The Success of Cryptocurrency

An Analysis of Several Imperative Digital Currency, For The Future

David Bruining

19 December 2020

Contents

Introduction

A global spectacle and marvel has been underway in recent years, stemming from the world's increase in technology and longing for security. From never before seen profits to security that can truly offer anonymity, all aspects of this phenomenon have one thing in common: cryptocurrency. There is much needed to learn about this ever-changing and rapidly evolving technology; however, many concerns are bubbling over this technology's ability to disrupt the traditional finance system and its doyens. One inherit and imperative characteristic of cryptocurrencies are their "trustless" systems; these digital currencies are not covertly tethered to a single nation-state, government, or other ruling body. This could be used as an argument for why such digital currencies are superior to traditional, fiat currencies. These systems are still technically tied to the networks and the organizations that operate such networks; however, they are not and may never be dependent upon federal governments such as the United States. There is a myriad of important criteria that go hand-in-hand with the argument of an anarchic system that gives users a sense of prudence going forward. Such criterion, in my belief, will be a crucial reason as to why cryptocurrencies will succeed. These standards are highlighted throughout the several digital currencies that I have chosen to be the most prosperous, most prudent, most essential, and most elementary to the future of blockchain technology and to the future of digital currencies in general. The standards I speak of include the ability to provide users with total anonymity and privacy, less volatility in the price of the underlying asset, extremely fast transaction speeds accompanied by low transaction costs, as well as the ability to provide outside, off-chain data to the blockchain. I have chosen to evaluate the following cryptocurrencies: Bitcoin ($BTC), Monero ($XMR), Tether ($USDT), Ripple ($XRP), and ChainLink ($LINK).

Monero ($XMR)

Privacy is a fundamental aspect of not only the internet ecosystem but also to that of digital currencies. The Monero cryptocurrency aids in providing its users with an axiomatically secure, private, and untraceable currency. Launched in April of 2014, Monero focuses on the decentralization and scalability of its digital coin. A central goal of the Monero organization and coin itself is to provide a low-fee, borderless digital currency that allows citizens of corrupt or broken governments to send money in and out of their perimeters (Seth, 2019). With the incorporation of egalitarian principles – meaning that all people are equal and deserving of similar opportunities – Monero is gifting economic power back to the sovereign individual. While this characteristic may make Monero one of the only digital currencies to serve as fungible, decentralized, digital cash, it is not the reason that I believe it will be essential to the future of cryptocurrencies.

The Monero coin is one of the only, if not the only, digital currency that enables completely private transactions. Monero has included ring signatures and stealth addresses to each and every transaction made on its network. Ring signatures are a special type of code that enables the sender to entirely conceal his/her identity from other participants and from the receiver him/herself. These signatures are simply anonymous signatures from a random member of the sender's group that does not reveal which member specifically signed and approved the transaction. This, of course, is done via an algorithm and the signer does not know he/she signed either. In other words, every member of the group verifies the transaction, but no one knows who signed it initially. This single aspect is one of the most imperative parts of this digital currency and has been recently removed from most larger cryptos, especially in the United States. On the opposite side of the transaction, stealth addresses hide the identity of the recipient by randomly generating addresses that are designed for a single use; new addresses are created before every transaction (Monero Outreach, 2020). Moreover, the amount of each transaction is concealed via the Ring Confidential Transactions system, also known as RingCT. The nexus of these three concepts brings a totally anonymous, unequivocally secure, and safe way to send and receive funds from nearly anywhere the world around, putting the power back in the people.

Unlike other digital coins such as Bitcoin and Ethereum, Monero uses a codebase that is known for its substantial privacy improvements, called CryptoNote Codebase. This codebase makes privacy mandatory and transparency optional (Monero Outreach, 2020). Every layer of a transaction is obfuscated: the sender's information, the receiver's information, and information regarding the transaction itself. When compared to other cryptocurrencies, Monero has more routine network upgrades, allowing for the developers to perform much needed and regular network upgrades (Seth, 2019). This ensures not only the precipitous security but also the highest quality in privacy and other features. This enables the Monero network to remain flexible and adapt to any and all opportunities or threats presented. It is for this and the aforementioned reasons that I believe the Monero network and Monero coin to be a foundational step in the future of digital currencies and a prudent look into the future of non-anonymous, identifiable transactions.

Tether ($USDT)

A large factor that one has to consider when investing funds into digital currency is the high amount of volatility that follows. If one were to invest in the traditional market – stocks, bonds, precious metals, and other securities – the volatility is seemingly low and generally follows the market. It is much less common to see stocks rise and fall ten to twenty percent in a single day, let alone precious metals or bonds. In the cryptocurrency ecosystem, this fluctuation is seen quite often. And, according to economist Peter Schiff, this is more likely than not to happen. Tether takes this volatility out of the equation and provides its users with a facsimile of real, physical, fiat money– it's just online. Tether converts cash into online currency and ties, or 'tethers' the value of the digital coin to the price of a national currency. There are many examples, such as the Euro or Yuan, but I will be mainly focusing on the United States dollar. Tether's prime focus and the reason for its design was to facilitate the use of fiat currencies in a digital world (Tether, 2020). In other words, it is a modern approach to money and allows users to transact and interact with traditional currencies on the blockchain, negating the wild volatility that is often seen in digital coins.

This low volatility can occur because Tether is anchored to physical, fiat currencies with a one-to-one ratio, backing the coin by physical reserves owned by the Tether organization. This type of cryptocurrency is known as a 'stablecoin' and represents an online coin that is pinned to real world fiats (Frankenfield, 2019). An imperative part of this coin is that it allows holders to stimulate the BTC/USD market without the need for regulation, as the user can simply hold BTC/USDT instead. What's more, transactions are completed within minutes on the Tether network, removing the settling times that traditional deposits and withdrawals from banks carry. This is extremely helpful if a user is trying to convert Currency A into Currency B or if a user is trying to send money from one party to another in a different country. In fact, Tether charges a $0.00 fee for all transactions from one Tether wallet to another. As one can imagine, international financial transfers often have vastly high transaction fees, reaching upwards of $20 to $30 (Hay, 2020). While this is not the sole reason I believe Tether to be a prudent expansion of digital currencies in the future, it surely can only aid in it.

Price stability, both in volatility and as one's reserve currency, is an imperative point in Tether's mission. The ability to move fiat currency online is, in my belief, the most important factor backing Tether. To put this into perspective, let's say a normal crypto user wishes to convert their Bitcoin into Ethereum. Not to the investor's surprise, Ethereum increases in value by ten percent. If that investor wants to secure his/her profits, he/she will have to sell Ethereum for Bitcoin. Shockingly, while the trade is being processed, Bitcoin's price falls by ten percent; all the profits are now diminished. Despite being correct about Ethereum, by taking profits and converting back into Bitcoin, the investor incurred a loss (or a break even). By using Tether, the investor only needs to be concerned with Ethereum's direction, as Tether's price does not fluctuate. The price of Tether's coin will never be anything but exactly $1.00. Tether is a medium of exchange and a mode of storage value; it is not to be confused with a medium of speculation. This coin is unlike any other digital currency on the market and helps facilitate the use of fiat currencies online. Not only can this serve as a transitional method for bringing more fiat users into the crypto realm, but it can also be a vessel for quick and parsimonious transactions.

Ripple ($XRP)

While on the subject of fast and cheap transactions, Ripple's open source protocol, in combination with its permissionless and decentralized blockchain technology, is designed to allow thousands of transactions to happen in seconds– for almost nothing. Ripple handles more transactions per second than any other digital currency in the world, facilitating upwards of 1,500 transactions per second (Ripple, 2020). And, to the surprise of many, each transaction costs an astonishing $0.00001 (yes, one one-hundred-thousandth of a dollar). Many currencies in today's market cannot be directly converted or exchanged into each other. Banks now have to use the US dollar as their reserve mediator; this leads to double commission. Banks have to convert Currency A into USD and convert that USD into Currency B (Frankenfield, 2019). Ripple is also, by definition, a mediator; however, it is cheaper to convert than USD, allowing for extremely low transaction costs. This benefits both traditional banks and the regular consumer, as transaction and conversion fees can become hefty and burdensome.

Ripple also benefits its users in the transfer of money from individual to individual and from country to country. In a normal transfer of money, individuals need to establish trust in who they send their money through. Ripple uses a medium known as Gateway that serves as the trusted link between two parties who want to make a transaction (Frankenfield, 2019). Gateway serves as the credit intermediary, receiving and sending currencies to public addresses on the Ripple network. Any individual or business, public or private, can register to open a gateway and authorize the registrant to act as the trusted middleman for the exchange of currencies or the transfer of payment on the Ripple network, RippleNet. The Gateway is designed to find transactions that are doubtful or obviously wrong (such as double spending) and prevent them from happening by incorporating an approval process. This single capability is so forward thinking and secure that large corporations and ultra-large traditional banks use it. In fact, American Express uses RippleNet to move corporate funding from their bank account in the United States to their account in the United Kingdom, all with zero lag time. This network is also backed by myriad other banks such as Santander, Axis Bank, Yes Bank, Westpac, Union Credit, and others (CoinTelegraph, 2020). What’s more, the Ripple organization is seeking out ways to eventually transform the Society for Worldwide Interbank Financial Telecommunications, also known as SWIFT. It is for this reason that I believe Ripple and the Ripple network will be a crucial part of cryptocurrency’s future and that of the blockchain.

Bitcoin and many other digital currencies rely upon a singular central authority to manage and secure transactions; conversely, Ripple is an open source, decentralized blockchain that allows confirmations to be more speedily approved, along with higher security and transaction speed overall. Furthermore, Bitcoin often gets scrutinized because of its use of energy in mining. Ripple uses less energy than most other networks, making the transaction fee affordable (Frankenfield, 2019). Bitcoins can be mined; however, Ripple was designed to never be mined. The Bitcoin network is often accused of being energy-hungry because of this mining system. The Ripple system consumes negligible power, as it has a mining-free system. I believe that this formality is one of the many reasons why Ripple will be prosperous in the future of cryptocurrency and will be a vital and all-important aspect of the blockchain.

ChainLink ($LINK)

Smart contracts, in terms of the blockchain, are used to analyze on-chain information such as crowd funding amounts, trade volume, price volatility, and other data in order to execute if/then statements, as outlined in the contracts. As blockchain technology has progressed, these smart contracts often need to know off-chain information in order to execute. ChainLink is an interoperability-focused project that has been working on solving this connectivity problem that is present in the current blockchain environment (ChainLink, 2020). In other words, ChainLink is a decentralized oracle service– and the first of its kind. Smart contracts are an imperative part of blockchain technology; however, smart contracts require data about the real world via resources like data feeds and application programming interfaces (APIs). This data, however, is external to the blockchain; the blockchain cannot directly access this critical data. ChainLink's focus and main objective is to bridge the world of on-chain data with that of external, off-chain information. This off-chain data includes: bank payments, market data, all APIs, event data, backend system data, retail payments (i.e. PayPal, Visa and Mastercard), bank payments (i.e. Chase, HSBC, and SWIFT), and data from various blockchains across the crypto ecosystem (Town, 2018). Oracles are agents that find and verify this real world information, from data feeds and APIs, and bring said data on-chain so that it can be unified and consolidated into smart contracts. Anything from investment market data, bank account balances, product purchases, election results, and so much more can be recorded to the digital ledger within the blockchain, making it accessible on-chain.

ChainLink is aimed at creating a decentralized network of oracles that can be comparable to that of Bitcoin, Ethereum, and Hyperledger blockchains. The entire process begins with on-chain contracts from the Ethereum blockchain. A major problem with current on-chain smart contracts is that they rely on one privileged party– the creator of the contract. ChainLink is providing a new kind of smart contract that binds all parties to an agreement as it is written in the contract. This counteracts the previous model by putting the trust in everyone, not just one party. According to ChainLink's founders, smart contracts replace the need for traditional legal agreements as well as centrally automated digital contracts. In the current state of smart contracts, performance verification and execution all are dependent upon manual actions from one of the contracting parties (Nazarov, 2017). A detrimental problem that smart contracts are facing is the fact that their consensus protocols inhibit the contracts to have communication with external systems that provide much needed data. Oracles seemingly solve this issue, providing connectivity to the off-chain, outside world. Unfortunately, the oracles of today are centralized services. ChainLink proposes to solve this by implementing a decentralized oracle network that allows on-chain components to gain external connectivity, as well as providing the software that powers this network (Nazarov, 2017). Blockchain interoperability is the key to blockchain's success in the future. Without the ability to verify real-world, off-chain data in a decentralized manner, then the blockchain can never truly be decentralized and smart contracts will always be controlled by a single party. This often leads to the alteration, termination, and even deletion of said contracts by said privileged party.

The ChainLink coin is “mined” by selling off-chain services and data via an API that is run by ChainLink’s network and business in order for it to become an actual oracle node within the blockchain. For this reason, $LINK is unlike any other digital coin on the market today and is providing services that so few companies are. As mentioned above, blockchain interoperability is imperative to the success of the blockchain in the future. With the help of ChainLink, such connectivity can be implemented and build a stronger, more reliable blockchain.

Bitcoin ($BTC)

Without delving into the trivial and elementary details of Bitcoin, this digital currency can possibly pave the path for the entire future of cryptocurrency. Bitcoin is a virtual currency operating on a decentralized network that is not subject to the cries or follies of central bankers, governments, or any one single authority. With the thousands of digital currencies on the market today, Bitcoin takes lead as their doyen. It is the most used, most widely accepted, and has the highest market cap of any other single cryptocurrency to date. By leaps and bounds, if not more, Bitcoin is the most versatile, adaptable, and multi-purpose digital coin available. In fact, over 120 private companies currently accept Bitcoin as a method of payment in the United States (Chapkanovska, 2020). This digital currency can be used to purchase goods or services from an ever-growing list of merchants and is even used for online gambling by almost every online gambling site. From brick-and-mortar businesses like restaurants, apartment complexes, law firms, and car dealerships to online stores like Overstock.com and Shopify, they allow for the purchase of goods via Bitcoin payments (Bitcoin, 2020). A major problem that cryptocurrencies present to the world is the difficulty of their physical use. A majority of the coins on the market cannot be used to purchase goods or services. Bitcoin is helping to bridge the gap between a dynamic, online economic system and the current, real-world economic system in place. This protean and flexible ease of payment offers endless possibilities for consumers across the globe, not to mention the countless benefits it brings to the businesses themselves.

Payment freedom is an imperative part of cryptocurrency and one that Bitcoin introduced to the world. Users of this coin can send and receive bitcoin from anywhere and at any time the world around. There are no borders to cross, no banks to hassle, no red tape from bureaucracy; users can be fully and axiomatically in control of their money. One aspect of Bitcoin that it holds over the heads of other digital currencies is the ability for the sender of Bitcoins to choose the fee that he/she is willing to pay (Bitcoin, 2020). There is no fee for receiving Bitcoin, meaning that the sender has to front whatever cost the fee will be. Oftentimes, users can choose what fee they are willing to pay; for example, a higher fee may indicate that the transaction will be processed and completed in a shorter amount of time. Moreover, the fee itself is unrelated to the amount of bitcoins a user is sending. It is entirely plausible that it would cost the same to send 50,000 bitcoins to someone as it would to only send one. The consumer is in control and given their financial authority back. With the combination of the aforementioned digital currencies and Bitcoin, the consumer is truly economically empowered.

Bitcoin also offers merchants safer, more reliable, and overall better methods for accepting payments. All transactions are secure, irreversible, and do not contain any customer's or business's sensitive and private information. This is an absolute protector for merchants worried of losses incurred by fraudulent checks, chargebacks, counterfeit paper money, and more. More so, there is no need for payment card industry compliance or point of sale terminal expenses (Martucci, 2020). Furthermore, merchants can freely expand to new territories, new countries, and new markets without the drawback of exchange rates, extremely costly POS terminal compliance, or fraud/ crime rates. Bitcoins cannot be stolen like traditional cash, and they can be protected by backup, two-factor authentication, and wallet encryption.

Bitcoin is comparable to a myriad of other virtual currencies. Frankly, there have been countless imitations of it and spin-offs of its capabilities. I firmly believe that the market is the true decision maker in regards to compatibility in the real world, the price of an underlying asset, and future implementations of the coin. The privacy, anonymity, and security are certainly akin to that of the aforementioned coins and many others, like LitCoin, EOS, and Stellar. What these coins do not possess, however, is market acceptance. Bitcoin's wide ease of use, social acceptance, worldly praise, and dynamic capabilities is what pushed it to the forefront.

Conclusion

Simply put, the cryptocurrency ecosystem is redefining and violently changing the future of finance. This digital currency is derived from grandiosely complex cryptographic encryption that is programmed to protect the network at all costs. These tokens are operated on a system called the blockchain; the blockchain acts as a public ledger of transactions that anyone and everyone is allowed to analyze and look at. Blockchain technology differs among the various cryptocurrencies, in regards to speed, security, privacy, and other aspects. This technology is often seen as one of digital currencies largest assets in the future. Every coin that is offered on the crypto exchange brings with it its own capabilities, powers, subtleties, enhancements, and security. The five crypto currencies listed above are simply the ones that I ardently believe will survive for decades to come and bring the technology of the blockchain to its precipitous. Not only are the aforementioned digital currencies beneficial to the entire market as a whole, but each bears its own unique property that aids in the future success of the market. Before writing this report, I identified four key criteria that I believed to be the most prudent, impactful, and beneficial aspects of cryptocurrency. These included the ability to provide anonymity and privacy, control its price volatility, exhibit particularly fast transactions with low cost to the user, and provide on-chain technology with off-chain data in order to enhance smart contracts. It is in my opinion that the above digital currencies embody these characteristics and are the most successful coins to do so. An investment into cryptocurrency is axiomatically an investment in the future financial system– one that is decentralized, private, and secure. The aforementioned digital currencies offer each of its users cutting-edge technology that provides advantages that are both diverse in scope and transformative in finance.

Resources

Monero. “Monero Quick Facts.” *Home - Monero Outreach*, Monero Outreach, 2020, www.monerooutreach.org/quick-facts.html.

Seth, Shobhit. “What Is Monero (XMR) Cryptocurrency?” *Investopedia*, Investopedia, 28 Aug. 2020, www.investopedia.com/tech/introduction-monero-xmr/.

Monero. “Monero Research Lab.” *Getmonero.org, The Monero Project*, Monero Research Lab, 2020, www.getmonero.org/resources/research-lab/.

Tether. *Tether*, Tether Operations, 9 Sept. 2020, www.tether.to/.

Tether. *Tether*, Tether Operations, 9 Sept. 2020, www.tether.to/faqs/.

Hay, Steven. “What Is Tether USDT - A Beginner's Guide (2021 Updated).” *99 Bitcoins*, 99 Coins International PTE. LTD, 2 Dec. 2020, 99bitcoins.com/what-are-stablecoins/tether/.

Frankenfield, Jake. “Tether (USDT).” *Investopedia*, Investopedia, 28 Aug. 2020, www.investopedia.com/terms/t/tether-usdt.asp.

Ripple. “XRP.” *Ripple*, Ripple, 22 Oct. 2020, ripple.com/xrp/.

Frankenfield, Jake. “Ripple (Cryptocurrency).” *Investopedia*, Investopedia, 16 Sept. 2020, www.investopedia.com/terms/r/ripple-cryptocurrency.asp.

Cointelegraph. “What Is Ripple. Everything You Need To Know.” *Cointelegraph*, Cointelegraph, 10 May 2018, cointelegraph.com/ripple-101/what-is-ripple.

“Decentralized Oracles for Blockchain Use Cases: Chainlink.” *Decentralized Oracles for Blockchain Use Cases* | *Chainlink*, ChainLink, chain.link/solutions.

Nazarov, et al. “ChainLink: A Decentralized Oracle Network.” ChainLink, 4 September 2017, https://link.smartcontract.com/whitepaper

Town, Sam. “Introduction to ChainLink (LINK) - The Decentralized Oracle Network.” *Introduction to ChainLink (LINK) – The Decentralized Oracle Network*, CryptoSlate, 3 Feb. 2020, cryptoslate.com/chainlink/.

Martucci, Brian. “What Is Bitcoin – History, How It Works, Pros & Cons.” *Money Crashers*, Money Crashers, 7 Aug. 2020, www.moneycrashers.com/bitcoin-history-how-it-works-pros-cons/.

“Frequently Asked Questions.” *Bitcoin*, Bitcoin Project, 2020, bitcoin.org/en/faq.

Chapkanovska, Evangelina. “Who Accepts Bitcoin in 2020? [The Complete Guide].” *SpendMeNot*, SpendMeNot, 21 Oct. 2020, spendmenot.com/blog/who-accepts-bitcoin/.