Bitcoin as a Viable Alternative to Legacy Reserve Assets:

Reasons, Risks, and Adoption

Jeffry Blake Dunson II

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2021

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial
fulfillment of the requirements for graduation from the
Honors Program of Liberty University.

_____

Robert Tucker, Ph.D.
Thesis Chair

_____

David Holder, Ph.D.
Committee Member

_____

James H. Nutter, D.A.
Honors Director

_____

Date

Abstract

Reserve assets include commodities, currencies, or other capital held by institutions as a hedge against the fluctuations of external factors. While the United States' rise to power helped establish the US dollar as the most predominant reserve asset of the past fifty years, current events & the fast pace of technological advancement has exposed some limitations in the system. Blockchain technology has allowed for assets with cryptographically verifiable integrity that fundamentally depart from the US dollar standard and has potential to overhaul reserve assets as we know it. The course of this research details the downsides of legacy reserve assets, the cryptographic innovations that make cryptocurrencies a viable alternative, and an adoption framework for interested institutions.

Bitcoin as a Viable Alternative to Legacy Reserve Assets: Reasons, Risks, and Adoption

Introduction

Reserve assets serve an important role in the balance sheet of many different entities that may hold cash in reserve. These assets are meant to serve as a store of value independent of volatile markets, allowing institutions to preserve their financial standing over time. Most recently, institutions both domestic and international have adopted the US dollar as their most predominant reserve assets. However, the system that supports this is beginning to show its age, as well as acquiring increased risk. Maintaining its status as the world's reserve asset has required continuous devaluation for the dollar, and persistent deficits to its hosting country that have begun to show symptoms which threaten the integrity of the system itself.

The advent of Blockchain technology, and its implementation in the form of cryptocurrencies such as Bitcoin, shows promise to usher in new innovations that may solve some of the risks associated with the legacy system. Despite a multitude of critics, the innovations that Bitcoin brings to the table have won out this far, with soaring demand since its inception in 2008. Its advocates paint a picture of a day when Bitcoin becomes the cornerstone of the global financial system. It is essential that every institution with value in reserve evaluate Bitcoin through the lens of both the risks of the current system, as well as the risks of being left behind by mass adoption.

Historical Background

The historical context for Bitcoin is essential to comprehending it. If one is to determine whether Bitcoin is the next chapter in the global financial system, proper understanding of the origins and risk associated with the current status quo may be beneficial. Advances in economic

technology have generated seismic changes in local and global economies throughout human history, most notably beginning with the adoption of precious metals.

The Gold Standard

The adoption of precious metals as sound money served as a great technological advancement for trade economies at scale. Divisible, scarce, and long-lasting metals such as gold & silver found use as universal commodities that allowed individuals & institutions to move the fruits of their labor in a much more efficient way, with greater value stability & security. Although more practical than hauling furs, precious metals still held limitations for everyday use, resulting in the creation of a layer of abstraction in the form of paper currencies. These were often issued by private banks, with each note backed by a portion of gold stored in a secure place. The late 19th century saw an international gold standard codified into law, with central banks setting fixed exchange rates between gold and their national currencies (Cooper, Dornbusch, & Hall, 1982).

The Bretton Woods System

European turmoil across both World Wars posed new risks, requiring a safe haven for the stores of involved countries' central banks. Gold was shipped en masse to the United States as it established itself as a global superpower, with home soil untouched by the carnage. This led to what has become referred to as the Bretton Woods system, in which many world governments began to put their faith in the United States to maintain its gold-backed dollar, tying their own currencies to it and holding US Treasuries in reserve (Klimiuk, 2016). This system, however, required the United States to run permanent deficits in order to match global demand for cash. This combined with rising inflation levels saw the weakning of public faith in the system,

causing US gold reserves to shrink and increasing instability. US liabilities eventually exceeded their gold backing, and it was clear a new system would be necessary. President Nixon formally ended the backing of dollars to gold in 1971, causing most world governments to adopt fiat currency models, issuing currency backed simply by faith in the government itself (Bordo, 2020).

Present – the US Petrodollar

A global system of fiat currencies was functionally flawed, as currencies held no value between countries and faith in a single entity's central bank had been weakened as a result of US inflation. This threatened US economic supremacy, and in response a deal was struck between the United States and Saudi Arabia in 1974. The US agreed to purchase oil from and provide protection to Saudi Arabia, and in exchange the Saudi oil exporters did their business in US dollars & invested heavily in US treasuries behind the scenes (Wong, 2016). This pushed other countries to conduct their international trade in US dollars, reestablishing US economic supremacy and creating a "petrodollar" system that largely continues to this day.

Risks Associated with the US Dollar

Although simply accepted by most institutions as their only option, the Petrodollar system holds a few key flaws that ultimately make its decline, and the need for a new system, inevitable. The most notable being what has been referred to as the Triffin dilemma, first publicly identified in the 1960s by an Belgian-American economist named Robert Triffin. The Triffin dilemma notes that any country who wishes to serve its currency as a global reserve asset must run a continuous trade deficit in order to provide enough to supply the global demand. The National Bureau of Economic Research ran a review of this dilemma and its implications to the

current dollar system and came to a grim conclusion: “Since desired reserves rise with world nominal GDP, which is growing faster than US nominal GDP, the growth of dollar reserves will raise US external indebtedness unsustainably. Either the United States will not run the current account deficits, leading to an insufficiency of global reserves. Or US indebtedness wlll rise without limit, undermining the value of the dollar and the reserves denominated in it” (Bordo, 2018, p. 13). This continual trade deficit has taken the United States from once being the world’s largest creditor nation, to its largest debtor.

Catalysts

Unrest & Disenfranchisement

The persistent trade deficit required by Triffin’s dilemma has had many ripple effects, but much of the weight has fallen on the shoulders of lower & middle class American citizens. The United States has not built its deficit by outsourcing white-collar jobs, but blue ones instead. As manufacturing jobs have moved overseas, many Americans have found themselves unable to find gainful employment without a college degree. The rapid pace of technological advancement has served as a catalyst for this, allowing small teams of engineers to leverage the internet and create tools & services to feed needs that previously may have employed thousands. Healthcare and Finance are also notable & elite industries that have experienced tremendous growth for those fortunate enough to work in them. Rural areas have been disproportionately affected by this economic shift, as the services and jobs they provide increasingly become less viable, with the best oppourtunities becoming concentrated in large cities. The US Government has a track record of supporting financial elites at the expense of the lower & middle classes, perhaps most notably in the wake of the 2008 market crash, in which Wall Street was infamously granted

billions of dollars in bailouts, while retail investors and everyday American citizens were left to fend for themselves (Horner, 2011). Wealth has become increasingly concentrated among the top 1% of citizens, while the bottom 90% face wages that have not kept pace with worker productivity and increases in family expenditures. This has led to increasing unrest and populist movements on all sides of the political spectrum (Dalio, 2021).

The United States is not unique in its experience of the effects of the current monetary system. Fiat currencies that are persistently devalued require constant competition among the financial elites to ensure the future of their status is secure. These elites have few incentives to invest in their local communities and governments, and the divide continues to grow. The lower classes see the wealthy as having the ability to fly private, work in offices high above the deteriorating streets of their cities, live in cleaner air, and shelter their lifestyles in order to separate themselves from the harsh realities of their less fortunate peers. The United States and United Kingdom are some of the wealthiest countries in the world, with extremely sophisticated healthcare systems, and yet they face declining life expectancy (Ho, 2018). Much of this can be attributed to growing disenfranchisement and deaths of despair, particularly among young Americans without a college degree. Rates of alcoholism, suicide, and opioid abuse have skyrocketed as these Americans find themselves with limited upward mobility and a system that has failed them (Case, 2015).

Public unrest has dramatically increased globally as the middle and lower classes have grown increasingly frustrated with their perceived mistreatment by society. Populist leaders such as Donald Trump in America and Jair Bolsonaro in Brazil have risen to power under the promise of change and fighting the establishment. Social and political movements have deteriorated into

violence & anarchy, whether it's conservative Americans marching on their own Capitol, the Yellow Vest riots in France, or hundreds of thousands of Black Lives Matter members and supporters taking to the streets in the middle of a global pandemic. This unrest has also been seen online & in the financial markets, a notable recent example being the targeted attack on Melvin Capital Management, a prominent investment management firm with assets in the billions. Users of r/WallStreetBets, an online forum community, managed to rally millions of retail investors to inflate the price of shares in GameStop Corp and trigger a short-squeeze. This caused Melvin to take a 53% loss in capital in a matters of days (Chung, 2021). Many of these retail investors were motivated purely by a desire to disrupt Wall Street elites, regardless of the cost to themselves in the inevitable crash that followed (Mosley, 2021). Sentiments like these potentially pose a great risk to the integrity of the US dollar, as a growing portion of the population has called for an overhaul of the financial system.

Foreign Competition

While the United States represented as much as 40% of the global GDP in 1960, its share of the global economy has steadily declined ever since, hovering around 20% in 2016, and lower today (Patton, 2016). While the country's GDP is still a disproportionate share in terms of population size, the reality is that global economy growth continues to outpace that of the US. This decreases the reliability of the US dollar as a barometer for the global economy on a yearly basis. Additionally, US competitors such as Iraq, Russia, and China have waged war against the dollar in a variety of ways. All three have intentionally and dramatically reduced their business dealt in US dollars, with Russia specifically dropping the US dollar in their export dealings from nearly 100% to less than half that (Doff, 2020). Iraq attempted to do this as well when Saddam

Hussein de-dollarized Iraqi oil. The United States made the decision to invade Iraq and remove Hussein from power in the following years, but this is not a pattern that one should expect to be replicated against the likes of larger superpowers. China announced its decision to dramatically decrease its investments in the US treauries in 2013, and has focused instead on acquiring foreign debt through trade surpluses & financing of international infrastructure projects ("PBOC Says..", 2013). Holders of the US dollar or treasuries as a reserve asset must understand the risks of these superpower struggles.

COVID-19

COVID-19 has served as a catalyst for accelerating both symptoms and negative public sentiment surrounding the sustainability of a permanent deficit. The US Government has poured trillions of dollars into fiscal stimulus & aid in order to try and keep its economy afloat despite massive lockdowns & supply chain disruptions. The funding for this came simply by injecting more cash into the economy, resulting in a nearly 20% increase in US dollars circulating worldwide ("Money Stock Measures..", 2021). This is expected to increase even more, as the government recently passed a $1.9 trillion stimulus bill (data will be available by final draft). With COVID-related restrictions pushing the American public out of brick & mortar businesses and onto the internet more than ever before, growth in the tech sector has skyrocketed, accelerating the rate at which the gap widens between those privileged enough to be a part of it, and those potentially left behind. Similar to the 2008 market crash, many believe those that have benefitted the most from government relief efforts are largely those who needed it the least. Additionally, the US Federal Reserve has been acquiring its own US Treauries at unprecedented rates, buying nearly $1.8 trillion worth in 2020 ("The Federal Reserve..", 2021). This is highly

concerning to many, as in an effort to inject cash into the economy the US is increasingly leaning against itself for support.

Technological Growth as Means for Individual Sovereignty

COVID-19 has greatly accelerated another indirect threat to the power of the US dollar. Remote work techniques & technologies were quickly pushed into the light as the result of statewide lockdowns, with many workers not returning to their offices in over a year. While many companies were considering making jobs remote-optional prior to COVID-19, it quickly became an absolute necessity for survival. Many companies have decided to keep these measures permanently in place, making remote work an option for all employees at any time (Armstrong, 2020). As the technologies and development methods for this become more robust, it will become easier each year for a company to eliminate brick and mortar offices and be run entirely on the cloud. This poses a threat to any first world economy, as companies will then have their pick of business registrations anywhere in the world, meaning countries could be in constant competition to see who can become the most appealing destination. Inklings of this have already begun to manifest themselves, with corporations such as Apple incorporating themselves in small island nations in order to shield hundreds of billions of dollars in profits from the IRS (Drucker, 2017). With small nations putting their citizenship on sale, increased access to international transportation, internet-hosted companies, and cryptocurrencies shielded from government eyes, it is easy to see a future where individuals hold the power to choose who governs them. The structure of the United States government has grown too large in size and reach to be able to compete with small nations that build themselves on low taxes and regulation-free trade. Individuals and organizations who wish to protect the integrity of their financial

reserves must be cognizant of this potential shift, and can derisk themselves by adopting stores of value independent of any nation state.

Risks - Conclusion

Institutions seeking to hold reserves in the US dollar today face a number of threats to the value of their assets, including rising inflation, weakening purchasing power, declining usage globally, negative sentiment & unrest towards its backing party, international competition, and emigration of participants into digital & international economies. Individual & organiations may want to consider looking into alternative reserve assets with scarcity & value unaffected by third-party forces. Many have pointed to gold as a solution to this problem, but gold is difficult to store and transact, and carries the risk of fluctuating supply entering the market. The digital space shows promise to generate a viable alternative, with decentralized cryptocurrencies demonstrated verifiable scarcity, high levels of security, easy divisibility, and frictionless transactions between any two internet-connected devices.

Bitcoin as a Proposed Solution

In 2008, an individual or group under the pseudonym of Satoshi Nakamoto published to a cryptography mailing list, *Bitcoin: A Peer-to-Peer Electronic Cash System*, a whitepaper for a proposed peer-to-peer (P2P) network that could facilitate “a system for electronic transactions without relying on trust” (Nakamoto, 2008, p. 8). The network was launched on January 3rd, 2009 with the creation of what is referred to as the genesis block, the first data link in a chain that now spans hundereds of thousands of blocks. The genesis block contained an embedded text of “The Times Jan/03/2009 Chancellor on brink of second bailout for banks” (Redman, 2020). Many have interpreted this as a commentary on the instability of fractional-reserve banking and

the handling of the 2008 financial crisis. Regardless of Nakamoto's original intentions, Bitcoin has grown immensely, both in terms of fiscal adoption and network size. Nodes number in the tens of thousands, with locations all over the globe (Best, 2021). Bitcoin's market capitalization at the time of this writing is just over $653 billion US dollars ("Crypocurrency Prices…", n.d.).

Core Properties

Bitcoin operates on the foundation of blockchain technology, which introduces the concept of linking "blocks," or segments of data finite in size. This is done by generating a hash for the preceding block in the chain and placing it in the data of the current block. This creates a chain that is immediately broken when any attempt to modify a past block is made, allowing a level of data integrity that was previously unprecedented. Bitcoin leverages this to create a distributed ledger, stored on thousands of nodes around the world, that stores transaction data for every bitcoin ever created. Wallets are applications or files that provide access to multiple bitcoin addresses, which are 34-character strings of letters and numbers. Each address can store a balance of bitcoin, much like a bank account. Users can generate as many addresses as they would like, and it is considered best practice to only use one per transaction. When an address is created, a key pair is created consisting of a private key for the user to keep secret, and a public key that can be shared at will. These keys are long strings of letters & numbers that serve multiple cryptographic purposes. Messages signed with a private key can have their integrity verified with the public key. Addresses are unique public keys, and the private keys are stored on the wallet. Public keys are used to receive bitcoins, while private keys approve transactions to spend them. Once a transaction is created and digitally signed, the entire bitcoin network verifies its integrity through a consensus algorithm, ensuring that no one can spend bitcoins they don't

have (“How Does..”, 2020). Every member of the network runs code locally to continuously audit transactions, making it a highly resilient verification system. The rate at which Bitcoins are distributed is programmed to decrease on a regular basis with the block creation reward cut in half every 210,000 blocks, which roughly equates to every four years. Wallets to store these coins can be found in a few different forms, being considered “hot” (Internet-connected), or “cold” (Internet-independent), as well as having the capacity to be hardware or software based. This innovation in the use of cryptographic hashing & signatures has created what many call the first mathematically verifiably scarce asset in history, with a maximum supply of 21 million bitcoin.

Storage

Software Wallets. Most software wallets hide the user’s private keys from prying eyes, only permitting individuals with the right wallet password or biometric identity to access them. Some developers have taken things a step further, supporting transactional features such as Simplified Payment Verification (SPV), or anonymity-boosting services known as “mixing,” in which coins are exchanged in an anonymous pool to reduce traceability. Some wallets support a singular cryptocurrency, while others can store hundreds of different types of coins. Software wallets are most commonly found on both desktop and mobile platforms, but in theory could be hosted on any programmable device.

Hardware Wallets. Hardware wallets have grown popular among the cryptocurrency faithful due to their ability to be completely isolated from the internet, thus placing private keys out of the reach of hackers that don’t have physical access. There is a widespread belief that in order to truly own your cryptocurrency you must have your private keys physically in hand.

Cryptocurrency exchanges, high net worth individuals, funds, and banks all typically store their keys on hardware wallets locked behind closed doors. A hardware wallet can take a variety of forms, from a QR code printed on a piece of paper to high-tech solutions that can cost hundreds of dollars. Perhaps the most prominent manufacturer of hardware wallets is Ledger, which has produced a number of wallets capable of interfacing with its software product, Ledger Live. Hardware wallets typically support a lower number of cryptocurrencies than software wallets, but many still carry support for multiple coins.

Banks & Brokerages. An appealing option to many retail investors and institutions is to entrust the custody of their Bitcoins to a third-party bank or brokerage. These are often insured, and in some circumstances can offer greater security & peace of mind. Popular exchange options have included CashApp by Square, PayPal, Coinbase, and Gemini. More traditional financial products have included the Grayscale Bitcoin trust, which holds over 600,000 Bitcoin in a product regulated by the SEC, and BNY Mellon, America's oldest bank, which made waves in February 2021 when it announced that it would begin custodying Bitcoin for its clients (Baer, 2021). It is important for institutions evaluating their options to consider that there are tradeoffs when dealing with regulated third parties. Brokerages are heavily subjected to anti-money laundering regulations, which potentially requires them to disclose identities, holdings, and transactions to government entities if requested. Any Bitcoin held by a third party is also potentially subject to breaches of said third party, it is important that a thorough review of the risks involved be conducted on a case-by-case basis.

Transactions

Transactions within a bank or exchange naturally are technically dependent on said entity's internal systems, but for those custodying their own Bitcoin there are a few different options in terms of transacting their Bitcoin. Bitcoin Core is the base Bitcoin source code and ultimately serves as the final say, but enhanced protocols have been built to attempt to facilitate more versatile functionality or faster, lower-fee payments. These most notably include SPV systems such as Electrum, as well as the Bitcoin Lightning Network.

Bitcoin Core. Bitcoin Core is the base layer of the Bitcoin network, a distributed blockchain verified by a robust consensus algorithm. Bitcoins are not represented by solid data, but transactional records are kept that can be used to determine the balance of each address. In order to initiate a transaction, node operators must input three values. The first is the input, or the address from which the sender initially received the bitcoin they would like to send. The second is the amount, which is the quantity of bitcoin to send in the transaction. Bitcoins are highly divisible, with many in the community considering one millionth of a coin to be the lowest standard increment, also known as a Satoshi. The third value is the output, or the public address that the sender would like to send their bitcoins to. This transaction is then signed with the sender's private key. Once this process is complete, the transaction is sent to the network, where the miners verify that the private key gives the sender the authority to send the bitcoins, and then add the transaction to the blockchain. Transactions on Bitcoin Core are not instantaneous, as most wallets require multiple network confirmations to verify the integrity and success of the transaction (Nakamoto, 2008).

Electrum. Simplified Payment Verification (SPV) was a mechanism proposed in the original Bitcoin whitepaper as a way to make everyday wallets more lightweight. While the Bitcoin core network operates on a peer-to-peer configuration, with all nodes on equal footing, SPV systems like Electrum operate in a client/server configuration. The wallets operate as clients, and connect to a network of servers which then connect to each other in a P2P format. This makes the client dependent on the server network for transaction verification, but benefits the client as it no longer has to dedicate the processing power needed to operate as a full node on the Bitcoin Core network ("Electrum Bitcoin Wallets…", 2019).

The Lightning Network. The Lightning Network serves as a second-layer abstraction on the Bitcoin Core network, in a different way than Electrum's implementation of SPV. Lightning creates a shared Bitcoin address between two parties, with mutually agreed upon shares of its balance. These shares can only be changed at the consent of both parties through a cryptographic invoicing mechanism, allowing transactions to occur off the blockchain. These transactions are not verified by the chain-wide consensus algorithm, but solely between the two parties. For example, each party could both deposit 1 BTC into a shared address, and if individual A wanted to make an instant payment to individual B, all they would have to do is agree that the proportions shift to a balance of 0.9 BTC for individual A and 1.1 BTC for individual B. Either party can withdraw their agreed upon portion at any time, which formalizes the balances of both parties on the Bitcoin Core ledger. By creating these "channels" between many different clients, a new network can be created that supports instant payments, without the scaling & speed limitations of the public ledger. This is widely considered to be the next step in the evolution of Bitcoin, and shows promise to usher in further adoption (Poon, 2016).

Security Threats & Rirks Associated with Bitcoin

Although Bitcoin Core's protocol is by its very nature secure, it is important that institutions assess the risks & security threats associated with Bitcoin. Effective custody of private keys is paramount, but ultimately faces the same challenges & need for vigilance of any other private data. Any abstraction laid over the Core network provides a new attack surface & presents unique security challenges, potentially manifesting themselves in large losses for trusting users.

Direct Wallet Attacks

The key item of interest for most users is protecting their private keys. If these keys are compromised, attackers can spend the victim's balances at will, with no need for consent or proximity. Wallets are simply a software or hardware abstraction designed to conceal a user's private keys, so it is important that users evaluate the risks associated with trusting a wallet developer or manufacturer. Software & hardware security mechanisms can vary widely, and are often proprietary in the interest of security, at times making it difficult to assess their trustworthiness. Past breaches and current penetration tests should be consulted to fully understand the risks, attack vectors, and actions that lead to key compromission.

Attack on Electrum Infrastructure circa 2018

In 2018, attackers conducted a Sybil attack on the Electrum network by flooding it with malicious nodes masquerading as legitimate ones. They were then used to take advantage of the fact that error messages from a server to a client regarding a transaction were transmitted in arbitrary rich text. Malicious servers would block transactions and reply with a fake update messges deceptively informing the user that they would need to update their client to continue

using the network, with a link to a convincing website populated with malicious clients. Attackers set up enough servers on the P2P network that the likelihood of connecting to a malicious one became very high. Once users downloaded a malicious client, their private keys would be uploaded to an attacker-run server and their coins immediately transferred out of their account ("Electrum Bitcoin Wallets…", 2019). It is estimated that this attack cost victims as much as 771 Bitcoin, worth over $14 million at today's exchange rates ("Cryptocurrency Prices…", 2020).

Electrum Mitigation. Mitigation of Sybil attacks like the one leveraged against Electrum often requires unconventional methods. Electrum's developers observed the attacks against their user base, and decided to intervene and attempt to protect their network. Developers immediately patched the issue and began exploiting a DOS vulnerability found in the still-vulnerable wallets in order to try and force potential targets to update before a malicious server got to them. This however provoked the attackers to respond with a DDoS attack to deny service to the legitimate servers. This is an ongoing issue at the time of this writing, with over a hundred thousand machines in a malicious botnet sustaining hundreds of gigabytes per second against legitimate servers. For now, this serves as a caution against any abstraction made to the Bitcoin network. Developers of such abstractions need to be incredibly careful, as once a P2P network is opened up, it may be irrecoverable ("Electrum Bitcoin Wallets…", 2019).

Ledger Wallet Exploitation

Although a significant attack on a Ledger wallet's core security has yet to be seen in the wild, a team of international security researchers that go by the name Wallet.Fail was able to find two different attacks that could potential compromise the trusted technology. The first was a

supply chain attack. The researchers discovered that Ledger used a sticker system on their boxes to ensure that they were tamper proof. Using a hairdryer, the researchers were able to remove and replace the sticker in order to be able to crack open the boxes without a trace. In theory, a bad actor could obtain a few wallets either from a retailer or factory, modify them in a way that compromised their integrity, and then return them to the marketplace to be bought by an unsuspecting user. Wallet.Fail's researcher then developed an implant for the Ledger Nano S that could be used in conjunction with an antennae to remotely send signals to the firmware normally associated with button presses. This could potentially be used to confirm a transaction remotely, if the attacker was able to identify the moment in time when the victim had their wallet plugged into their machine (Dale, 2018).

Another possible attack demonstrated was an atennae side channel attack. Researchers discovered a particularly long wire in the Ledger Blue that produced signals that could be picked up locally using the proper kind of receiver. They discovered that button presses each produced a slightly different signal, and trained a machine learning algorithm to be able to recognize and interpret these signals. This theoretically could be used by an attacker to listen in on the PIN codes of the victim, in order to be able to steal the Ledger and transfer away the coins at a later date (Dale, 2018).

Ledger Mitigation. Wallet.Fail's study gained a substantial amount of public attention, and the Ledger team thoroughly reviewed the disclosed vulnerabilities before issuing a statement. Ledger's security team determined that there was not a substantial need for a technical solution to either attack. Users are already encouraged to open their Ledgers and check for any implants that may compromise security. Even if an implant made it past inspection, attackers

would need to closely monitor the user's activity, likely in their home. This goes beyond the scope of Ledger's responsibility. Although the antenna attack was quite sophisticated, a more practical option would be to simply film the user as they typed in their PIN. Ledger determined that neither of these were significant threats they were capable of resolving and made no changes. Thus the onus falls on users and organizations to mitigate these potential vulnerabilities for themselves by always double checking their hardware integrity and ensuring the security of the wallet storage locations ("Still Got…", 2019).

Phishing

Like any other industry, trusted users may find themselves vulnerable to sophisticated phishing attacks. A recent example targeted users who had bought Ledger's hardware wallets from their website. An ecommerce database holding customer information, including names, email addresses, and other contact information was compromised via an API key, and the information leveraged to send requests for sensitive information, including user's recovery phrases (Powers, 2020). These requests were nearly indistinguishable from legitimate messages sent by Ledger customer support, and may have compromised unsuspecting users. It is vital that the individuals entrusted with cryptographic reserve assets be educated on the dangers of phishing, and any request for wallet recovery information should be immediately dismissed as fraud.

False Promise Scams

A variety of scams have populated on the internet that take advantage of the irreversible nature of a Bitcoin transaction. Many claim to "double' any bitcoin balance sent to a certain address. The most prominent example of this came in July 2020, when the Twitter accounts of

various world leaders & influencers were compromised. Compromised accounts tweeted out a message saying that they would charitably double any balance sent to them in the next 30 minutes. Naturally, this did not occur and the attacker simply kept the bitcoins that naïve users sent to them. Accounts compromised included Barack Obama, Elon Musk, Kim Kardashian, and others. Hundreds of users were fooled and over $100,000 worth of Bitcoin was stolen in a matter of minutes (Iyengar, 2020). As Bitcoin becomes more mainstream and less tech-savvy users are brought into the space, one can expect these types of attacks to remain somewhat effective. Many users of legacy finance are accustomed to being able to call their financial services provider and have a transaction canceled or reversed if something goes awry. The only solutions to mitigate these kind of threats is expedient flagging and removal of scams, as well as basic user education on how to avoid them.

Dusting Attacks

A huge part of the value of Bitcoin to many parties is its anonymity. Savvy attackers have found a way to compromise this through what has been dubbed a *Dusting Attack*. Dusting Attacks exploit how wallets handle tiny fractions of cryptocurrencies. Typically a wallet has many addresses for the sake of untraceability on the blockchain. However, nearly every time there is a transaction there is a very tiny amount of any given coin left behind. This is reffered to as *dust*, and wallets keep these fractions from being lost forever by *sweeping* them together when they go to make a transfer. An attacker that sought to piece together what addresses make up a user's financial network can send a tiny fraction to a known address. That fraction is then traceable as it operates on a public blockchain. The attacker can observe what addresses that dust is swept into and where it gets transferred. If the dust touches a single account that could contain

real-world identifying information, such as any US regulated cryptocurrency exchange, that user's anonymity can be determined and the privacy of their holdings elimintated (Mapperson, 2019).

The mitigation strategy against dusting attacks simply involves wallets having an option to disable the sweeping function, and instead mark all tiny fractions as "do not spend." While this may lose them a few US cents here and there, many users would see it as a small price to pay for privacy. Ledger has implemented this in their hardware wallets, and many software wallets have begun to as well (Young, 2020).

Institutional Adoption

Microstrategy CEO Michael Saylor made waves in August 2020 when he announced his decision to add $250 million in Bitcoin to his company's balance sheet. He has since doubled and tripled down on his decision, with the company reaching over $1B in total Bitcoin purchases in 2020 (Kharif, 2020). Saylor determined that a move like this was strategically advantageous for his company, and was quoted as saying he believed that keeping their treasury holdings in Bitcoin was less risky than holding US dollars. With tumbling US treasury yields and consistently growing asset prices, Microstrategy faced an estimated 20% decrease in purchasing power for their reserves each year. Bitcoin presented itself as an asset with verifiable scarcity, that did not require Microstrategy to tie themselves to a real estate business, equity in other companies, or any world government (Kharif, 2020). This decision has paid off, both in treasury growth and a 700% increase in company stock price since the announcement (Stankiewicz, 2021). Saylor's decision opened the gates for further institutional adoption. Payment processor Square acquired $50 million in Bitcoin in August 2020, and electric automaker Tesla announced

in February 2021 that it would be adding $1.5 billion worth to its balance sheet. Instiutions looking to preserve their purchasing power and hedge against the US dollar may look to Bitcoin as a reserve asset, but must take the proper steps they do so in a secure, legally compliant, and financially advantegous way (Domonoske, 2021).

Legal Compliance

Legislation surrounding the addition of Bitcoin to a balance sheet is beyond the scope of this research, but is something that institutions must be extremely vigilant on both during the acquisition process, and on an ongoing basis. One of the biggest risks that Bitcoin faces is government interference in attempt to preserve the status quo, and institutions must properly prepare themselves to remain compliant.

Acquisition

When evaluating the approaches to acquiring Bitcoin in the volume necessary for it to serve as a reserve asset, institutions must take into account a few key factors. These include privacy, cost, ease of withdraw, and security. The importance of each will determine the options and courses of action possible. While Bitcoin's transactional algorithm is inherenetly trustless, meaning it is always algorithimically fair, the vast majority of methods for conversion between Bitcoin & fiat or other cryptocurrencies are not. Onboarding into Bitcoin can pose greater threats to asset security than any other part of the custody process, and is important that interested parties evaluate their options carefully.

Private Sales

The most basic form of acquisition is through a private sale. This can be brokered between two parties either directly, or through a middleman service. The two parties would agree

on a price, and facilitate a simultaneous wiring of fiat to the seller, and transfer of Bitcoin to the buyer. Agreements like this require a tremendous deal of trust between the two parties, as the differences between dollar-based financial systems & Bitcoin's network do not allow for a trustless transaction, and Bitcoin transactions are always permanent. It is highly important that buyers or sellers looking to employ this method be aware of the risks, and only partake in transactions with reputable & trusted individuals. Any institution looking to do this should make sure they enter a binding & legally enforceable agreement, so that any failure to uphold the deal can be brought before a court of law. This option allows for instantaneous private custody of funds, as the assets are never handed to the middleman. This is not a secure acquisition method for the needs of most buyers, but in cases where high levels of privacy are needed above all else, may be a potential course of action.

Retail Exchanges

The most common form of acquisition globally, retail exchanges offer a trusted platform to broker sales between all types of investors. Many trusted options, with daily volumes in the tens of billions, are available and can provide ample liquidity to interested buyers. Exchanges are typically heavily insured against breaches and errors, providing peace of mind to buyers concerned with the safety of their assets. While these exchanges typically cater to the everyday, individual investor, they can serve larger clients as well. This approach does not offer much in the way of privacy, as most exchanges require account holders to disclose identities & intentions, as well as providing transaction data to governments in order to comply with anti-money laundering (AML) regulations. A key disadvantage to this approach for large buyers is the risk of moving the market in a way that negatively affects the cost basis. Institutions must be willing to

be patient and develop a strategy to avoid being the victims of self-generated volatility. Dividing up purchases into as many transactions as possible and executing them at regular time intervals over an extended time period is the approach many take, with Microstrategy executing their initial buy in 88,617 transactions over 76 hours (Saylor, 2020). Another downside to the use of an exchange is ease of withdraw. Many exchanges require a holding period before withdraws are able to made, potentially causing hiccups for time-sensitive buyers.

Institution-Exclusive Platforms

Many brokerages & exchanges exist that cater only to institutions or high-dollar investors. These typically offer similar systems and arrangements to retail exchanges, but can provide some key advantages to large entities, including lower fee rates, more comprehensive insurance, and insured custody services that don't require investors to fret over the storage of their assets.

Decentralized Finance (DeFi)

Although in its infancy at the time of this writing, DeFi represents an entirely new technology stack, focused on offering all the same transactional services found in traditional finance in a distributed and decentralized manner, eliminating the middleman and associated roadblocks. For buyers with a high degree of technical competency, this may be a viable options but carries substantially more risk than purchasing through a centralized provider. Transactional mistakes are permanent, irreversible, and easy to make for inexperienced users. Fees are still present, but vary according to market volume and demand. This is not currently a viable or recommended option for the vast majority of institutions.

Storage

Third-Party Solutions

Many institutions may elect to custody their Bitcoin via a third party. A myriad of options are available, with varying levels of security & insurance. This is best for institutions that may not have the resources to custody their own coins, or those that are beholden to stakeholders that would have a greater peace of mind entrusting their assets to a reputable, professional solution.

Private Wallets

Institutions confident in their ability to securely custody their own reserves may elect to do so through hardware or software based wallets. Best practice recommends that assets be stored in multiple, cold hardware wallets, with organizational security policies that prevent any one individual from being able to steal or otherwise maliciously transact assets.

Conclusion

The above sections explore the technological innovation of Bitcoin as it relates to its viability as a reserve asset. The US Dollar has traditionally served as the standard reserve asset, but faces threats to its stability. Bitcoin is widely considered to be the first asset with mathematically verifiable scarcity, and solves many of the risks associated with the US Dollar system. Because of its decentralized network, Bitcoin becomes more robust and efficient the more that it is adopted. Every institution must make a decision in the coming years on where Bitcoin fits in their asset structure if at all, properly weighing the risks both of custodying Bitcoin, and of being left behind should an escape velocity of adoption be reached.

References

Armstrong, B. (2020, May 21). Post-COVID-19, Coinbase will be a remote-first company. Retrieved February 09, 2021, from https://blog.coinbase.com/post-covid-19-coinbase-will-be-a-remote-first-company-cdac6e621df7

Best, R. (2021). Bitcoin – Statistics & Facts. Retrieved February 02, 2021, from https://www.statista.com/topics/2308/bitcoin/#:~:text=As%20of%20July%2020%2C%20this,grown%20rapidly%20since%20early%202016.

Baer, J. (2021, February 11). WSJ news exclusive | bitcoin to come to America's Oldest Bank, BNY Mellon. Retrieved February 11, 2021, from https://www.wsj.com/articles/bitcoin-to-come-to-america-s-oldest-bank-bny-mellon-11613044810

Bordo, M.D. The Imbalances of the Bretton Woods System 1965 to 1973: U.S. Inflation, the Elephant in the Room. *Open Econ Rev, 31*, 195–211 (2020). https://doi-org.ezproxy.liberty.edu/10.1007/s11079-019-09574-2

Bordo, M., & McCauley, R. (2018). Triffin: Dilemma or Myth? *National Bureau of Economic Research Working Paper Series, 24195*. doi:10.3386/w24195

Case, A., & Deaton, A. (2015). Rising morbidity and mortality in midlife among white non-Hispanic Americans in the 21st century. *Proceedings of the National Academy of Sciences of the United States of America, 112*(49), 15078-15083. doi:https://doi.org/10.1073/pnas.1518393112

Chung, J. (2021, January 31). Melvin Capital Lost 53% in January, Hurt by GameStop and Other Bets. Retrieved April 21, 2021, from https://www.wsj.com/articles/melvin-capital-lost-53-in-january-hurt-by-gamestop-and-other-bets-11612103117?st=nkgd4es4kgjua0k&reflink=article_copyURL_share

Cooper, R. N., Dornbusch, R., & Hall, R. E. (1982). The Gold Standard: Historical Facts and Future Prospects. Brookings Papers on Economic Activity, 1982(1), 1. doi:10.2307/2534316

Cryptocurrency Prices, Charts And Market Capitalizations. (n.d.). Retrieved December 05, 2020, from https://coinmarketcap.com/

Dale, B. (2018, December 31). Security Researchers Break Ledger Wallets With Simple Antennae. Retrieved December 05, 2020, from https://www.coindesk.com/security-researchers-break-ledger-wallets-with-simple-antennae

Dalio, R. (2021). *The Changing World Order: Why Nations Succeed and Fail*. Simon & Schuster.

Doff, N., & Biryukov, A. (2020). Russia Ditches the Dollar for Bulk of Its Exports to China. Retrieved February 11, 2021, from https://www.bloomberg.com/news/articles/2020-08-12/russia-ditches-the-dollar-for-bulk-of-its-exports-to-china

Domonoske, C. (2021, February 08). It doesn't get More BUZZY than This: Tesla is INVESTING $1.5 billion in bitcoin. Retrieved February 12, 2021, from

https://www.npr.org/2021/02/08/965494932/it-doesnt-get-more-buzzy-than-this-tesla-is-investing-1-5-billion-in-bitcoin

Drucker, J., & Bowers, S. (2017, November 06). After a Tax Crackdown, Apple found a new shelter for its profits. Retrieved February 09, 2021, from https://www.nytimes.com/2017/11/06/world/apple-taxes-jersey.html

Electrum Bitcoin wallets under siege. (2019, April 23). Retrieved December 05, 2020, from https://blog.malwarebytes.com/cybercrime/2019/04/electrum-bitcoin-wallets-under-siege/

Ho, J. Y., & Hendi, A. S. (2018). Recent trends in life expectancy across high income countries: Retrospective observational study. *British Medical Journal, 362*. doi:https://doi.org/10.1136/bmj.k2562

Horner, J. (2011). Clogged systems and toxic assets. *Journal of Language and Politics, 10*(1), 29–49. https://doi.org/10.1075/jlp.10.1.02hor

How Does Bitcoin work? Deep dive into technical aspects of Bitcoin. (n.d.). Retrieved December 05, 2020, from https://crypto.com/en/university/article.html?category=crypto101.

Iyengar, R. (2020, July 16). Twitter blames 'coordinated' attack on its systems for hack of Joe Biden, Barack Obama, Bill Gates and others. Retrieved December 05, 2020, from https://edition.cnn.com/2020/07/15/tech/twitter-hack-elon-musk-bill-gates/index.html

Kharif, O. (2020). CEO Says Bitcoin Is Safer After Moving Firm's Cash to Crypto. Retrieved February 10, 2021, from https://www.bloomberg.com/news/articles/2020-09-22/ceo-says-bitcoin-is-safer-after-moving-firm-s-cash-to-crypto

Klimiuk, Z. (2016). The principles and operation of the Bretton Woods international monetary system in the years 1944–1971. The reasons for its collapse. *Internal Security, 8*(2), 225-257. http://dx.doi.org.ezproxy.liberty.edu/10.5604/01.3001.0010.2280

Mapperson, J. (2019, August 15). Understanding Litecoin's Dusting Attack: What Happened and Why. Retrieved December 05, 2020, from https://cointelegraph.com/news/understanding-litecoins-dusting-attack-what-happened-and-why

Money Stock Measures - H.6 Release. (2021). Retrieved February 09, 2021, from https://www.federalreserve.gov/releases/h6/current/default.htm

Mosley, T., & Hagan, A. (2021, January 29). WallStreetBets, Reddit, GAMESTOP: What's going down on Wall Street? Retrieved February 02, 2021, from https://www.wbur.org/hereandnow/2021/01/29/wallstreetbets-reddit-gamestop

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer electronic cash system. Retrieved February 2, 2021, from https://bitcoin.org/bitcoin.pdf

Patton, M. (2016, February 29). U.S. role in global Economy Declines nearly 50%. Retrieved February 11, 2021, from https://www.forbes.com/sites/mikepatton/2016/02/29/u-s-role-in-global-economy-declines-nearly-50/?sh=40524a4d5e9e

PBOC Says No Longer in China's Interest to Increase Reserves. (2013, November 21). Retrieved February 11, 2021, from https://www.bloomberg.com/news/articles/2013-11-20/pboc-says-no-longer-in-china-s-favor-to-boost-record-reserves

Poon, J., & Dryja, T. (2016) The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments - Version 0.5.9.2. Retrieved February 11, 2021, from https://lightning.network/lightning-network-paper.pdf

Powers, B. (2020, November 02). Ledger Customers Targeted by 'Convincing' Phishing Attack. Retrieved December 05, 2020, from https://www.coindesk.com/phishing-attack-ledger-cryptocurrency-wallet

Redman, J. (2020, January 03). A Deep Dive Into Satoshi's 11-year old Bitcoin Genesis Block. Retrieved April 21, 2021, from https://news.bitcoin.com/a-deep-dive-into-satoshis-11-year-old-bitcoin-genesis-block/

Saylor, M [@michael_saylor]. (2020, September 18). *To acquire 16,796 BTC (disclosed 9/14/20), we traded continuously 74 hours, executing 88,617 trades ~0.19 BTC each 3 seconds. ~$39,414 in BTC per minute, but at all times we were ready to purchase $40-50 million in a few seconds if we got lucky with a 1-2% downward spike.* [Tweet].

Stankiewicz, K. (2021, February 10). Before Tesla's bitcoin play, this company bought first and may have inspired Elon Musk. Retrieved February 10, 2021, from https://www.cnbc.com/2021/02/09/why-microstrategy-shares-surged-after-teslas-1point5-billion-bitcoin-buy.html

Still Got Your Crypto: In Response to wallet.fail's Presentation. (2019, May 15). Retrieved December 05, 2020, from https://www.ledger.com/chaos-communication-congress-in-response-to-wallet-fails-presentation

The Federal Reserve Holds More Treasury Notes and Bonds Than Ever Before. (2021, January 27). Retrieved February 11, 2021, from https://www.pgpf.org/blog/2021/01/the-federal-reserve-holds-more-treasury-notes-and-bonds-than-ever-before

Wong, A. (2016, May 30). The Untold Story Behind Saudi Arabia's 41-Year U.S. Debt Secret. Retrieved January 14, 2021, from https://www.bloomberg.com/news/features/2016-05-30/the-untold-story-behind-saudi-arabia-s-41-year-u-s-debt-secret

Young, M. (2020, September 18). Ledger wallet upgrade can prevent 'dusting attacks'. Retrieved December 05, 2020, from https://cointelegraph.com/news/ledger-wallet-upgrade-can-prevent-dusting-attacks