon. (22) This mechanism, which also worked with Starbucks, BestBuy, and other retailers, used an instant electronic gift card as an intermediary mechanism behind the curtain. (23) Coinbase's ShiftCard is a Visa debit card usable in a select number of U.S. states which is funded by the user's Bitcoin wallet at Coinbase; for now, transaction fees associated with Bitcoin exchange are waived. (24)

Person-to-person transactions, historically using cash, have become possible electronically with PayPal, Venmo, Zelle, Square Cash, Facebook Messenger Payments, Apple Pay Cash, and similar payment solutions.[g] Individuals are unlikely to be tolerant of fees for such transactions unless they are quite small, because they currently do not face them. The greatest barrier to cryptocurrencies in this space is lack of familiarity and lack of adoption among one's peers, as well as the competing existing solutions. Cryptocurrencies could compete in this space if they can offer benefits over the existing solutions or if they achieve adoption in the user-to-merchant space first to obtain the network effects of widespread user adoption comparable to competing solutions.

3. **Convertibility:** Cryptocurrencies that are easily convertible into other goods, services, and payment methods are more likely to be adopted and used by consumers. Therefore, wide-scale

[e] It has been argued that millennials exhibit a preference for debit over credit. The younger generation also uses mobile devices for more activities and are more likely to use mobile payments. (56)

[f] The current average Bitcoin transaction cost (paid to miners) to avoid delays is 200 satoshis per byte, and the median transaction is 226 bytes, for a total fee of 45,200 satoshis (per http://bitcoinfees.21.co/). A satoshi is the smallest unit of Bitcoin which can currently be spent, a hundredth of a millionth of a Bitcoin, or 0.00000001 Bitcoin. At the August 10, 2017 Bitcoin price of about $3,400, that fee for a median transaction is $1.54. Once all Bitcoin has been mined, the only compensation to miners will be from transaction fees. Economic incentives of miners are discussed in *The economics of digital currencies* (19) and *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (66).

[g] M-PESA is a notable early mobile payments solution which became successful in Kenya in part due to its use of intermediary agents, how it provided financial resilience for the unbanked by making feasible support from long-distance social ties, and the risks and costs of moving physical cash. Dr. Tavneet Suri of MIT discussed her research on M-PESA and why it achieved rapid widespread adoption on the May 21, 2017 episode of the "Appetite for Disruption: The Business and Regulation of Fintech" podcast. (60)

use of cryptocurrencies by consumers is more likely to occur with cryptocurrencies that have real world value (open scheme) versus those that are restricted to a specific domain (closed scheme).

Popular cryptocurrencies that are easily convertible to fiat currency include: Bitcoin, Ethereum, and Litecoin.[h] In addition to convertibility to fiat currency via exchanges, some of these cryptocurrencies, such as Bitcoin, are also accepted by various merchants as a payment for goods and services (without being converted into fiat currency) thus increasing the likelihood of their use by consumers. The legitimate methods by which a cryptocurrency is easily converted also appeals to a larger variety of consumers. For instance, Bitcoin allows consumers to trade fiat currency for Bitcoin via online exchanges as well as in-person Bitcoin ATMs, making it easily accessible.

4. **Stability** (25) (26) (27)**:** Consumers care about stability of a cryptocurrency if they expect to be able to use it as money rather than an asset. Higher volatility can be desirable in an investment asset, as higher volatility means higher risk and higher potential for return. The volatility of cryptocurrencies has led some to consider them to be an additional asset class for investment. In addition, the fact that it is not tied to a specific country allows it to be uncorrelated asset that enables diversification.[i] But for use as money, consumers want sufficient stability so that they do not incur significant losses and that the prices of everyday goods and services they purchase are predictable.

   Stability does not necessarily mean parity with prevalent local fiat currencies, and it can't mean parity with all local currencies in a global monetary system post-Bretton Woods[j], where currencies float rather than being pegged at fixed exchange rates. But consumers want sufficient predictability in the future value of the currency they hold, which means relatively low volatility with respect to the prevalent local currency. If a cryptocurrency is expected to increase in value with respect to the local currency it becomes more attractive to hold; if it decreases too much in value with respect to the local currency then it becomes unattractive. But this is not necessarily a barrier to short-term usage of the cryptocurrency for local currency transactions if the potential for losses in a transaction are on a par with other fees which may be charged or if a merchant or payment processor absorbs any exchange losses.

   A generally increasing value which encourages savings/investment is not necessarily fatal to adoption of a cryptocurrency for use as a method of payment (as Bitcoin has demonstrated); it is the periodic large drops in value which make users doubt the wisdom of its use. Consumers

[h] These are the three cryptocurrencies supported by Coinbase, which aims to make use of cryptocurrencies simple for the retail consumer. Coinbase representatives discussed their goals on the July 16, 2017 episode of the "Appetite for Disruption" podcast. (60)

[i] It was estimated in 2016 that 54% of Coinbase users use Bitcoin strictly as an investment. (1)

[j] The Bretton Woods system was a negotiated system of currency convertibility dependent upon the gold standard. When the U.S. unilaterally ended the gold standard in 1971, the dollar became a fiat currency instead of a commodity currency and many major currencies became free floating rather than pegged to a commodity or other currencies.

find declines in value over a longer period of time more palatable as seen with other fiat currencies. Some Bitcoin advocates have expressed an intent to hold Bitcoin and think of values in Bitcoin terms rather than U.S. dollar terms, thereby allowing the cryptocurrency to act as a unit of account. If users are able to create communities which most transactions are denominated in Bitcoin, they can perhaps reduce the apparent relevance of Bitcoin price fluctuations with respect to the U.S. dollar in the same way most Americans ignore fluctuations of the U.S. dollar with respect to other currencies. Significant fluctuations of Bitcoin value in an environment with a stable local fiat currency means significant fluctuations in the prices that must be paid for everyday goods and services. However, (28) environments with unstable local fiat currency might benefit from using Bitcoin.

There have been multiple attempts to create cryptocurrencies pegged to the U.S. dollar by different mechanisms—BitUSD, NuBits, CoinUSD, Tether (USDT), and Steem Backed Dollars (SBD) or Steem Dollars (SD) (these are synonymous) are examples. NuBits and CoinUSD launched in late 2014 and neither is currently prevalent due to, in part, insufficient demand leading to a failure of their system of pegging. BitUSD was launched in 2014 by BitShares, and has been more successful, but has a low volume and market cap, though has remained fairly well tied to the U.S. dollar.[k] Tether, created in 2015, has been even more stable with a larger market cap and trading volume, though its peg temporarily failed by about 10% when it dropped below $0.92 per coin over the days of April 21-26, 2017.[l]

5. **Ease of Use:** Consumers prefer and adopt technology that is easy for them to understand and use. For example, mobile phone adoption was quick (from introduction to saturation in two decades) and smart phone adoption even quicker (from introduction to 80% market penetration in the U.S. in a decade) (29) even though it was more complicated technology, because it operated in a similar way to traditional telephones. Cryptocurrencies usually struggle to gain adoption because consumers have difficulty understanding and using the technology. Cryptocurrency designers or third-party actors have recognized these problems and are developing new interfaces to help speed up adoption. Other cryptocurrencies that cater to hobbyists or developers have complicated interfaces that will not generate widespread adoption.

   There are two ways that cryptocurrencies are becoming more usable for common consumers: third-party interfaces or user-friendly initial design. Third-parties are using more established cryptocurrencies, such as Bitcoin and Ripple, as payment networks behind the scenes and are presenting consumers with a familiar banking account interface. Companies like Bitpay and Coinbase are good examples where the consumer can access a cryptocurrency through a user-friendly interface. Others, such as Abra, create interfaces that do not reveal to consumers that they own Bitcoin, making its use completely invisible. The other trend in the usability is that smaller cryptocurrencies are being designed with user-friendly interfaces in mind. Cryptocurrencies, such as Gamecredits, Lisk, Steem, Stellar, and Waves are designed with

[k] BitUSD ranges from just over $0.86 to $1.20 over the last year, but usually in a range of $0.96 to $1.06.
[l] Tether currently ranges from $1.00 to $1.04. It previously ranged from $0.9999 to $1.00.

ease-of-use in mind. Developers of these cryptocurrencies are judging that the familiarity of the interface drives consumers to use their product.

The majority of major cryptocurrencies do not currently cater to consumer usability. The cryptocurrencies are focused on enabling developers to create new features or provide anonymity. If these cryptocurrencies maintain popularity, third-parties may develop more user-friendly interfaces to drive adoption. Otherwise, these cryptocurrencies will maintain usage in a niche market.

Cryptocurrencies that Closely Align to Desired Features

At present Bitcoin is by far the dominant cryptocurrency in the consumer space and has had the most development of user-friendly wallet software and applications, but Ethereum has rapidly gained ground. The stability issue does not appear to have been resolved by any cryptocurrency to date, which makes it more likely that cryptocurrencies will need to be easily convertible into the local fiat currency or even hidden in the background of financial applications to be invisible in order to catch on for widespread use. Specialized cryptocurrencies associated with specific uses which are inherently of interest to consumers may also be successful, in the same way that consumers purchase tickets or tokens for admission to events or theme park rides, or collect and spend frequent flier miles or loyalty points.

Official Sector

Central banks, like commercial banks, are drawn by the idea of fast, efficient, digital money that does not carry the cost of handling cash and that can be tracked as it moves through the financial system. Central banks' interest in deploying a blockchain to do this mirrors moves by commercial banks to use the technology to ease cross-border settlement transactions and overhaul antiquated back-office infrastructure. In addition to using the foundation of cryptocurrency, blockchain, for settlement and infrastructure, some central banks—including the Australia, Canada, Denmark, Russia, and the United Kingdom, and Vietnam—are also exploring issuing their own digital currency. Central banks, however, appear to be far from issuing their own digital currency and governments are primarily focused on regulating private cryptocurrencies.

Challenges and Risks

The establishment and maintenance of a currency has traditionally been regarded as a key prerogative of the official sector (i.e., government and central banks), as well as a central institution of democratic societies. (30) Cryptocurrencies are designed to function as an alternative for this activity. Cryptocurrencies, which rely on decentralized networks to facilitate transactions in a particular unit of account, have no central administrator in the way that a government issues and backs fiat currencies. Cryptocurrencies are designed so that users may trade 'currency' directly, with limited or no interference or participation of any official sector, financial sector intermediary, or third-party administrator. As such, cryptocurrencies pose risks to the official sector in the below areas in which the traditional financial system allows government to affect. Risks fall into a continuum, with immediate and pressing concerns about financial integrity, consumer protection, tax evasion, and the regulation of capital movements. Concerns about financial stability or the implications for monetary policy are less immediate but will require further analysis and monitoring. (31)

- **Financial integrity.** Cryptocurrencies can be used to conceal or disguise the illicit origin or sanctioned destination of funds, thus facilitating money laundering, terrorist financing, the evasion of sanctions, fraud, and cybercrime. (31) (32)
- **Consumer protection.** The regulatory uncertainty and lack of transparency into cryptocurrencies create significant consumer protection vulnerabilities including disruptions to cryptocurrency ecosystems, risks related to unregulated cryptocurrency intermediaries and service providers, fraud schemes, and the irreversibility of transactions. (31) Users of cryptocurrencies could lose funds without total loss protection programs like the Federal Deposit Insurance Corporation.
- **Tax evasion/avoidance and treatment.** Cryptocurrencies, anonymous or pseudonymous in nature and taking place in a peer-to-peer system, have a high risk as a potential means for evading or avoiding taxes. In addition, to the extent cryptocurrencies are performing an economic function, whether as a store of value or a medium of exchange, they will have tax implications. (31)
- **Enforcement of exchange controls and capital flow management.** Cryptocurrencies can be used to effectively conduct a cross-border transfer of a fiat currency while bypassing traditional payment systems, and therefore may be used to circumvent exchange and capital controls. (31)
- **Financial stability.** Individual cryptocurrency holders and users may be exposed to significant risks as the cryptocurrency ecosystem is susceptible to disruptions, including security breaches, bankruptcy, financial fraud, and payment-like system risk such as operational risk, credit risk,

liquidity risk, and legal risk. Large-scale use of cryptocurrencies and greater interconnectedness with other parts of the financial sector could generate systemic financial risks. For example, the erosion of bank revenue from payment services or vulnerability to cryptographic risks. (31)

- **Monetary policy.** Controlling the money supply, by different means, is one of the main instruments that governments can leverage to shape the economy. (30) Cryptocurrencies currently lack critical features that stable monetary regimes would typically provide to guard against three key monetary stability risks (the risk of structural "deflation"; flexibility to respond to temporary shocks to money demand and thus smooth the business cycle; and the capacity to function as a lender-of-last-resort) (31) and therefore the official sector could not rely on cryptocurrency to effect monetary policy. It is worth noting that even if cryptocurrencies became the primary payment method, the official sector could still impact monetary policy via setting the overnight interest rate. (33)

Although cryptocurrencies vary in design, cryptocurrencies generally maintain the below design characteristics that pose financial and political risks: (32) (30)

- **Anonymity/pseudonymity.** Cryptocurrencies provide varying degrees of anonymity both in name and in transaction-level detail, which directly confronts Know-Your-Customer/Customer Due Diligence principles and transaction reporting, both core components of anti-money laundering and countering the financing (AML/CFT) regimes. Mixing services and other location/identity hiding services add additional anonymity. (32)
- **Rapid transaction settlement.** Cryptocurrencies provide near real-time transaction cross-border settlement at a lower cost than other well-established methods. Cryptocurrencies could present an attractive opportunity for globalized criminal and terrorist groups requiring borderless financial channels. (32)
- **Decentralized and contained environments.** With a broad range of actors in the cryptocurrency ecosystem (e.g., miners, exchanges, wallet providers, payment processors, ATM providers, etc.), whom to hold accountable in cryptocurrency networks is not always clear. Law enforcement cannot target one central location or entity for investigative or asset seizure purposes. In contained environments—environments where transactions are not recorded at an exchange or other node attached to the traditional financial system—established regulated firms have no role or insight. (32)
- **Self-governance model.** Cryptocurrency, as a socio-technical trustlessness network, seeks to obliterate the need for a central control point, but as the technology grows, new or unanticipated issues emerge which ultimately require the setting up of a social institution in order to protect or regulate the technology. Cryptocurrencies, specifically Bitcoin, are managed by a small community of developers without a governance structure to democratically respond to the technical, social, economic, and political implications of the technology. (30)

Desired Features

Governments will have to address risks in each of the areas above (e.g., financial integrity, consumer protection, etc.) without stifling innovation and they will have to do so in a collaborative manner with a global response due to the transnational nature of cryptocurrency. Failure to address risks globally, with the inclusion of other governments and international organizations, cryptocurrency sectors, and the traditional financial system, is likely to drive innovators and criminals alike further into secrecy.

Governments will have to consider acceptable cryptocurrency attributes that allow governments to continue to perform its functions of providing consumer protection, collect tax, enforce exchange controls, provide financial stability and financial integrity, and affect monetary policy. The following are suggested attributes that are likely to be acceptable to the official sector.

1. **Transparency of customer information and transaction information:** Transparency into customer information and both contained (within the cryptocurrency system) and open transaction information, whether public or limited to law enforcement and financial agencies, would allow governments to retrieve information in alleged criminal matters and have insight into financial stability. The cryptocurrency code could allow for a third-party to store personally identifiable information, similar to ICANN, a US-based non-profit corporation that oversees coordinating all unique identifiers across the World Wide Web. A number of cryptocurrency firms are developing methods for individuals to maintain encrypted data on the blockchain in a manner that would enable a degree of anonymization while also ensuring firms have access to up-to-date and reliable KYC information. (32)

2. **Government smart contracts:** The cryptocurrency should allow for governments to build smart contracts on the cryptocurrency's blockchain in order to perform key state functions, such as identifying suspicious activity or enabling tax collection.

3. **Rapid international transaction settlement:** The cryptocurrency's technology will need to be scalable to allow for continued rapid settlement as transaction volume grows, thereby maintaining the lower cost benefits of the technology and deepening financial inclusion.

4. **Inherent governance structure:** The cryptocurrency will need a governance structure that allows for some form of social institution that ensures accountability and preserves the legitimacy of the system as a whole. The blockchain could be used as a platform on which people might encode their own set of rules and procedures that will define a particular system of governance—one that can benefit from the distinctive characteristics of the blockchain (i.e., transparency, traceability, accountability, and incorruptibility) but would also leave room for the establishment of an institutional framework that could operate on top of that (decentralized) network. (30)

Cryptocurrencies that Closely Align to Desired Features

No existing cryptocurrency fulfills the features that the official sector would prefer in a cryptocurrency. Cryptocurrencies, due to their inherent psuedanonymous nature, prevent the official sector, financial institutions, and other actors in the cryptocurrency ecosystem from performing key regulatory functions. Third-party provided data analysis can provide limited insight into actors behind Bitcoin transactions, but the availability of this data is not complete and comes at additional expense to regulators and financial institutions.

A potential solution that the official sector could employ to assist in cryptocurrency regulation would be to use smart contracts to perform some regulatory functions. Ethereum, launched in 2015, was the first and continues to be the most popular cryptocurrency which allows for an application, or smart contract, to be built on top of the blockchain and protocol.

Cryptocurrency innovators continue to make changes to the cryptocurrency blockchain and protocol in order to scale the system as volume grows and thereby maintain the lower cost benefit that could provide for financial inclusion. No cryptocurrency has come to light as having solved the scalability issue, especially as the user base grows to greater than 10 to 20 million users. Some cryptocurrency analysts advocate that Ethereum may be the only cryptocurrency that has the resources, insight, and support from corporation and institutions to scale Ether for volume. (34) (35)

Cryptocurrencies continue to struggle with coherent governance in a decentralized, technology based payment system. This struggle has been most recently evidenced in the split of the most widely used cryptocurrency, Bitcoin, into two different ledgers due to an inability to resolve several issues about the technological direction of the currency. It appears that new cryptocurrencies are looking to tackle this problem. Qtum, a Singaporean-based cryptocurrency launched in 2017, will be developed and maintained by the Qtum Foundation, a non-profit organization representing Qtum's stake and token holders, which will advocate governance transparency, and promote the safety and harmony of the Qtum open source ecosystem. (36)

Financial Institutions

In order for financial institutions to accept Cryptocurrencies as a method of payment and store of value, many factors must be considered to determine the risks and challenges as well as the potential benefits to financial institutions and their clients. There are a variety of desired features including real time settlements, lower costs and fees, and ease of use which can make the technology many cryptocurrencies are built upon attractive to financial institutions. However, the decentralized nature of popular cryptocurrencies present significant regulatory compliance challenges to financial institutions and the inherent absence of trust engineered into current cryptocurrency transactions runs counter to the fiduciary duties of retail, commercial, and investment banking.

While financial institutions are involved in consortiums to identify the benefits of employing underlying cryptocurrency technologies such as blockchain and distributed ledger systems, traditional financial institutions are less involved in cryptocurrencies as a form of payment or transaction. (37) Financial institutions that have interest in the transactional aspects of cryptocurrencies; however, have expressed this interest through the backing of cryptocurrency exchanges and providing a medium for customers to view their third-party cryptocurrency holdings on their platforms rather than directly transacting on the financial institutions platforms. (38)

Risks and Challenges

1. **Compliance & Regulatory**

Current regulatory requirements governing financial institutions are likely one the greatest barriers to the adoption of cryptocurrencies in their current state by financial institutions. Cryptocurrencies in many countries, including the U.S., continue to have confusing legal statuses. A lack of specific cryptocurrency regulation has directly resulted in the hesitancy of financial institutions to adopt cryptocurrencies as a form of transaction or payment. (39)

Financial institutions are required by current U.S. regulations to know their customers' identities as well as their expected activities, in order to facilitate economic sanctions enforcement and suspicious activity detection and reporting. This regulation applies to all accounts established with a financial institution as well as many transactions that flow through a customer's account (e.g., commercial entity), on behalf of their clients. Many of the largest cryptocurrencies by market capitalization present challenges for financial institutions due the anonymous nature of transactions. If these cryptocurrencies were accepted for transaction or payment by a financial institution it would be difficult, if not impossible, to identify origins and destinations of transactions. The process of identifying customers and compiling adequate transaction history has potential to offset any savings realized through using a cryptocurrency. Also, third party vendor tools used to track cryptocurrency transactions and potentially identify transactional history do not provide solutions for all cryptocurrency transactions and increase the cost and dedicated resources required for a financial institution to track transactions. Financial institutions would likely require additional regulatory guidance from banking regulators prior to allowing cryptocurrency transactions to occur on their platforms in any significant way.

Securities laws are also applicable to financial institutions involved in the securities industry. The Securities and Exchange Commission recently issued an investigative report concluding that tokens offered and sold by a "virtual" organization known as "The DAO" (for "Distributed Autonomous Organization") were securities and, therefore, subject to the federal securities laws. (40) However,

securities regulators have not issued comprehensive guidance on how financial institutions should treat cryptocurrencies as a whole. (41) Financial institutions will likely remain hesitant to allow trading of cryptocurrencies on their platforms without additional guidance from regulators such as the SEC and FINRA.[m]

2. **Security**

In addition to regulatory concerns, financial industries must also consider consumer protections and security of assets when considering allowing cryptocurrency transactions on its platforms. These issues can range from storage of cryptocurrencies to cryptocurrencies in transit.

Currently, financial institutions employ mature systems to store and transact on their networks. These systems include industry standards such as PCI and SWIFT which deploy controls to protect consumer funds from theft and fraudulent transactions. While cryptocurrencies could provide a faster and lower cost solution to current methods, security and trust in the transactions would need to meet industry, consumer and regulatory standards to be accepted by financial institutions as an alternative to methods already in place. It is not likely that cryptocurrencies in their current form possess the features needed to provide cost-effective enhancements to current methods of transaction. (42)

Financial institutions also need to consider the protection of stored assets. Cryptocurrencies are regularly targeted by hackers through malware crafted specifically to steal from cryptocurrency wallets and compromise credentials to access the asset. Financial institutions, to safely and securely introduce cryptocurrencies to their platforms, would need to develop standards and controls to protect these digital stores of value from theft and fraud. This issue would require a suite of protective measures to include increased network security, credential protection, disaster recovery, insurance and a means of backing up stored cryptocurrencies. (43) Financial institutions would need to weigh the cost of implementing these protective measures against the benefit of hosting cryptocurrencies on their systems.

Desired Features

1. **Low Cost:** Low cost is a desired protocol necessary for the adoption of cryptocurrencies by financial institutions. There are two aspects of low cost to consider, including cost of cryptocurrency transactions and overhead cost of hosting virtual currencies. Cryptocurrency transaction costs include fees, transmission costs, and price fluctuations; whereas overhead costs include hardware, software, personnel, insurance and other infrastructure related costs.

   Cryptocurrency costs must also be low to support customer adoption. If the cost of transacting in cryptocurrency is higher than transactional costs in traditional forms such as credit cards, ACH, and Swift, adoption would not be supported by customers.

   Presently, many cryptocurrencies offer low transaction costs, with the only associated cost related to data transmission and infrastructure. This makes cryptocurrencies an attractive

[m] FINRA issued a report in January 2017 identifying potential applications, impacts, and implementation and regulatory considerations which arise from digital ledger technology. (65)

replacement for traditional financial transactions which can incur fees ranging from 0.5% to 5%, plus $0.20 to $0.30 for each transaction processed.

Typically, there are no transaction fees for cryptocurrency exchanges because the miners are compensated by the network. Even though there is no cryptocurrency transaction fee, many expect that most users will engage a third-party service. These services, or cryptocurrency exchanges, act like intermediaries and do collect fees for transactions. (44) Established financial institutions have potential to lower the transactional fees if customers widely adopt cryptocurrencies as a method of financial transactions.

2. **Real Time Settlement:** Another desired protocol of cryptocurrencies for financial institutions is real time settlement of financial transactions. With respect to the availability of funds, blockchain protocols offer near-real time transaction settlements that are not currently available through other traditional means of financial transactions. The lack of regulation and the issuance of unique digital hashes, allows consumers of these cryptocurrencies to move funds almost instantaneously around the globe and outside of the conventional banking system. (42) Digital wallets are easily established and can be done so from remote locations; those newly established accounts could be funded and used minutes later. Unlike credit card payments and some ACH, cryptocurrencies are 'pushed' from a consumer's account; so, all transactions are considered final and settlement is immediate. Currently, there are no verification processes, reversals/chargeback rights with cryptocurrency, nor any other mechanism for stopping or recalling of a payment.

3. **Widespread Acceptance and Use:** Bitcoin is the most popular cryptocurrency in regard to popularity, number of users, and market capitalization. A popular cryptocurrency with a large market capitalization, such as Bitcoin, can ultimately provide a financial institution with an assessment of a cryptocurrency's durability. However, there are hundreds of other cryptocurrencies offered which provide unique features. Financial institutions are unlikely to develop systems to support cryptocurrency transactions until a cryptocurrency is identified which is believed to be widely accepted for use by consumers, and regulators provide guidance on what cryptocurrency features are needed for acceptance by a financial institution.

Cryptocurrencies that Closely Align to Desired Features

While major financial institutions have taken an interest and devoted significant investments to underlying cryptocurrency technology, there has been less interest in introducing cryptocurrencies to financial institution platforms as a payment method or method of financial transaction. Issues such as operational and regulatory risks create uncertainty, which hinders many financial institutions adoption of cryptocurrencies. The current challenge for a financial institution is to develop guidelines and regulations that protect consumers, prevent money laundering, minimize disruptions to existing banking systems, and are profitable, while safeguarding transformative innovation. Financial institutions abilities to move past these hurdles could allow for the leveraging of benefits associated with cryptocurrencies and distributed ledger systems, such as efficiency gains to provide a positive customer experience present additional concerns to financial institutions.

Bitcoin was introduced in 2009 and was intended to function as a normal currency. Bitcoin's introduction as a peer-to-peer payment system transformed the way cryptocurrencies were used, representing a system that operates outside traditional financial infrastructure. Bitcoin's underlying technology, a distributed ledger system, provides a historical record of all Bitcoin transactions by associating transactions with addresses or public keys. Bitcoin consumers need to enter the Bitcoin market typically using an intermediary. Bitcoin transacting maintains individual anonymity which is a hurdle for financial institutions. However, third party vendors that work to identify addresses associated with the Bitcoin network could provide a solution for regulations which require financial institutions to know their customers and transactions taking place on their platforms for the purposes of AML and sanction regulations.

Ripple, another cryptocurrency, was developed in 2012 to appeal to the financial technology industry and as an enterprise solution. Ripple describes itself as a "real-time global settlement network that offers instant, certain and low-cost international payments." The cryptocurrency is built on a model to allow banks and other financial institutions to facilitate cross-border payments in near real-time. Ripple differs from its cryptocurrency counterparts in that it does not require mining. Instead, Ripple utilizes a consensus style ledger for its blockchain. By not requiring mining, Ripple reduces the need for computing power, which in turn limits network latency. Like its cryptocurrency counterparts, Ripple provides cross-border payments. Ripple has potential to provide real time settlement solutions to financial institutions and has already been adopted by a few international financial institutions. U.S. domestic financial institutions are unlikely to adopt this type of technology without further input from regulators.

Ethereum, started in 2015, has the second largest market capitalization to Bitcoin of any cryptocurrency. Unlike Bitcoin, Ethereum is mainly used by developers as a decentralized platform enabling companies to create what are known as Smart Contracts. This technology allows users to codify, decentralize, secure and trade on the Ethereum platform. Prime adopters of the technology include those in the financial technologies industries and its use case is more of an enterprise solution. The technology improves upon Bitcoin's blockchain technology by enhancing fraud controls and limiting interference from third parties. The ability to create Smart Contracts which are essentially computer programs to conduct financial transactions is a very attractive feature to financial institutions. Many financial institutions are exploring use cases and the technology is likely to be very useful to financial institutions. However, the cryptocurrency run on Ethereum has less potential as a method of payment for financial institutions. The use of the cryptocurrency hosted by the Ethereum network has a more likely use case in crowd funding for startup companies. Financial institutions would require guidance from both banking and securities regulators as to how Ethereum could be implemented as an investment vehicle and/or transaction engine on their platforms.

Cryptocurrency Feature Preferences

Bitcoin, and other cryptocurrencies established since 2009, have introduced new consensus mechanisms (e.g., proof-of-stake), enhanced their underlying protocols, and added protocol and application features that are layered on top of the blockchain to meet user demands, expand the market, and respond to regulatory actions. Cryptocurrency users and organizations impacted by cryptocurrency used as a payment method, including illicit actors, consumers, the financial sector, and the official sector have varying preferences for cryptocurrency features that would encourage endorsement or the use of cryptocurrency. The below table provides a subjective analysis of how each of these actors is likely to view a particular cryptocurrency feature.

Likeliness to Find a Cryptocurrency Feature Desirable

+ +	Highly likely
+	Likely
-	Unlikely
- -	Highly unlikely

Cryptocurrency Feature	Official Sector	Financial Sector	Consumers	Illicit Actors
Transactional Properties				
Convertible to fiat currency	+	+ +	+ +	+ +
Irreversible	- -	-	- -	+ +
Transparent customer information	+ +	+ +	-	- -
Transparent transaction information	+ +	+	-	-
Rapid settlement	+ +	+	+ +	+ +
Ease of use	+ +	++	++	++
Smart contracts	+ +	+ +	+	+
Permissionless	-	+ +	+ +	+ +
Secure	+ +	+ +	+ +	+
Monetary Policy Properties				
Exchangeable for goods and services	-	+ +	+ +	+ +
Controlled supply	+	+	++	+
Inherent governance framework	+ +	+ +	+	-
No debt but bearer	-	+	- -	-

Features of Cryptocurrencies

Transactional Properties

Convertible to Fiat Currency. By using cryptocurrency exchanges, users may buy and sell cryptocurrencies in exchange for the fiat currency of their choice (subject to the availability at the exchange), much like a foreign currency exchange. Exchanges in the U.S. are subject to state regulations as money transmitters/money services businesses and to Know Your Customer regulations under the Bank Secrecy Act. Cryptocurrency exchanges offer a variety of different services which may resemble retail banking services and merchant payment processing services in addition to cryptocurrency/fiat currency exchange. Exchange rates could fluctuate significantly daily and from exchange to exchange, offering potential arbitrage opportunities for traders.

Irreversible. A transaction cannot be reversed by either party after it is confirmed. No cryptocurrency currently provides a mechanism to reverse transactions even in the situation where someone may have fallen victim to malicious actors. Cryptocurrencies which support multi-signature transactions (where M of N signatures are required to access the output of a given transaction) and time locks (where the output of a transaction is unspendable until a future time) allow the construction of transactions which are effectively reversible or escrowed.

Transparent Customer Information. Cryptocurrencies range in degree of anonymity but are typically described as enabling "pseudonymous" rather than anonymous transactions, since distributed ledgers are generally publicly available. Cryptocurrency ecosystem participants want varying levels customer information to be recorded in transactions. The degree of anonymity provided by some cryptocurrencies may discourage a range of financial system participants from direct use or from providing facilities for cryptocurrency use to their customers, as anti-money laundering compliance requirements may be difficult to satisfy. (45)

Transparent Transaction Information. Similar to varying degrees of customer information, cryptocurrencies record varying levels of transaction information (i.e., physical location of transaction endpoints, value of the transaction, time of the transaction, etc.). The degree of transaction information provided by cryptocurrencies may discourage ecosystems participants from adoption as it prevents those participants from being able to conduct activity that is available in the traditional financial system. For example, without transparent transaction information, governments may not be able to identify suspicious activities.

Rapid Settlement (Scaling). The cryptocurrency technology should enable rapid settlement of transactions as increasing users join the network in order to prevent unconfirmed transactions and maintain low transaction fees. Due to their limited scale and acceptance, the number of transactions cryptocurrencies can process is orders of magnitude smaller than those currently handled by retail payment systems. It remains to be seen if and to what extent cryptocurrencies would be able to evolve in order to process a significantly higher number of transactions. The increased efficiency of these schemes cannot be taken for granted; some of the most important cryptocurrency schemes seem to be resource-intensive in terms of the energy and computing power required to process a small number of transactions. Improvements in processing power and speed and the tendency for computing and hardware costs to decrease imply that scalability and efficiency issues might be addressed over time. Other digital currency schemes purportedly require fewer resources to operate. (45)

Ease of Use. Cryptocurrencies with user interfaces that are easy to understand and compatible with third-party interfaces are more likely to be adopted and encouraged. Cryptocurrencies may struggle to gain adoption because users have difficulty understanding and using the technology.

Smart contracts. Smart contracts are distributed contracts, built on top of an existing distributed ledger and protocol, that allow for an 'if, then' executable function. They are used to form agreements with people or entities and act like autonomous agents that run entirely on the blockchain, making them automated, open, secure, and trustless. Smart contracts can enable functionality that is desirable to cryptocurrency ecosystem participants. For example, cryptocurrencies that want to prevent their system from illegal activity could write a smart contract that identifies transactional red flags and prevents the transaction from being executed.

Permissionless. Users can download and install the software necessary to receive and send Bitcoins and other cryptocurrencies for free on their own. Anyone may submit transactions to the network without any authentication other than the ability to put valid signatures on transactions, demonstrating ownership of the funds being spent.

Secure. Cryptocurrency funds are locked using a public key cryptography system. Only the owner of the private key can send cryptocurrency. This use of cryptography and current computational limitations to break this cryptography bolster the security of cryptocurrency transactions. The acceptance of cryptocurrencies can be affected if differing versions of the ledger coexist during extended periods of time, or if the procedures to achieve consensus are flawed. Malicious actors may seek to profit by introducing fraudulent transactions in to the ledger and inducing other participants to verify the falsified ledger. (45)

Monetary Policy Properties

Exchangeable for Goods and Services. Cryptocurrencies' viability to perform the three traditional functions of money: a medium of exchange, store of value, and unit of account, is still in question. All cryptocurrencies can theoretically serve as a medium of exchange as in any basic bartering system. Cryptocurrencies, beyond fulfilling that technical role, must find demand for being used as a medium of exchange, which is reliant on obtaining demand as a store of value or unit of account. Cryptocurrencies are largely inadequate as a unit of account due to fluctuating demand, inflexible supply, and the absence of an authority that can manage the supply to maintain a constant value. Bitcoin has found some success in demanding a store of value due to its high degree of credibility, predictable supply, and historical resilience. (46)

Controlled supply. Many cryptocurrencies limit the future supply of the tokens. For example, Bitcoin's rate of new supply decreases in time and will reach its final number in approximately 2140. All cryptocurrencies control the supply of tokens by a schedule written in the code. This means the monetary supply of a cryptocurrency in every given moment in the future can roughly be calculated today. While there have been some discussions about how cryptocurrency supply might be governed in an automated, decentralized manner that is responsive to consumer demand, we are not aware of any existing cryptocurrencies implementing such a scheme. Cryptocurrencies which have implemented schemes for stability with respect to some fiat currency have instead relied on mechanisms for pegging to a fiat currency, such as Tether's currency-board-style mechanism holding U.S. dollar and Euro

currency reserves and pledging to redeem the cryptocurrency for the fiat currency on a 1-for-1 basis. (47)

Inherent Governance Framework. A governance system is a means of democratically resolving issues and change. In order to ensure a cryptocurrency's long-term sustainability, it is necessary to incorporate a governance structure that enables both architects and users to democratically discuss and coordinate on how the technology should evolve. (48)

No debt but bearer. Cryptocurrencies are not represented by debts, as is the case with traditional fiat money. Cryptocurrencies represent themselves and the intangible assets they are built on. Cryptocurrencies have meaning only to the extent that participants agree that they have meaning. Not being a debt or liability of a central bank does not prevent cryptocurrencies from being used as money, but it does mark a significant difference between them and national currencies. (49)

Conclusion and Next Steps

With the relative disparate needs of the various groups that are or might utilize the various forms of cryptocurrency, it is clear that no currency will meet the relative demands for all. As acknowledgement and acceptance of cryptocurrencies' feasibility increases demand from various groups, they are likely to flourish in existing and emerging markets – though it is unlikely that a single currency will be able to meet the demands of all the groups that would use it. This will likely result in the creation of new cryptocurrencies or adjustments to existing ones to give their targeted groups the satisfaction and confidence needed to move forward. The dynamics involved in these developments will determine if the market is flexible enough to meet these needs and the volatility that would come with them.

In moving forward; cryptocurrency is still in preliminary stages of development and adoption, giving rise to other challenges that have yet to be fully addressed or answered. There are many questions related to regulations and governance of cryptocurrencies for traditional markets. For example, within the current cryptocurrency taxing structure, are property or capital gains taxes appropriate for a currency? When used for transactions, should sales taxes be applied and how would they be incorporated?

Additionally, while smart contracts eliminate intermediaries by setting payment conditions into code in the blockchain, what sorts of risks could arise from vulnerabilities in contract code or unanticipated conditions? With no knowledge of the identities of the parties involved, how would an institution that used cryptocurrency be able to mitigate flaws in the contracts exploited by malicious actors? How would funds be recovered, or would they be? These sorts of questions will continue to surface as cryptocurrency tries to prove its validity in traditional markets and for institutions; an area that will require further examination. However, the developments that have progressed thus far show that cryptocurrency will continue having a growing presence, requiring governments, institutions and consumers to prepare to incorporate it into future.

References

1. **Hileman, Garrick and Rauchs, Michel.** Global Cryptocurrency Benchmarking Study. *Cambridge Center for Alternative Finance.* [Online] April 7, 2017. [Cited: August 7, 2017.] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf.

2. **Camera, Gabrielle.** *A Perspective on Electronic Alternatives to Traditional Currencies.* WWZ, University of Basel : Economic Science Institute, Chapman University, 2016.

3. **Cheng, E.** Bitcoin to surge nearly 80% to $5,000, ethereum to double, Standpoint's Moas predicts. *CNBC.* [Online] July 31, 2017. [Cited: August 6, 2017.] https://www.cnbc.com.

4. **CoinMarketCap.** CryptoCurrency Market Capitalizations. *CoinMarketCap.* [Online] August 6, 2017. [Cited: August 6, 2017.] www.coinmarketcap.com.

5. **Tasca, Paolo, Liu, Shaowen and Hayes, Adam.** The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment Relationships. *SSRN.* [Online] July 13, 2016. [Cited: August 6, 2017.] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2808762.

6. **Robertson, Kelly.** Bitcoin Regulation Around the World. *Wallet Weekly.* [Online] August 3, 2017. [Cited: August 7, 2017.] https://www.walletweekly.com/bitcoin-regulation-around-world/.

7. **Financial Action Task Force.** Guidance for a Risk-Based Approach to Virtual Currencies . *Financial Action Task Force.* [Online] June 26, 2015. [Cited: August 7, 2017.] http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html.

8. **Poon, Joseph and Dryja, Thaddeus.** The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. *Lightning Network.* [Online] January 14, 2016. [Cited: August 9, 2017.] https://lightning.network/lightning-network-paper.pdf.

9. **Hernandez-Castro, Julio, Cartwright, Edward and Stepanova, Anna.** Economic Analysis of Ransomware, p. 3. *arxiv.org.* [Online] [Cited: August 3, 2017.] https://arxiv.org/pdf/1703.06660.pdf.

10. **Bursztein, Elie, McRoberts, Kylie and Invernezzi, Luca.** Tracking desktop ransomware payments, slide 14. *Black Hat Briefings.* [Online] July 2017. [Cited: August 3, 2017.] http://www.blackhat.com/docs/us-17/wednesday/us-17-Invernizzi-Tracking-Ransomware-End-To-End.pdf.

11. **Leydon, John.** AlphaBay and Hansa: About those dark web marketplace takedowns. *The Register.* [Online] July 24, 2017. [Cited: August 10, 2017.] https://www.theregister.co.uk/2017/07/24/alphabay_takedown_analysis/.

12. **Higgins, Stan.** https://www.coindesk.com/110-million-btc-e-fined-us-vows-crackdown-unregulated-exchanges/. *Coin Desk.* [Online] July 27, 2017. [Cited: August 6, 2017.] https://www.coindesk.com/110-million-btc-e-fined-us-vows-crackdown-unregulated-exchanges/.

13. **Bitcoin Project.** How does Bitcoin work? *bitcoin.* [Online] [Cited: August 4, 2017.] https://bitcoin.org/en/how-it-works.

14. **European Police Office.** The Internet Organised Crime Threat Assessment (IOCTA) 2016. *Europol.* [Online] September 27, 2016. [Cited: August 4, 2017.] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

15. **Greenberg, Andy.** Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire. *Wired.* [Online] January 25, 2017. [Cited: August 4, 2017.] https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/.

16. **Zerocoin Electric Coin Company.** Internet Money. *Z.Cash.* [Online] [Cited: August 4, 2017.] https://z.cash/.

17. —. Technology. *Z.Cash.* [Online] [Cited: August 4, 2017.] https://z.cash/technology/index.html.

18. **Bovaird, Charles.** What Investors Should Know Before Trading Zcash. *coindesk.* [Online] November 27, 2016. [Cited: August 4, 2017.] http://www.coindesk.com/investors-know-trading-zcash/.

19. **Ali, Robleh, et al.** The economics of digital currencies. *Bank of England Quarterly Bulletin.* Q3, 2014, Vol. 54.

20. **Federal Reserve Bank of St. Louis.** Functions of Money - The Economic Lowdown Podcast Series, Episode 9. *Federal Reserve Bank of St. Louis.* [Online] [Cited: August 10, 2017.] https://www.stlouisfed.org/education/economic-lowdown-podcast-series/episode-9-functions-of-money.

21. **Redman, Jamie.** Decentralized eSports Platform FirstBlood Raises $5.5M in Minutes. *Bitcoin.com.* [Online] September 26, 2016. [Cited: August 4, 2017.] https://news.bitcoin.com/esports-firstblood-raises-5-5m/.

22. **Soper, Taylor.** Now you can use Bitcoin to buy stuff on Amazon, thanks to this Seattle startup. *GeekWire.* [Online] November 23, 2016. [Cited: August 4, 2017.] http://www.geekwire.com/2016/now-can-use-Bitcoin-buy-stuff-amazon-thanks-seattle-startup/.

23. **Bie, Nanok.** Online Wallet iPayYou Adds Bitcoins to Amazon Shopping. *Bitcoin.com.* [Online] November 22, 2016. [Cited: August 4, 2017.] https://news.bitcoin.com/ipayyou-bitcoin-amazon-shopping/.

24. **Coinbase.** The Shift Card. *Coinbase.* [Online] July 8, 2016. [Cited: August 9, 2017.] https://support.coinbase.com/customer/en/portal/articles/2228646-the-shift-card.

25. **Buterin, Vitalik.** The Search for a Stable Cryptocurrency. *Ethereum Blog.* [Online] November 11, 2014. [Cited: August 4, 2017.] https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency/.

26. **Buntinx, JP.** Top 3 Stable Cryptocurrencies Based on USD Value. *The Merkle.* [Online] March 4, 2017. [Cited: August 4, 2017.] https://themerkle.com/top-3-stable-cryptocurrencies-based-on-usd-value/.

27. **Lifespring.** Is Tether a stable cryptocurrency? *steemit.* [Online] April 21, 2017. [Cited: August 4, 2017.] https://steemit.com/cryptocurrencies/@lifespring/is-tether-a-stable-cryptocurrency.

28. **Antonopoulos, Andreas.** *The Internet of Money.* 2016.

29. **Lella, Adam.** U.S. Smartphone Penetration Surpassed 80 Percent in 2016. *comScore.* [Online] February 3, 2017. [Cited: August 4, 2017.] https://www.comscore.com/Insights/Blog/US-Smartphone-Penetration-Surpassed-80-Percent-in-2016.

30. **De Filippi, Primavera and Loveluck, Benjamin.** The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. [Online] September 30, 2016. [Cited: June 12, 2017.] http://policyreview.info.

31. **International Monetary Fund.** Virtual Currencies and Beyond: Initial Considerations. *International Monetary Fund.* [Online] January 11, 2016. [Cited: June 12, 2017.] www.imf.org.

32. **Carlisle, David.** Virtual Currencies and Financial Crime: Challenges and Opportunities. [Online] March 9, 2017. [Cited: June 12, 2017.] https://rusi.org.

33. **Woodford, Michael.** Monetary Policy in a World Without Money. *The National Bureau of Economic Research.* [Online] July 2000. [Cited: August 7, 2017.] http://www.nber.org/papers/w7853.

34. **Stephens, Luke.** Which crypto-currency has the most scalable architecture? *Quora.* [Online] July 1, 2017. [Cited: August 11, 2017.] https://www.quora.com/Which-crypto-currency-has-the-most-scalable-architecture.

35. **Lunarpages.** The Age Of Cryptocurrencies And Blockchain Technology. *Lunarpages.* [Online] June 7, 2017. [Cited: August 11, 2017.] https://lunarpages.com/age-cryptocurrencies-blockchain-technology/.

36. **Crypto Coins Market.** Qtum. *Crypto Coins Market.* [Online] July 22, 2017. [Cited: August 11, 2017.] https://cryptocoinsmarket.com/qtum/.

37. **Stafford, Philip.** *Blockchain Consortium raises record $100m.* s.l. : Financial Times, 2017.

38. **Irrera, Anna.** *Fidelity allows clients to see digital currencies on its website.* New York : Reuters, 2017.

39. **Rees, Tom.** *Regulating Bitcoin: how new frameworks could be a catalyst for cryptocurrencies.* London : The Telegraph, 2017.

40. **Securities and Exchange Commission.** SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities. *Securities and Exchange Commission.* [Online] July 25, 2017. [Cited: August 10, 2017.] https://www.sec.gov/news/press-release/2017-131.

41. **Helms, Kevin.** *SEC Declares DAO Tokens Securities and ICOs Subject to Federal Securities Laws.* s.l. : Bitcoin.com, 2017.

42. *BankThink Will the Blockchain Replace Swift?* **Skinner, Chris.** s.l. : American Banker, 2016.

43. *Managing the risks of cryptocurrency.* **BAE Systems.**

44. ***Beigel, Ofir.*** *s.l. : Cryptocoins News.*

45. ***Committee on Payments and Market Infrastructures.*** *Digital Currencies. Bank for International Settlements. [Online] November 2015. [Cited: August 7, 2017.] www.bis.org.*

46. ***Ammous, Saifedean.*** *Can cryptocurrencies fulfil the functions of money? Columbia University Center on Capitalism and Society. [Online] August 22, 2016. [Cited: August 9, 2017.]*

http://capitalism.columbia.edu/files/ccs/workingpage/2017/ammous_cryptocurrencies_and_the_functions_of_money.pdf.

47. ***White, Lawrence H.*** *Dollar-Denominated Cryptocurrencies: Flops and Tethered Success. Cato at Liberty Blog. [Online] Cato Institute, April 6, 2017. [Cited: August 9, 2017.] https://www.cato.org/blog/dollar-denominated-cryptocurrencies-flops-tethered-success.*

48. The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure. ***De Filippi, Primavera and Loveluck, Benjamin.*** *3, s.l. : Internet Policy Review, September 30, 2016, Vol. 5.*

49. ***Ali, Robleh, et al.*** *The economies of digital currencies. Bank of England. [Online] September 11, 2014. [Cited: July 31, 2017.] http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.pdf.*

50. ***Kasireddy, Preethi.*** *Bitcoin, Ethereum, Blockchain, Toke, ICOs: Why should anyone care? Hackernoon. [Online] July 5, 2017. [Cited: August 3, 2017.] https://hackernoon.com.*

51. ***Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeber.*** *Bitcoin and Cryptocurrency Technologies,Preface—The Long Road to Bitcoin. s.l. : Princeton University Press, 2016.*

52. ***Antonopoulos, Andreas M.*** *The Internet of Money. s.l. : Merkle Bloom LLC, 2016.*

53. ***Soeriaatmadja, Wahyudi.*** *The Straits Times. The Straits Times. [Online] January 10, 2017. [Cited: August 4, 2017.] http://www.straitstimes.com/asia/se-asia/indonesian-militant-used-paypal-to-fund-terror-acts.*

54. ***Schwartz, Mathew J.*** *Bye, Bitcoin: Criminals Seek Other Crypto Currency. Dark Reading. [Online] February 18, 2014. [Cited: August 4, 2017.] http://www.darkreading.com/vulnerabilities-and-threats/bye-bitcoin-criminals-seek-other-crypto-currency/d/d-id/1113864.*

55. ***Leinwand Leger , Donna.*** *How FBI brought down cyber-underworld site Silk Road. USA Today. [Online] October 21, 2013. [Cited: August 4, 2017.] https://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/.*

56. ***Tepper, Taylor.*** *Millennials Prefer Debit Cards to Credit Cards. Here's Why They're Wrong. Money. [Online] Time, October 5, 2015. [Cited: August 4, 2017.] http://time.com/money/4058491/millennials-choose-debit-credit-cards/.*

57. ***Yates, Tony.*** *The consequences of allowing a cryptocurrency takeover, or trying to head one off. Financial Times Alphaville. [Online] June 7, 2017. [Cited: July 13, 2017.] https://ftalphaville.ft.com.*

58. ***Committee on Payments and Market Infrastructures.*** *Digital Currencies. Bank for International Settlements. [Online] November 2015. [Cited: August 4, 2017.] www.bis.org.*

59. Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling. ***Brito, Jerry, Shadab, Houman and Castillo, Andrea.*** *Fall 2014, s.l. : The Columbia Science & Technology Law Review, 2014, Vol. XVI.*

60. ***Paredes, Troy A. and Schneider, Lee A.*** *Appetite for Disruption: The Business and Regulation of Fintech. Apple iTunes. [Online] May 22, 2017. [Cited: August 6, 2017.] https://itunes.apple.com/us/podcast/appetite-for-disruption-business-regulation-fintech/id1190934515.*

61. ***DeepDotWeb.*** *Dark Net Market Comparison Chart. DeepDotWeb. [Online] July 7, 2017. [Cited: August 9, 2017.] https://www.deepdotweb.com/dark-net-market-comparison-chart/.*

62. ***Paoli, Giacomo Persi, et al.*** *Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web. RAND Corporation. [Online] 2017. [Cited: August 9, 2017.] https://www.rand.org/pubs/research_reports/RR2091.html.*

63. ***Bursztein, Elie, McRoberts, Kylie and Invernizzi, Luca.*** *Tracking desktop ransomware payments. Black Hat Briefings. [Online] July 2017. [Cited: August 9, 2017.] http://www.blackhat.com/docs/us-17/wednesday/us-17-Invernizzi-Tracking-Ransomware-End-To-End.pdf.*

64. ***Cheng, E.*** *Bitcoin to surge nearly 80% to $5,000, ethereum to double, Standpoint's Moas predicts. CNBC. [Online] July 31, 2017. [Cited: August 6, 2017.] https://www.cnbc.com.*

65. ***FINRA.*** *Distributed Ledger Technology: Implications of Blockchain for the Securities Industry. FINRA. [Online] January 2017. [Cited: August 10, 2017.] http://www.finra.org/industry/blockchain-report.*

66. ***Narayanan, Arvind, et al.*** *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton : Princeton University Press, 2016.*

67. ***Kumar, Amrit, et al.*** *A Traceability Analysis of Monero's Blockchain. International Association for Cryptologic Research. [Online] April 17, 2017. [Cited: August 10, 2017.] https://eprint.iacr.org/2017/338.pdf.*

68. ***Miller, Andrew, et al.*** *An Empirical Analysis of Linkability in the Monero Blockchain. ResearchGate. [Online] April 2017. [Cited: August 10, 2017.] https://www.researchgate.net/publication/316163255_An_Empirical_Analysis_of_Linkability_in_the_Monero_Blockchain.*

Appendix A: Key Terms

Blockchain: A feature of cryptocurrency, where a digital ledger that maintains a temporal database of transactions (called blocks) via cryptographic hashing. Blockchain ledgers are distributed which prevents tampering and ensures transparency as every participant maintains and verifies copy of the ledger.

Commodity "Reserve" Systems. A type of commodity, it varies widely in scope and scale. The large-scale system of using commodity reserves to guarantee national paper currencies (e.g., the U.S. gold or silver standard) is commonly referred to as a "bullion standard". Bullion standards have the advantage of restricting a government's ability to spend more than it has in its reserves, which may limit deficit spending. The disadvantages, however, include restricting money supply, inhibiting monetary policy for large economies, and exposing the system to speculative attack.

Commodity Money. A type of commodity, it is also the use of commodities as currency dates back thousands of years and is a principal economic reality many economies today. Trading or "bartering" goods, services, and all manner of physical assets is wide spread in 1st world economies and an absolute necessity, if not a "way of life", in 3rd world economies. These systems, formal and informal, can be extremely difficult to catalog, trace, tax, or even evaluate for performance.

Cryptocurrencies. A form of virtual currency which leverages cryptographic practices to ensure secure transacting and to control the minting of additional units. Cryptocurrencies may not necessarily be redeemed. Bitcoin represents one type of decentralized cryptocurrency.

Digital Currencies. Form of fiat currency, electronically stored, accessed, and tenderable representation of legitimate physical currency. Digital currencies allow for instantaneous transacting and remote access of funds, and account for roughly 95% of all currency in the world.

Distributed Ledger Technology (DLT). A feature of cryptocurrency, where a digital recorder of ownership that differs from traditional database technology, since there is no central administrator; instead, the ledger is replicated among many different nodes in a peer-to-peer network, and each transaction is uniquely signed with a private key.

Ecosystem-Specific Virtual Currencies. Some virtual currencies are, in many ways, interchangeable with legitimate currency while others, such as currencies developed for computer gaming environments, are valueless outside their intended ecosystem. Virtual Currencies such as 'gold' in the online environment of 'World of Warcraft' can be purchased with real dollars, but cannot be redeemed for goods or services outside of the gaming environment.

Fiat Currencies. A form of money, fiat currency is a currency is a currency that is backed by the full faith and credit of the issuing government. The currency itself may be intrinsically valueless, but used in good faith that the issuing authority will ensure its redeemable value. Fiat currencies can be separated into two categories: reserve currency and proxy currency

Four Pillars of Money. 1.) Consensus; money must be adopted by a consensus of users. 2) General Acceptance; money must be widely accepted. 3) Form; money must be easy to recognize as "genuine". 4) Value; money must have an "intrinsic value" imparted by exchange of a physical commodity or acknowledgement of a reliable debt.

Money. The economics definition of money is a medium of exchange, standard of value, unit of account, store of value; or standard of deferred payment. A "practical" definition of money is more closely aligned with how most people think about money: "money is anything that is generally accepted as a means of payment". A "more useful" definition of money is brought to light by understanding the "Four Pillars" of money.

Physical (paper or coinage) currencies. Form of fiat currency in wide spread circulation and by force of law represent a medium for payment of all debts public and private

Proxy Currency. Commonly defined as a currency that closely mirrors the global valuation of a reserve currency, and might be used to hedge less liquid currencies.

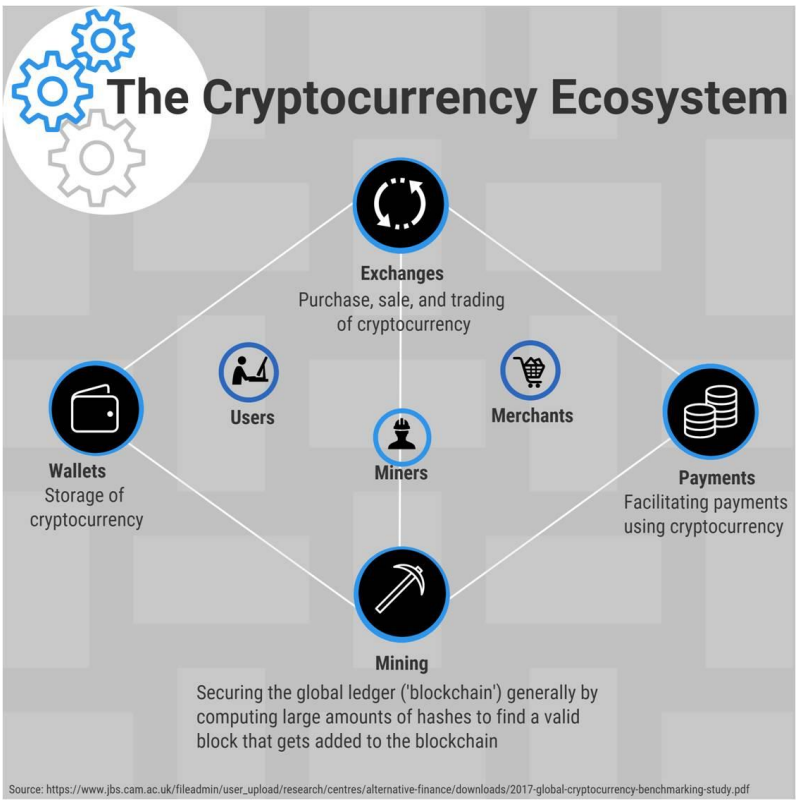
Reserve Currency. A currency that is backed by the full faith and credit of the issuing government. Reserve Currencies are typically held in sufficient quantities by other governments such that it constitutes a significant portion of their foreign exchange reserves. A reserve currency (the U.S. Dollar, the Euro, etc.) may also act as a benchmark for other global currencies.

Trustless Consensus Mechanism. A feature of cryptocurrency, where a method of authenticating and validating a value or transaction on a distributed ledger without the need to trust or rely on a central authority. These are central to the functioning of any DLT system.

Virtual Currencies. A type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community. Virtual currencies are NOT fiat currencies as they fail the simple definitions outlined above (they not being issued by a central government); however, some virtual currencies are convertible for legal fiat currency at the discretion of its user community. Virtual currencies lack sovereign state backing, legal or otherwise, and have no "intrinsic value". They are better described as commodity money or commodity currency. Virtual commodity money often has two common forms: ecosystem-specific virtual currencies and cryptocurrencies.

Appendix B: What are Cryptocurrencies?

A recent study on describes a cryptocurrency is a digital token that exists within a specific cryptocurrency system which generally consists of a peer-to-peer network, a consensus mechanism, and a public key infrastructure. There is no central authority that governs the system: instead the rules governing the system (e.g., defining what constitutes a valid transaction, specifying the total supply of the digital token and its issuance scheme, etc.) are enforced by all network participants (also called 'nodes). The entire transaction history can be independently verified by each node as everyone has a copy of the shared ledger. The shared ledger, generally taking the form of a chain of blocks comprised of transactions ("blockchain") is constantly updated via a process called 'mining,' through which new units of the native token (i.e., the cryptocurrency) are created. Anybody is free to join and leave the system at any time and there are no identified attached to users. (1)

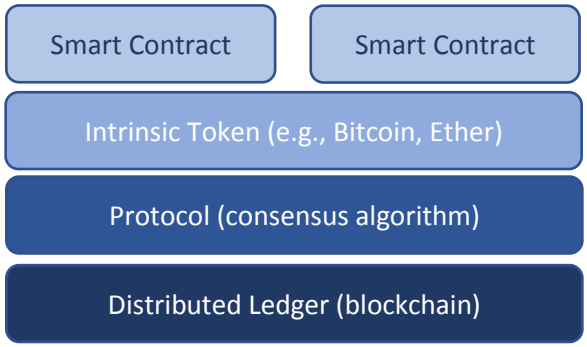


Cryptocurrency protocols may allow for the issuance of a limited or unlimited number of currency units or tokens. Cryptocurrencies are not denominated in dollars or any other sovereign currency, but instead are their own unit of value. The value of the currency is not derived from gold or government fiat, but from the value that people assign to it based on their belief that others would also value and use them.

Cryptocurrencies are governed by the protocol, or a set of rules that nodes in a network use when they transfer information or communicate. When discussing blockchain, protocol refers to the "crypto economic rules" that are enforced by a blockchain to maintain distributed consensus across the blockchain's peer-to-peer network. Cryptoeconomic rules govern a decentralized digital economy that uses public key cryptography for authentication and has economic incentives, such as tokens or cryptocoins, to ensure that the rules are followed. In general, tokens refer to units of measure, for example a Bitcoin, that are built on top of a blockchain and represent a digital asset which you own and can transfer to someone else. As compared to traditional currencies, tokens represent the currency itself (e.g., USD, EUR, etc.) and the blockchain protocol represents the monetary policy. (50)

Cryptocurrencies also allow for additional decentralized applications or "smart contracts" to be built on top of the blockchain. The additional application or smart contract adds additional communication or

protocol to the transaction, for example a set of rules for how funds are transferred between two parties or “if then” transaction rules. This additional protocol does not drive an economic incentive for the network. (50)



Appendix C: Preferred Feature Preferences by User Group