What are the potential future roles of blockchain-based cryptocurrencies in the economy?

Benjamin Malone

Senior Project Advisor: Kyle Edmonson

Abstract

The transaction of common units of currency is the basis for how our current economy operates. Cryptocurrencies are a developing class of currency that utilize a digital blockchain rather than traditional financial institutions to broker, process, and record transactions. This paper explores the potential roles that cryptocurrencies may play in the economy in the future. This analysis draws primarily on the technological function of cryptocurrencies, their relative advantages over traditional currencies, and the challenges they face for adoption. Cryptocurrencies offer many transactional benefits that make them faster, cheaper, and more reliable than customary payment methods. Problems exist within the technological infrastructure of certain cryptocurrencies, with service providers that mediate between fiat currencies and cryptocurrencies, and with the overall stability of the price of cryptocurrencies, but these issues should subside as the market matures and cryptocurrencies develop further. Aspects such as monetary policy and anonymity vary from cryptocurrency to cryptocurrency, but could act as barriers to widespread usage as a currency. Cryptocurrencies could simply continue in their current role as an alternative method of payment and type of financial security. Governments may try to regulate or ban them, but such action either would be ineffective or would block off a useful technology. However, if usage trends persist and the cryptocurrency market continues to develop, cryptocurrencies could very well become dominant currencies used within society.

12th Grade Humanities

Animas High School

5 March 2018

Part I: Introduction

Every day, parties exchange hundreds of billions of dollars, with Visa alone handling a peak of 65,000 financial transactions per second in 2016 ("Visa Inc." 2). The combination of having a common currency that people trust and the infrastructure to support the processing and verification of transactions is the basis for how our current economy functions. Financial transactions throughout history have usually consisted of exchanges of physical units of currency such as coins or bills, and centralized institutions such as banks and governments have historically managed currencies and their exchange. That is no longer the case. Today, governments are no longer the only issuers of currency, large banks and financial institutions such as Visa are no longer the only processors of financial transactions, and physical coins and bills are no longer the only stores of value. In the past decade, cryptocurrencies, decentralized digital currencies, have arisen as a form of currency and payment system. Cryptocurrencies operate independently from government banks or private financial institutions and utilize digital encryption and protocols to handle the supply of currency and the verification and security of transactions. Their usage may be limited presently, but they have the potential to revolutionize current financial structures. What roles will these currencies have in the economy in the future? Cryptocurrencies could simply continue in their current role as an alternative method of payment and type of financial security. Governments may try to regulate or ban them, but such action either would be ineffective or would block off a useful technology. However, if usage trends persist and the cryptocurrency market continues to develop, cryptocurrencies could very well become dominant currencies used within society.

Part II: Historical Context and Background Knowledge

Bitcoin and the Beginning of Cryptocurrency

In October 2008, an anonymous person or persons under the pseudonym Satoshi Nakamoto published the theory of Bitcoin, the first blockchain-based cryptocurrency, in a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." In the paper, Nakamoto cites the state of the current transactional system, stating that commerce "has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments" (1). Indeed, large financial institutions receive a massive amount of trust to process transactions, as they are necessary for mediating disputes between parties and tracking ownership of digital money. While this system is functional, the presence of intermediaries drives up the time, cost, and uncertainty within a transaction. Nakamoto states their motivation for developing the technology behind Bitcoin: "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party" (1). Bitcoin and other cryptocurrencies created that electronic payment system.

Cryptocurrencies started largely from a libertarian, anti-authority position (Sauer 117). Early cryptographers and cryptocurrency pioneers took issue with the necessity of big financial institutions to act as mediators of transactions and with governments having complete control over monetary policy and supply through fiat currency (Subramanian and Chino 27). Fiat currencies are usually national currencies, such as the US Dollar, UK Pound, or Japanese Yen, that have no intrinsic value but that governments and central banks declare valuable and as valid legal tenders. The Federal Reserve Bank is the main body in charge of setting monetary policy and therefore controls the supply, interest rate, and circulation of the US Dollar. However, many object to an unelected and unregulated institution having absolute control over the nation's

currency. Because of the traditional control and influence that financial institutions and governments have had over currency and their transaction, Bitcoin and other cryptocurrencies developed as a way for two parties to securely exchange directly with each other without relying on a financial institution to process the transaction or a central bank to control the currency.

Blockchain: The Technology Behind Cryptocurrency

Cryptocurrencies are a technological breakthrough, not only for electronic payments, but for many other industries as well. Cryptocurrencies rely on a distributed ledger technology known as blockchain. Blockchain is essentially a digital ledger that records every single transaction that has ever occurred within a network. Transactions are grouped together into blocks of information that are tied together to form the blockchain. The blockchain ledger is stored on thousands of computers within a peer-to-peer network, which allows everyone to maintain trust in the accuracy and security of the ledger. For Bitcoin, blockchain acts as a "database that contains the payment history of every bitcoin in circulation, the blockchain provides proof of who owns what at any given juncture" ("The Great Chain"). The blockchain ledger, in essence, *is* the currency. Decentralized consensus guarantees ownership of cryptocurrency: a distributed and autonomous network of computers each maintains a copy of records allowing for consensus on which transactions have taken place and therefore who owns what.

Blockchain works using cryptography, making each transaction digitally secure. For new transactions, the parties involved first agree to exchange with each other and one party sends a certain quantity of cryptocurrency to the other party's unique cryptocurrency account or "wallet" address. The large network of computers that makes up the blockchain then processes and

confirms the transaction. First, the data of the transaction, including parties involved, the amount transacted, and the time of the transaction, go through a cryptographic program known as a hash function. The hash function takes the data of the transaction and, regardless of the content or size of the transaction, converts it into a unique string of characters of a fixed length known as a hash value. Once a hash function converts data, it can never return to its original form. The hash value joins the values of other recent transactions and they become part of a new block in the blockchain. This block contains the hash values of the transactions that have occurred, a timestamp of the creation of the block, and the hash value of the previous block in the blockchain. This header then undergoes a complex cryptographic mathematical puzzle that the thousands of computers on the network solve to ensure the authenticity of the information contained within the block ("The Great Chain"). Once solved, the new block gets stored on every computer on the network and becomes a part of the blockchain; all of the transactions within the block become encrypted and permanent.

When the computers solve cryptographic puzzles, they are essentially verifying transactions. These computers devote a lot of computational resources to verifying transactions, so they receive new units of the cryptocurrency as rewards when they solve puzzles and verify blocks (Sontakke and Ghaisas 12). This is a process known as cryptocurrency mining. Through mining, transaction costs remain low, as the verifiers of transactions get compensation from the currency itself rather than its users, and the security of the network increases by attracting more computers to verify transactions. Additionally, this is how new units of currency are circulated into the economy in a transparent and non-discretionary manner. The ledger is secure by design and irreversible: because every block is linked to the previous block, editing even a single entry in the ledger would require control over a majority of the computers on the network and for

every single other block in history to be edited as well, which is virtually impossible (Nakamoto; "The Great Chain"). All told, the blockchain creates distributed consensus over the currency, allowing cryptocurrency to be a trustless, autonomous, and secure payment system.

While blockchain allows for payment systems like cryptocurrency to exist, it also has much farther-reaching implications. Blockchain is a "foundational technology," an open platform that can be developed, programmed, and manipulated to serve a variety of applications and act as the foundation for many economic, legal, and social systems (Iansiti and Lakhani). Because transactions, contracts, and records play such a big role in society, blockchain has the potential to be revolutionary. Cryptocurrency was just the first application of blockchain and distributed ledger technology. Others might include "voting, stock ownership, asset registration, notarization," and other applications that rely on record-keeping (Antonopoulos 2). Cryptocurrency changed the way that transactions can occur and the management of currency, but its underlying technology may change much more than that.

Current Applications of Cryptocurrency

Bitcoin was the first cryptocurrency, and remains the most popular cryptocurrency, but there are many more today. As of February 2018, there were approximately 1,500 cryptocurrencies hosted on cryptocurrency exchanges ("Cryptocurrency Market Capitalizations"). Some of the most popular cryptocurrencies today are Ethereum, Ripple, Litecoin, VeChain, and NEO. These cryptocurrencies have different blockchains that record their transactions and different protocols for functions such as encryption, verification, and circulation. Variations within their protocols can result in differing transaction speeds, levels of anonymity, control of supply, and other functional properties. Cryptocurrencies have ballooned

in popularity, especially in the past couple years, with the total market capitalization of all cryptocurrencies jumping from approximately US$7 billion in January 2016 to a peak of over US$800 billion in January 2018 ("Cryptocurrency Market Capitalizations").

These cryptocurrencies are currently serving roles as both a tradable financial asset and as a currency. As a currency, they are a means of payment. Every day, tens of billions of US Dollars' worth of cryptocurrency exchanges take place and the amount of cryptocurrency transactional volume and number of merchants that accept cryptocurrencies are increasing (Sahoo 53; Subramanian and Chino 32). While cryptocurrency has use today as a means of payment, a large amount of its popularity is due to speculative trading. Many treat cryptocurrency like a stock or any other financial security. Some, seeing the underlying value of cryptocurrency as a payment system, buy cryptocurrency and hold a long position, hoping for large gains over time (Sontakke and Ghaisas 12). Others, due to the high volatility of the price of cryptocurrencies, speculate on and trade cryptocurrencies in the short-term, with some of the biggest derivatives exchanges now even offering cryptocurrency futures contracts ("Factbox: Bitcoin Futures"). Whether they see usage as a means of payment or a speculative security, the popularity of cryptocurrencies is increasing but their future remains just as uncertain.

Part III: Research and Analysis

Characteristics of Currency

What is currency? What gives one unit transactional value, but makes another worthless? At its most basic level, currency is a means of payment and barter. Rather than having to exchange directly with goods and services themselves, people have adopted money as a way to store value temporarily. Currencies do not have to be physical, as a huge amount of transactions

with fiat currencies are electronic. Currencies throughout history have been commodity-based as an assurance of value, such as the usage of commodities like gold and silver as units of currency or in representative currencies, but they do not have to be. Fiat currencies are not commodity-based and have no intrinsic value; they only have the backing of a government. The only thing that a currency truly requires in order to work is the trust of the community using it. People can use currency to exchange with each other, but only if they both trust in the value of the currency. Perhaps because of how new cryptocurrencies are, their digital nature, or their lack of intrinsic value, cryptocurrency seems to be in a different category than most circulating currencies today. However, cryptocurrency is, based on most functional definitions, a currency. While cryptocurrency has use today as a means of exchange, it still has a long way to go before it has the trust, and therefore usage, of currencies like fiat currencies.

Payment Systems vs Currency

An important distinction to make in financial transactions is the system of payment and the currency used for payment. The currency is the means of payment, the money itself. This includes units of coins, bills, or even digital bits that circulate and see usage within a community. The payment system is the means of transaction, the method by which a single currency exchanges between parties. Payment systems can consist of in-person exchanges of physical units of currency, trusted intermediaries working to broker and process transactions, or even digitally encrypted and peer-to-peer transfers as with cryptocurrency. Cryptocurrencies operate as both payment systems and currencies: units of cryptocurrency circulate and are a means of payment, making it a currency, and cryptocurrency transfers are self-contained within a peer-to-peer network that stores them on the blockchain, giving cryptocurrency its own built-in payment

system. Cryptocurrencies therefore have unique advantages and potential future roles, as well as challenges and barriers, as both systems of payment and as units of currency.

Transactions

Cryptocurrency's biggest strength is as a payment system and its ability to handle transactions. The transactional capability of cryptocurrency is promising and the capacity to make transfers of "$150 million between two [cryptocurrency] accounts, in one second, for zero fees" will be extremely disruptive for the payments industry (Antonopoulos 1). The underlying blockchain technology fundamentally alters the way that people can transact with each other and the system that processes those transactions. Because the record-keeping capability of the blockchain makes intermediaries unnecessary, transactions are "directly between buyer and seller, thereby obviating the need for transaction costs (or retaining such costs to very low levels)" (Sauer 119). In addition to being almost free of transaction costs, cryptocurrency transfers are also quicker and more reliable. Cryptocurrency payments will be completed and verified as long as they are legitimate, rather than being subject to potential error through intermediaries. Cryptocurrency transactions happen instantaneously and their records become permanent within minutes, while international transfers through current systems can take several days (Raymaekers 37). Transfers through cryptocurrency are also much more secure than traditional payment systems. The blockchain itself is essentially immune to hacking, cyber-attacks, or any sort of data breach. Conversely, traditional centralized institutions and companies are constantly subject to hacking and other digital attacks, and there are often breaches and leaks of passwords and other sensitive user information. Additionally, security malfunctions are much

more problematic for centralized institutions as they hold so much user information all in one place.

Cryptocurrency provides transfers that are cheaper, faster, more reliable, and more secure than traditional payment systems and are the most promising function of cryptocurrency. It is possible that people could continue to use fiat currencies on a regular basis, but could convert to cryptocurrency and utilize the transactional capability of blockchain for money transfers such as domestic and international remittances. The reality of peer-to-peer, virtually frictionless transactions that cryptocurrency provides will disrupt and change traditional payment systems, regardless of whether people adopt cryptocurrency as a common day-to-day currency.

Price Stability

While cryptocurrencies offer many transactional benefits, they still have many barriers that they face for more widespread usage and adoption. One of the largest is the lack of price stability: the relative value of cryptocurrencies fluctuates rapidly. For instance, Bitcoin's value hit a record high of US$19,895 on December 17, 2017. On January 17, 2018, exactly one month later, the price had dropped to US$9,691, a decrease of over 50% ("Cryptocurrency Market Capitalizations"). Other cryptocurrencies face similar levels of volatility, if not even higher due to their smaller market capitalizations. The volatility of cryptocurrency is mostly a result of the infancy of the industry, speculation on the value of the technology, and uncertainty over future regulations (Sontakke and Ghaisas 17). While the volatility of cryptocurrencies may prove to be a good investment opportunity for some, it disincentivizes the public from holding cryptocurrency as an asset and using it as a currency. Because people use currency as a store of value, they rely on that value to remain stable. A currency is not usable if it loses 50% of its

value over the course of one month. Unless people convert to cryptocurrency, complete their transaction, and then convert back to fiat currency immediately, the lack of price stability endangers the viability of cryptocurrency as a common currency. However, as cryptocurrency becomes more widespread, as more people utilize it for transactions, as more businesses accept it as a payment option, and there is a better understanding of the true value of the underlying technology, then the value of cryptocurrencies will likely begin to stabilize (Sahoo 63). In turn, a more stable price would cause cryptocurrency to become more widespread, creating a cycle where cryptocurrency would become more and more trusted and used as currency. If the price does not stabilize, then the volatility of cryptocurrencies may limit them to a risky investment opportunity and a currency that is only useful in the very short term.

Technological Infrastructure

Like any other payment system, cryptocurrency relies on a technical infrastructure to support its verification and storage of transactions. The infrastructure of cryptocurrencies consists of the blockchain where transactions are stored, the network of computers that verify transactions and maintain copies of the blockchain, and the digital protocol that governs the process of verification and encryption. Within that protocol, the way that a cryptocurrency ends up working and behaving can vary greatly, resulting in different cryptocurrencies being more or less suited for different applications. For some cryptocurrencies, namely Bitcoin, their protocol and infrastructure is lacking in scalability and efficiency. In Bitcoin's protocol, the maximum size of a single block in the blockchain is around 1,400 transactions. As a result, the Bitcoin infrastructure is only able to handle around seven transactions per second, a number that pales in comparison to the tens of thousands that traditional payment processors are able to handle every

second (“The Great Chain”). If Bitcoin were to become more widespread, its ability to handle transactions would need to scale as well. Additionally, while a transaction on the Bitcoin network might occur in an instant, it still takes as much as 10 minutes for complete transaction verification, settlement, and storage on the blockchain. There is also no distinction between authorization time on the part of the buyer and settlement time on the part of the seller, just one point of full transaction verification for both parties (Kasiyanto 31). While this verification time is still much faster than most payment systems and still makes Bitcoin useful in online and international money transfers, it does make Bitcoin less compelling for applications such as in-person point of sale.

Another important aspect of the Bitcoin protocol is the process of transaction verification. Bitcoin relies on a model known as proof-of-work to maintain consensus on its blockchain. Proof-of-work requires computers on the network to solve those complex cryptographic equations and puzzles in order to track and verify transactions, the central aspect of mining. This process provides Bitcoin a necessary level of encryption and trust, but the excessive computational work done by the computers uses a lot of power. Bitcoin mining reportedly consumes more electricity than several mid-sized countries, using enough energy to power over three million US households (Mooney and Mufson). The massive amount of energy required for Bitcoin mining is problematic from both a financial and environmental point of view, and will only become a bigger problem as Bitcoin becomes more widespread and the computational work required to support it increases. All of these problems may seem big, but it is important to realize that these problems are all specific to Bitcoin and the protocol for verifying transactions that Bitcoin uses. Through altering previous protocols and developing new ones, cryptocurrencies

can overcome these challenges, and they will need to if they are to become anything close to a mainstream method of payment.

Service Providers

While the blockchain and cryptocurrency networks are completely autonomous and peer-to-peer, cryptocurrency still requires certain service providers to mediate between cryptocurrencies and fiat currencies. These service providers include exchanges that allow conversion between cryptocurrency and fiat currency and between different types of cryptocurrencies, wallet providers that maintain a digital cryptocurrency account or "wallet," remittance providers that will broker money transfers using cryptocurrency, and merchant processors that allow businesses to accept cryptocurrency and have it immediately converted to fiat currency. Given that cryptocurrency started in part to get rid of financial intermediaries, it is ironic that there is now "a huge cryptocurrency ecosystem involving a multitude of intermediaries ... all charging a fee for their services (Raymaekers 38). The necessity of these service providers, and the potential costs they may end up imposing, may nullify many of the transactional benefits provided by cryptocurrency.

Cryptocurrency service providers themselves are also facing challenges. Wallet providers and cryptocurrency exchanges are constant targets of hacking and malware. In 2014, Mt. Gox, the largest Bitcoin exchange in the world at the time, collapsed and declared bankruptcy after hackers had breached their security. A combination of negligence and poor programming allowed hackers to steal over 800,000 bitcoins from the accounts of the company and its users, a sum worth over US$450 million at the time (McMillan). Security breaches of cryptocurrency service providers such as the one afflicting Mt. Gox make cryptocurrency adoption even more

unlikely due to the risk associated with it. However, cryptocurrencies and the blockchains that store their transactions are entirely secure; only the service providers that have developed around them to mediate between fiat and cryptocurrencies face security problems. Fiat currencies are similarly free of security problems, but their financial institutions, banks, and payment processors can also be subject to breaches, and such breaches are likely to cause more damage than a cryptocurrency service provider due to their relative size. Additionally, because the service provider industry is so nascent, there has been little time for service providers to receive adequate regulation and develop appropriately secure systems. As time passes, it is likely that service providers will address and solve security issues, but the threat of increased compliance costs will always exist, making service providers a present and potential future barrier for cryptocurrency adoption,

Anonymity and Illegal Usage

Despite being digital, cryptocurrencies are largely anonymous and can be used for illegal purposes. Because all transactions go through a cryptographic hash function before being stored on the blockchain, the details of the transaction itself are indecipherable. Thus, it is impossible to connect people reliably to cryptocurrency transactions that occur. Although, the level of anonymity can depend on the cryptocurrency. Some currencies, such as Monero, are fully anonymous, while others, such as Stellar, have digital signatures that could link to individuals (Raymaekers 38). Due to the anonymity provided by cryptocurrency, illegal transactions can and do take place. The Silk Road was an online marketplace specializing in illegal goods such as drugs, weapons, malware, and child pornography that only dealt in Bitcoin. In 2013, the FBI shut down the site and seized almost US$30 million in Bitcoin from the owner of The Silk Road

(Sahoo 61). In addition to the illegal transactions that can take place, the anonymity of cryptocurrency also allows users to avoid taxes. Because of the anonymous nature of cryptocurrency, the FBI has called Bitcoin a "haven for money-laundering and other criminal activity – including ... a tool for hackers to rip off fellow Bitcoin users" (qtd. in Subramanian and Chino 31). Cryptocurrencies allow for anonymous online financial activity. Even though criminal transactions can take place with fiat currency, its anonymity is limited to cash. However, while almost all cryptocurrencies today are mostly or completely anonymous, leveraging the underlying blockchain technology could make transactions traceable and identifiable. If a cryptocurrency's blockchain did not have such a high level of encryption, all transactions would be readily available on the ledger, making taxation, law enforcement, and therefore cryptocurrency adoption much easier ("Bitcoin Transactions"). While cryptocurrency could feasibly be a traceable and public means of payment, current cryptocurrencies are well suited as anonymous online payment systems, a huge advantage for criminals and in anti-government circles, but a headache for governments, regulators, and law enforcement.

Rules and Regulation

The future of cryptocurrency will largely depend on what sorts of rules and regulations governments decide to implement. Already today, different governments place varying degrees of regulation on cryptocurrency. Ireland's government, for example, does not currently regulate cryptocurrency, while Bolivia has banned their usage outright. For purposes of taxation, consumer protection, law enforcement, and monetary control, additional regulations are likely to develop around cryptocurrency. The US currently treats cryptocurrency as property; users must report all gains and losses to the IRS for tax purposes (McKenna). Regulation in the US could

become stricter, possibly even resulting in a cryptocurrency ban, especially if illegal usage does not diminish and security issues with service providers are not resolved. Because cryptocurrencies operate within peer-to-peer networks, the regulations cannot affect the currencies themselves. Instead, regulations must govern the cryptocurrency service providers (Raymaekers 35). Any regulations placed on service providers will increase compliance costs, driving up the cost of currency exchanges and other services. If these costs become too high, then the transactional benefits brought by cryptocurrency may no longer be compelling enough for them to receive adoption as a payment system.

Regulations will also likely end up being different from country to country, as is the case now. The existence of clashing laws in separate jurisdictions is likely to "increase disputes involving conflict of laws" and is therefore "bound to increase regulatory compliance costs" (Neyer and Geva 222). With different regulations in different jurisdictions, there will inevitably be areas with much lighter regulations and restrictions than others. Hence, it is possible that service providers could simply incorporate their businesses and operations in countries with few regulations on cryptocurrency. They would then be able to run their businesses relatively unhindered through a sort of regulatory loophole, similar to how banks or other financial institutions may base their operations out of areas like the Cayman Islands. Due to the anonymous and digital nature of cryptocurrencies, the only truly effective form of restriction by a government could be an all-out ban on their usage, and even then, the technology would still exist and see usage. However, blocking the public from the valuable technologies of cryptocurrency and blockchain would cause more harm than would be prevented by banning it. The future of cryptocurrency will be in large part decided by regulators: hefty compliance costs affecting service providers or a ban on cryptocurrency usage would only bar the public from an

important technology, or, with little or ineffective regulation, the industry could continue to develop and mature.

Decentralization and Monetary Policy

One of the core aspects of cryptocurrencies is that they are completely decentralized. Cryptocurrency has no central bank setting monetary policy and controlling the supply and circulation of the currency. The decentralized nature of the currency brings up the debate over how much control the government should have over currency and what type of monetary policy is best for maintaining the stability of the currency, circulating new units of currency into the economy, and keeping inflation and unemployment under control. Bitcoin, for example, has a fixed supply and a non-discretionary system for the circulation of new units. New Bitcoins circulate through rewards given to miners for transaction verification. The total supply of Bitcoins that will ever exist and circulate is fixed. Given that the total supply of Bitcoin is public information, the rate at which new units join the economy is predictable and known publicly based on the volume of transactions handled by miners (Sontakke and Ghaisas 12).

A fixed total supply of currency is unique from fiat currencies, which have a virtually unlimited supply, and from other currency proposals, which usually advocate for a fixed rate of growth rather than fixed total supply. There are concerns that a fixed and uncontrolled monetary supply can never respond to changes in monetary demand, leading to deflation (Sauer 121). With a decentralized currency, there is no way to mitigate problems or discrepancies, potentially leaving users and entire economies at the mercy of the market. However, while monetary institutions can act as a stabilizing force, they can also cause issues such as hyperinflation through their currency creation. Issues with the monetary policy of cryptocurrency is lessened

because if a cryptocurrency were to become a dominant payment method it would still exist alongside fiat currencies and different cryptocurrencies, so there would always be alternatives. On the other hand, fiat currencies have usually been monoliths within countries, leaving the citizens with no alternatives. It is very possible that governments will try to ban cryptocurrency in order to retain a monopoly over the money supply. The decentralization of cryptocurrencies is an important part of their autonomous and independent nature, but it could end up making them unsustainable as currencies.

Innovation and Diversification within Cryptocurrencies

Cryptocurrency began with Bitcoin, but its future likely lies elsewhere. The development of other cryptocurrencies allows for innovation within the industry and an opportunity to overcome some of cryptocurrency's challenges. Already, other cryptocurrencies are replacing Bitcoin, with Bitcoin representing only about 35% of the total cryptocurrency market capitalization as of February 2018, compared to about 85% in February 2017 ("Cryptocurrency Market Capitalizations"). While still relying on the foundational distributed ledger technology, these cryptocurrencies have their own uniquely programmed protocols that change their function and capability. For instance, the second most popular cryptocurrency by market cap, Ethereum, operates on a blockchain that allows for "smart contracts," contracts that can be programmed into the platform that automatically execute themselves once certain conditions are met (Sontakke and Ghaisas 15). Other cryptocurrencies utilize different protocols for the verification of transactions. Ripple, for example, uses a "proof-of-stake" algorithm to achieve distributed consensus, rather than the proof-of-work algorithm used by Bitcoin. Proof-of-stake awards the creation of new blocks, and thus new units of currency, based on the time and quantity that users

have contributed to the network, rather than based on the amount of computational work done through proof-of-work. This model allows for a blockchain that is just as secure, but negates the need for much of the complex mathematical work done in proof-of-work systems, resulting in significantly less energy usage for the verification of transactions and settlement times that take just seconds (Buterin; White 390).

Innovation within the development of cryptocurrencies addresses and solves many of the technical infrastructure problems of cryptocurrency such as transaction speed, scalability, and power usage, and allows for variation in characteristics of anonymity and monetary policy. However, to receive widespread adoption, there likely needs to be one or several main cryptocurrencies that grow in popularity and usage, rather than thousands. Given the massive number of cryptocurrencies, achieving consensus among the cryptocurrency community about which protocol is best will be a challenge (Neyer and Geva 220). Developments with cryptocurrency technology and programming provide a solution to many of the problems facing cryptocurrency and allow for more applications of cryptocurrency, but the community must coalesce around the most practical developments in order for them to gain popularity.

Part IV: Conclusion

Cryptocurrency as a Payment System

Cryptocurrency is a revolutionary payment system. Through cryptocurrency, willing parties are able to transact in an inexpensive, anonymous, fast, and secure manner, without the need for a separate trusted party to act as a mediator. By relying on and trusting in technology, transactions are far more efficient than traditional payment methods. However, there are still a number of barriers in the way of widespread use of cryptocurrency for transactions.

Cryptocurrencies rely on their protocols and technological infrastructure to function. For some cryptocurrencies, their technological infrastructure is either too small, too slow, or too inefficient for them to be widespread global payment systems. However, thanks to developments in cryptocurrency technology, many cryptocurrencies overcome these technical infrastructure problems through their design: transactions are now verifiable in seconds rather than minutes and the system of transaction verification does not use colossal amounts of energy.

Cryptocurrency service providers are currently necessary to use cryptocurrency as a payment system. Though they have faced security problems and are nowhere near as reputable or trusted as many traditional financial institutions, it is likely that trusted providers will emerge as the market matures. The main problem faced by service providers will be regulatory compliance costs. Service providers already exact a cost for their services and regulations would drive up those costs, possibly even to the point where cryptocurrency becomes a more expensive form of transaction than fiat currency. As long as service providers are able to maintain low costs and technological developments persist in the cryptocurrency industry, cryptocurrencies will continue to be superior to traditional payment systems.

Cryptocurrency as a Currency

Cryptocurrencies are especially unique as currencies. They are both decentralized and anonymous, a stark difference from most digitally held assets today. The decentralized nature of cryptocurrencies is a huge benefit for those who object to an unelected bureaucracy having complete control over a nation's currency, but a huge weakness for those that believe a currency cannot function properly otherwise. The anonymity provided by cryptocurrencies is a boon for those who prefer to keep their lives private, but also for those seeking to circumvent the law. The

chance of regulation or restriction because they are uncontrolled and anonymous currencies still exists as a threat to the future of cryptocurrency. Although, tweaks to the protocols of cryptocurrencies could alter their respective monetary policy and levels of anonymity, making them more practical as widespread currencies.

Regardless, cryptocurrencies will never become a common currency if they do not have people's trust. The biggest obstacle for public trust in cryptocurrencies seems to be the volatility of their price. As usage and popularity of cryptocurrencies increases, the stability of their price will do the same, allowing people to see clearly the value of cryptocurrencies as a means of payment. With a stabilizing price and the ability to change monetary policy and anonymity within their protocol, there is no reason why cryptocurrencies could not exist alongside fiat currencies as dominant means of payment.

The Future of Cryptocurrency

Cryptocurrencies have the potential to revolutionize exchange within society. Cryptocurrencies are extremely effective as payment systems and unique as currencies. Given the amount of factors still preventing widespread adoption, cryptocurrencies could easily continue in their current role as a tradeable financial security and an alternative means of payment, with people converting to cryptocurrency to complete transactions but using fiat currencies as a main store of value. Governments may try to heavily regulate or ban cryptocurrencies because of the anonymity and decentralization they provide. However, such attempts would could be ineffective, as cryptocurrencies operate within peer-to-peer networks and service providers can feasibly incorporate in areas with little or no regulation. If it were successful, regulation and restriction would only bar the public from advantageous technology.

However, if cryptocurrencies receive little to no regulation, their prices stabilize, more and more individuals and businesses use them as a means of payment, and consensus and trust builds around certain cryptocurrencies and service providers, then cryptocurrencies have the potential to become a dominant form of currency used in the future.

Works Cited

Antonopoulos, Andreas M. *The Internet of Money: Talks by Andreas M. Antonopoulos*. Edited by S.H El Hariry et al., Merkle Bloom LLC, 2016.

"Bitcoin Transactions Aren't as Anonymous as Everyone Hoped." *MIT Technology Review*, MIT Technology Review, 23 Aug. 2018, www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/.

Buterin, Vitalik. "What Proof of Stake Is And Why It Matters." *Bitcoin Magazine*, BTC Media LLC, 26 Aug. 2013, bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/.

"Cryptocurrency Market Capitalizations." *CoinMarketCap*, CoinMarketCap, coinmarketcap.com/.

"Factbox: Bitcoin Futures Contracts at CME and Cboe." *Reuters*, Thomson Reuters, 15 Dec. 2017, www.reuters.com/article/us-bitcoin-futures-contracts-factbox/factbox-bitcoin-futures-contracts-at-cme-and-cboe-idUSKBN1E92IR.

Iansiti, Marco, and Karim R. Lakhani. "The Truth About Blockchain." *Harvard Business Review*, Harvard Business School Publishing, 17 Feb. 2017, hbr.org/2017/01/the-truth-about-blockchain.

Kasiyanto, Safari. "Bitcoin's Potential for Going Mainstream." *Journal of Payments Strategy & Systems*, vol. 10, no. 1, Spring2016, pp. 28-39. EBSCO*host*, fortlewis.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=114579752&site=eds-live&scope=site.

McKenna, Francine. "Here's How the U.S. and the World Regulate Bitcoin and Other Cryptocurrencies." *MarketWatch*, MarketWatch Inc., 28 Dec. 2017,

www.marketwatch.com/story/heres-how-the-us-and-the-world-are-regulating-bitcoin-and-cryptocurrency-2017-12-18.

McMillan, Robert. “The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster.” *Wired*, Conde Nast, 8 Feb. 2018, www.wired.com/2014/03/bitcoin-exchange/.

Mooney, Chris, and Steven Mufson. “Why the Bitcoin Craze Is Using up so Much Energy.” *The Washington Post*, WP Company, 19 Dec. 2017, www.washingtonpost.com/news/energy-environment/wp/2017/12/19/why-the-bitcoin-craze-is-using-up-so-much-energy/?hpid=hp_hp-top-table-main_bitcoin-205pm%3Ahomepage%2Fstory&utm_term=.72fba40c1899.

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” *Bitcoin Project*, 31 Oct. 2008, bitcoin.org/bitcoin.pdf.

Neyer, Gene and Benjamin Geva. "Blockchain and Payment Systems: What Are the Benefits and Costs?." *Journal of Payments Strategy & Systems*, vol. 11, no. 3, Autumn/Fall2017, pp. 215-225. EBSCO*host*, fortlewis.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=127077460&site=eds-live&scope=site.

Raymaekers, Wim. "Cryptocurrency Bitcoin: Disruption, Challenges and Opportunities." *Journal of Payments Strategy & Systems*, vol. 9, no. 1, Spring2015, pp. 30-40. EBSCO*host*, fortlewis.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=101799734&site=eds-live&scope=site.

Sahoo, Pradipta Kumar. "Bitcoin as Digital Money: Its Growth and Future Sustainability." *Theoretical & Applied Economics*, vol. 24, no. 4, Winter2017, pp. 53-64. EBSCO*host*,

fortlewis.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=126740808&site=eds-live&scope=site.

Sauer, Beate. "Virtual Currencies, the Money Market, and Monetary Policy." *International Advances in Economic Research*, vol. 22, no. 2, May 2016, p. 117. EBSCO*host*, doi:10.1007/s11294-016-9576-x.

Sontakke, Kaustubh Arvind and Aishwarya Ghaisas. "Cryptocurrencies: A Developing Asset Class." *International Journal of Business Insights & Transformation*, vol. 10, no. 2, Apr-Sep2017, pp. 10-17. EBSCO*host*, doi:10.1080/1540496X.2016.1193002.

Subramanian, Ramesh and Theo Chino. "The State of Cryptocurrencies, Their Issues and Policy Interactions." *Journal of International Technology & Information Management*, vol. 24, no. 3, July 2015, pp. 25-40. EBSCO*host*, fortlewis.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=122400143&site=eds-live&scope=site.

"The Great Chain of Being Sure about Things." *The Economist*, The Economist Newspaper, 31 Oct. 2015, www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

"Visa Inc. Facts & Figures." *Visa*, Visa Inc., Jan. 2017, usa.visa.com/dam/VCOM/global/about-visa/documents/visa-facts-figures-jan-2017.pdf.

White, Lawrence H. "The Market for Cryptocurrencies." *CATO Journal*, vol. 35, no. 2, Spring/Summer2015, pp. 383-402. EBSCO*host*, fortlewis.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=102976693&site=eds-live&scope=site.