Integrated Crypto; And Why That's Good for Investors

Cryptocurrencies have found their way into many investment portfolios and will continue to find their way into many more. The purpose of this paper is to provide a perspective on the history and processes of these unconventional assets to show that their integration into conventional investment and oversight processes makes many of the highlighted dark market risks less relevant to investors, while also making some less discussed or understood technology and governance risks more relevant. The style of this article may be somewhat unconventional for an academic publication as, just like a crypto exchange, it is an attempt to bridge two audiences.

Peter Horne
has worked for over 30 years in product and technology development in the financial services industry, and has worked in Australia, the USA, and Hong Kong. Peter maintains an active interest in developing cybersecurity and cryptocurrency systems, and was credited by the New York Times for discovering the Superfish Spyware (https://bits.blogs.nytimes.com/2015/02/19/researcher-discovers-superfish-spyware-installed-on-lenovo-pcs). Peter is also a Research and Development Associate at Northfield Information Systems and holds a B.Sc. (Hons) from the University of New South Wales.

PREFACE

Cryptocurrencies, of which Bitcoin and Ethereum are the most popular, are a hot topic in investment markets. It's driven by many things – part thematic in the search for risk management in an unusual monetary policy environment, part fear of missing out driven by massive price gains, part timing as the technology matures and achieves greater acceptance, and perhaps a large part - fashion and adoption into modern culture. But as these new assets, if indeed they are and remain assets, take their place inside the investment process, we cannot deny the fact that Bitcoin is also the first currency of the "dark markets," which is just a euphemism for technology enabled crime. The recent JBS and Colonial Pipeline hacks show that Bitcoin is still a handy currency that replaces the unmarked bills and wire transfers to Swiss bank accounts that used to be favored by international criminals. And because the 21st century version of the ransom and hijacking attacks of time eternal are modernized to be ransomware and network hijacking cyberattacks, it follows that the currency of these crimes are also in the cyber realm. But likewise, law enforcement and regulators are moving with the times and policing cyberspace. Not all the Bitcoin paid for the Colonial Pipeline ultimately made it into the hands of the criminals because the FBI was involved in the process, and the information and knowledge gleaned from the process will be used for years to come as institutions and culture respond. Dread Pirate Roberts, who started the Silk Road, is in jail.

In this paper, I make the argument that cryptocurrencies are being cleaned up and sanitized as adoption integrates them into the existing systems of financial regulation and control. I am neither star struck nor glibly wiping away facts about cryptocurrencies, but they are in effect, being cleaned and layered into the financial system by the financial system itself, and they are increasingly useable inside normal investment processes and so people will use them if they can perform a valid function inside valid investment risk management. If you are in investment markets and you think that the cryptocurrencies of old will bring new opportunities to skirt tax and oversight, you are naïve. So, while I make the case that crypto is becoming cleaned up and integrated into existing control systems, the subtext is also that anyone who uses it better also ensure they are using it for clean purposes, or you will suffer your fate for trying to use a very clever technology to do very dumb things.

INTRODUCTION

Cryptocurrencies are moving into town whether you like it or not. The dodgy punk kid with a bad attitude, questionable entertainment choices, parents from the wrong side of the track, and no manners is moving in, and they are bringing their entourage with them. The young people are turning up to the party at an unstoppable rate, and old hipsters are trying to get into the action with the cool kids, too. The mayor is getting complaints, the police harassment is being ignored, and the old people are sucking their teeth and complaining about the noise. Some say it is the future, others say it is a passing phase, and Buffett and Munger say it's just plain evil. There is something in it for everyone in the Twittersphere.

It is quite amazing when you think about it, that Bitcoin has only just got to high school and Ethereum is still in grade school. But with the recent listing of Coinbase, the disclosure of sovereign wealth funds investing into crypto, Wall Street banks such as Goldman Sachs, and Asset Managers such as Fidelity all publicly participating with crypto focused business lines, and the drive to release crypto ETFs, it is safe to say that cryptocurrencies are entering the mainstream conversation and mainstream portfolios.

Given the overwhelming speed at which cryptocurrencies are now appearing on the agenda of investment decision makers, I believe that there is a lot of misunderstanding around the broader questions of what exactly are these assets that we are putting inside existing investment processes, and what does it mean to use mechanisms that were designed to circumvent financial control inside systems that rely on financial control. To jump to the answer to this question, it is that the cryptocurrencies held in investment portfolios are moving away from the dark markets that made them money. The cryptocurrencies that are held in portfolios are being "sanitized by regulation" as they are integrated into the money management system and that is a good thing. The market has voted and started to put a value on cryptocurrencies as an investment, but the regulators have also woken up and started to put a very hard stop on them becoming alternatives to nation state (or "fiat" from the Latin "let it be so" or more simply, because the government says it's the money you can use) currencies with the effect of cancelling many of the attributes that are popular discussion points. This also creates new risks that need to be understood, especially within the geopolitical context.

What I want to do in this paper is give the reader a perspective that comes from watching the "freedom experiment" move from its roots as an attempt to replace nation state money, to Bitcoin's new place as a proposed hedge against fiat currency debasement, and Ethereum's utility for experiments in making markets open and programmable. I will look at the history and mechanisms of cryptocurrencies and show how they are far from their original purpose, and I will use that to build the case for the new risks that come to the fore while the original and most discussed risks are irrelevant and move to the background.

THE BEGINNING

I find that the best place to start when explaining something that is complex is to start at the very beginning – what problem is this thing trying to solve and for whom? So, let's anchor cryptocurrencies into a historical and utilitarian frame. The realization of cryptocurrencies started well before Bitcoin. Fringe technologists, the most documented being those who coalesced around the cypherpunk mailing lists, have been working on technology to "beat the man" since the original MIT hacker group just wanted to get socialist about shared computer time. Many diverse people, and for even more diverse reasons, have been interested in creating technology outside of corporate and government control structures. Their reasons ranged from freedom of speech, anarchist thought experiments, plain old orneriness, self-righteousness, academic and commercial reasons, through to bored clever people and enterprising thieves. Basically, people have been chipping away at using technology to break traditional control structures as and when new technology became available to experiment and develop new ideas and disruptive business models. This dynamic has meant that cryptographic and peer to peer techniques have been at the forefront of many technology innovations. Mail relays to hide identity in public discussion groups, anonymous online chat, peer-to-peer music sharing using the gnutella net followed by BitTorrent, document drop sites, and good old PGP email encryption and the web of trust, were all technologies that were developed by people who were trying to solve the problem of creating information sharing and communication tools that governments and corporations could not control.

And so, while cryptocurrencies are suddenly popular, they didn't just pop out of nowhere; they built on a whole tradition of people wanting to break control structures, and it was from the techniques and approaches that came from what was done before that helped cryptocurrency attack the apogee of controlled systems – the money system. And so it started as a thought experiment among a rag tag group of maybe libertarian gold bugs, but definitely ornery nerds, focused on how technology could be used to create a system where people transact with a digital version of gold that was scarce and could not be debased by "profligate" politicians, transact in a way that was free of the "usurious" middle men who clipped the ticket and could control access to the system, and of course, it should be anonymous like a cash transfer under a restaurant table so transactions couldn't be "censored."

Of course, computers could store records and the internet could transmit them, so creating ledgers and messaging transactions was old tech. The main technical challenge was how to solve the "double spending" problem which is knowing how someone hasn't already given away the digital gold that they are going to give to you. Those maligned middlemen did provide a very valuable function – they said who had what, who had spent what, and were regulated by "the man" to ensure stability in a fractional reserve banking system. And so, the unsolved problem was how to remove the people we can't trust in trust positions and replace them with a digital gold system that didn't need to trust anything other than an algorithm that could not be changed. The solution came in the famous Satoshi Nakamoto "white paper" that proposed Bitcoin.[1]

That "Satoshi Nakamoto" is a pseudonym is already punk in the first instance, but the use of the term "white paper" added another layer of politics to the proposal. The history of the "white paper" is that it was a political document created by Winston Churchill where he made a policy proposal and made it available for discussion, as opposed to actual formal policy documents which were contained in "blue books." Perhaps "policy" is a bridge too far for punks; a white paper allows you to pronounce policy with some wiggle room before it's formal. But to be punk is to be political even if it is attempting change from the "wrong" direction. And politics is about pragmatism; working with what is there to solve the problem in front of you. So, the white paper proposed by Satoshi Nakamoto to describe Bitcoin didn't actually invent anything; it was a construction of existing technology. But it was laser focused on the problems that needed to be solved to create a trustless money system that solved the "byzantine general" problem where untrusted actors can operate inside a process that is in aggregate, trustworthy. These problems were – 1) money creation, 2) a way to transfer it person to person to effect payments, and 3) enabling the network of users to know that coins have been transferred from one person to another so that the money couldn't be "double spent" (the same coin given from the same person to two different people).

MONEY CREATION

Much ado is made about how cryptocurrencies are created, particularly as people search for the "intrinsic" value of the cryptocurrency. The simplest answer is – a large number is chosen, and the creator says "ta-da; I've made some money." They record it as the first transaction making them the owner of a very large integer on a computer network. Many readers may be saying that's wrong – mining creates the money, but that is putting the cart before the horse. The miners must want the money first – mining may be additive to what is known as the "coinbase" (the total supply) of the cryptocurrency, but the notion of the value of the coin precedes the establishment of the mining process. A miner must believe a coin is worth something before they decide to spend the capital to compete to get more. And in the case of Bitcoin, the network algorithm reduces the mining fees from the creation of new coins to zero (the "halvenings") so that the miners ultimately have to charge fees to mine a transaction from those that want a transaction to be included, making bitcoin "deflationary" over time as coins are lost, and proving that the value system is completely self-referential with no external inputs. The money is created because a network of people says it is, and then they behave like it is. That's the beginning and the end of crypto coin creation. That's it – you can do it yourself on your own computer and call yourself a gazillionaire. Now as a gazillionaire, you need to go out and transfer it to someone who wants it. Bitcoin started with the "genesis block" which is the first transaction and the total "coinbase" at the start which was owned by Satoshi Nakamoto, Bitcoin's inventor and first gazillionaire.

MONEY TRANSFER

It is obvious (but often forgotten) that an exchange of cryptocurrency requires that both parties have computers that are peers. Peering creates a large set of preconditions which means that both run software that adhere to the same rules, they need to be able to pass messages to each other over a network, and both need to agree that the cryptocurrency in use has a value suitable to for the purposes of a real-world value exchange for property or services. Enter the second problem – how to transfer cryptocurrency and its solution – some tools borrowed from cryptography.

Cryptography is the art and science of keeping and passing secrets and knowing the identity of participants. At its core it is about sending messages so that only those who should read it, read it, and that those who send it and receive it can trust that they are who they say they are – all the while ensuring that no one else can know who they are or see what they should not be able to see. It sounds arcane and it is arcane, and it also requires a lot of "faith" in tools and processes; in real life secret keeping situations, field craft is as important as the tools taken into the field. Cryptocurrencies only use a small subset of the tools of cryptography – a cryptographic hash function and a digital signature algorithm. There is no encryption in cryptocurrencies, and even the power of the blockchain comes from infeasibility, not encryption. But we will come to that later; let's first look at how signatures are used to implement a payment mechanism.

While all this gets complicated in the detail, the process of digital signatures is the same as paper-based signatures - your handwritten signature is assumed to be unique because only you can write it. But for someone to know it is signed by you, they need a public copy of it to make a comparison to verify it is from you. For example, the bank keeps an image of your signature and then when you do your magic with a pen and sign something, the image can be used by a clerk to verify it. The public image can be passed around, and it is often made very public for many – the treasury secretary's personal signature is on American banknotes. Digital signatures are the same process; your secret key is a number held in secret so that no one else can use it, and your public key is a mathematically derived public copy that can be used for verification. You use your secret key to sign digital data, and someone else can use your public key to verify your signature.

And so, cryptocurrencies use digital signatures to move a holding from one account to another. With cryptocurrency holdings, the public key is used to create an account ID (or wallet) on the blockchain. If an account (wallet) is owned by me, all transactions correctly signed by me can be relied upon to have been done by me, because only I have the secret key that generated the public key used as the account ID (wallet), and only I can create the signatures of the account. The public key is made available for verification of the transaction as part of the transaction data, and so the transaction can be verified by the data, the public key, and the signature that is included on the blockchain. This is how new accounts in cryptocurrencies are created – by new actors turning up with randomly generated account numbers (aka. wallet addresses created from public keys generated from secret private keys), and people transferring value to it from their account by signing values over to the new address, thus making a new account on the blockchain. So, if someone turns up to me with a valid address (public key), and I transfer some of my cryptocurrency value to their account on a blockchain, then we have a new account with a balance, and I now have whatever I had minus whatever I transferred to them. Satoshi Nakamoto had to get busy finding people who wanted him to transfer them his Bitcoin balance.

DOUBLE SPENDING

The transfer of digital money has the problem of "double spending," which is simply the problem where if I send a message to you saying here's five digital dollars, what's to stop me sending the same message to someone else? How do we know I have a debit and you have a credit, and what stops me from doing it again and again with someone else? The answer is, you need a register somewhere that everyone agrees is the penultimate register of who has what based on what has been passed to whom, and who signed it.

Digital signatures used in financial messaging technologies have been around for as long as electronic banking networks. This is how SWIFT and interbank transfers work – each regulated bank has keys, they send signed transfer messages to each other, and the receivers and the network can verify the data, and all is well. But the difference here is that these are regulated institutions that must make sure the numbers reconcile via the clearing house accounts that keep the penultimate register so that no one keeps what they sent away to spend it again. They do all this as trusted parties working through a trusted independent third party. It's the time-honored system of an organization of bankers controlled by regulators that enable the control of nation state banking systems. It was the only known way until the invention of the blockchain, which solved the problem of central control so that a rag tag group of untrustworthy network participants could come together and create a penultimate register that was distributed, not centralized, and access to it and the identities of those using it were not controlled.

The blockchain is simply a public register that a network of peer-to-peer computer participants agree is the valid set of all messages sent between public keys since the beginning of time; the epoch known as the blockchain genesis, which contains the original coinbase. This is the "consensus" that is talked about – all peers agree that we all have the same messages and hence all peers can calculate the same holding balances to see if they can trust that they are going to get the cryptocurrency being sent in a message from another peer. The ordering of messages is managed by linking transactions from one to the next using a cryptographic staple (a hash value made off all prior and present data organized into an eponymous "Merkel Tree" created by Ralph Merkel) so the peers can verify order and content. Inclusion on the register is achieved by peers competing to win a competition to solve a hard problem to create an approved "block" of transactions. Winning the competition lets you charge fees, and the network may also award you an agreed number of new coins, hence slowly growing the coinbase. This competition, known as "proof of work," was borrowed from an idea designed to stop email spam where it was proposed that if an email did not have a value on it that showed that meaningful computer work was expended to create the value, mail servers could choose not to accept it. The assumption was that spammers couldn't do the work to create the value on a broadcast of emails to massive distribution lists, while to an individual the time delay would be of no real consequence.

Much is made of this competition – now known as mining. In simple terms, the mining algorithm is a race to find a value in a space that has a tuning factor that makes the search space larger or smaller (measured in clock time to complete) based on the number of participants trying to win the competition. Once it's been won, after a few more blocks it becomes impossible to redo the prior searches and re-write the chain. So, for as long as a single participant does not have more than half computational the power of the network, no one can re-write what the last transaction was because the algorithm makes it so hard that you're too busy trying to win the next one rather than rewrite the old ones (if they do, they are able to perform what's called a 51% attack). And because the blocks are cryptographically stapled to each other, going back block by block accumulates the amount of power required to go back through time and so re-writing history becomes infeasible, like calculating a secret key from a public key. The genius of the mining process is that it also allows the network to protect itself from "spam" transactions; the miners will only win if the transactions are canonical according to the peer-to-peer network rules, and so they just throw the bad ones away.

To summarize at this point, we have shown how cryptocurrencies are created – you just make a big number when you start a blockchain. You then go and find others so you can sign messages to pass that money to them, and then they do the same, and so on and so forth. And then the network of computers everyone uses for the task keeps a record of all the messages using the blockchain registry process so that everyone knows who has what. No one needs to be asked permission to join, and only those transacting with each other know who's on the other side of that specific transaction; the rest are all anonymous. That's it in a nutshell.

THE BOOT PROCESS

Now we see a Rube Goldberg machine created by Satoshi Nakamoto that requires some very sophisticated software created by clearly genius (but perhaps unbalanced) hackers, we see a network of connected computers, and we see a group of people (affectionately known as nerds) skilled in the field craft of creating cryptographic keys and performing arcane commands to create and send transaction messages about a pot of value created out of nowhere. How did this thing ever become anything more than entertainment for a bunch of nerds even more nerdy than gamers trying to save Azeroth in the World of Warcraft? How did this network boot itself? The answer is that it was booted with libertarian tech nerds, adoption exploded with drug nerds, and now it is being colonized by financial nerds.

The libertarian tech nerd phase was the World of Warcraft phase – a bunch of libertarian nerds from the cypherpunk and related communities combining with interested programmers to have some fun with a new tech toy. It was (and still is) nerd entertainment like trying to save Azeroth. Who knows what motivates people to do things? But in the world of open-source software there are many people playing with enterprise ideas that never end up being used by an enterprise.

And then one day the idea that Bitcoin could work as money certainly got some enterprising drug nerds interested. Crypto didn't just help dark markets – crypto created dark markets. There are plenty of books written on the history of dark markets, but the most interesting marker to me is that the month that the Silk Road online market opened and accepted Bitcoin, the Bitcoin to USD exchange rate reached parity at 1 USD for 1 BTC. Basically, Bitcoin became the USD proxy for dark market transactions, and off it went. Money is what money does – and in dark markets Bitcoin became money. Satoshi Nakamoto had inadvertently kicked off a revolution in the drug and related markets.

Which now brings me to the colonization by the financial nerds. This is a provocative statement to make in the crypto chat rooms, but beyond its history and preeminence as the first instance of a massive innovation in computer science, I find Bitcoin the least interesting of the cryptocurrencies. It is the Model T of cryptocurrencies; you can have any Bitcoin you like, but it can only do one thing – be a medium of exchange – and a very resource hungry medium at that. Blockchains can be used for so much more than just value exchange.

First, a quick diversion back into the blockchain process description. Notice that I always say that the blockchain is used to store messages. That's because what is stored on the Bitcoin blockchain is little messages written in a very simple computer scripting language (it is a reverse polish notation, stack-based language like Forth, which means nothing to most people. Think of an HP12C financial calculator if you are as old as me). What is stored on the Bitcoin blockchain is these little signed fragments of code that each peer reads and then evaluates to perform transactions against a ledger or database held on the peer. The transaction is implied by the message's code and is applied at the peer node so that history can be rebuilt and verified. The size of the transaction block and the number of instructions that could be included in this scripting language were just programmer decisions made by Satoshi Nakamoto, but the programmers that got control of the Bitcoin code base became the High Priests of Maximalism (people who say bitcoin is the perfect first and last word in cryptocurrencies and superior to any other cryptocurrencies) who said thou shalt not compute on our blockchain, thou shalt only transfer value the way our lord Satoshi Nakamoto created it. So Vitalik Buterin, a now proven genius (with the pussy cat handbag to prove that all geniuses look crazy before they prove their genius) said, "Okay, I'll make a new one," and Ethereum and "smart contracts" were born.

Unfortunately (according to me), Vitalik was also infected with the metaphor mangling mind-bug common in basement living technologists, and he adopted the imprecise term "smart contracts" for what is precisely a procedure call written in a scripting language that had all the instructions in it to do whatever you want (it is also a reverse polish notation, stack based virtual machine language like the java virtual machine but the difference is it has a scripting language similar to JavaScript, which is known to almost everyone working on the web). And so "smart contracts," or the programmable blockchain is born. So Ethereum was created as a blockchain that uses ETH as the charging mechanism (which is Bitcoin-like as a fungible cryptocurrency) for sending "Turing Complete" programs (i.e., with the full set of instructions required to be a complete computer language) to the network in one type of message and allows the programs to be called in another type of message. In simple terms, the sum of these messages means you can build a database with programs on top of them to do things like – create new tokens and implement algorithms to control and use them.

The invention of the programmable blockchain has created two paths – the public blockchain path such as when assets are created and managed on public blockchains like Ethereum, and "permissioned" blockchains where logic is implemented by stock exchanges, corporate controlled coins such as Facebook's Libra proposal, and blockchains that implement "fiat" coins controlled by national governments such as the Chinese Digital Yuan. Permissioned blockchains are anathema to those interested in decentralized crypto currencies – and I include myself in that group. And so, I now return to Ethereum where all the interesting action has occurred and the colonization of it by the financial nerds.

Because Ethereum is programmable, you can make any token you like however you like, and many people did so in the initial rush. However, the next innovation was a standardization of how tokens were created on the Ethereum blockchain. The loose collaboration around "Ethereum Request for Comments" (ERC) in the Ethereum community gave rise to common patterns such as ERC20, which is a common interface for "fungible" token smart contracts (*i.e*., a token that is a coin), and ERC721 which is a common interface for "non fungible" token smart contracts (*i.e*., a token that references a data file of media or some other unique data item). By standardizing these interfaces, other contracts such as those that perform exchange functions, provide liquidity pools, or even enable gearing, emerged to use them. And so, we now have ended up with a complex layered architecture of blockchains and coins for creating and calling smart contracts, smart contracts that implement tokens, and then smart contracts that use the token smart contracts. Some common examples are:

- ETH/BTC - blockchain native coins
- DAI - an ERC20 fungible token designed as a "stable coin" with a USD price peg algorithm.
- USDC – an ERC20 fungible token backed by real USD in a regulated trust managed by Circle.
- 0x – an exchange smart contract.
- UniSwap – an exchange smart contract that provides automated liquidity pools for tokens.
- Zora – an ERC721 non fungible token for digital media trading.

There is also a Cambrian explosion of smart contracts for creating experimental derivative algorithms and program trading models, all of which means that it is a very fertile ecosystem for the financial nerds. And so today there is a lot of venture capital chasing experimental business models using programmable blockchains, and Ethereum is still the blockchain of choice for this purpose.

THE PROGRAM OF PROGRAMS

Of course, I know you've worked out by now that everything in old financial markets is seen as being fair game for a smart contract experiment, and so what about the corporation? Well, what is an initial public offering of a public corporation other than the division of a corporate entity that owns assets into units that are sold to the market with certain rights, including voting rights. And so, it didn't take long for the nerds to work out that a form of incorporation could be created as a smart contract program, where token holders in that smart contract could have voting rights based on the size of their holdings. This is what is now known as a Distributed Autonomous Organization – or a DAO. In simple terms, popular smart contracts with high utility and use such as UniSwap are known as "protocols," and so the creators of them who have the right to change them (because they hold the keys that made them) are holding something of value. So why not "IPO" that value and get a pay day? So, a DAO is a form of smart contract that has units that represent ownership and voting rights, and the DAO smart contract is programmed to allow changes to the protocol program. Et voila – you have created a blockchain based form of corporate entity that can be sold to the market based on the value of the "protocol" smart contract that the DAO controls. An ICO (initial coin offering) of the tokens in the DAO can be made in return for other tokens of value such as ETH and DAI. Congratulations financial nerds, you have replicated the real world into the blockchain world, and we can all get on with the time-honored business of hustling to make things and sell things and taking on and selling away risk. They call it "DeFi" (Decentralized Finance), which is an emerging topic that is beyond the scope of this paper.

EXCHANGES

I have left Crypto Exchanges until last because they are an add on to the ecosystem, not a core concept. The whole cryptocurrency edifice was designed and can operate as a somewhat solipsistic thought bubble; it is a self-referential thought experiment of value created by programs that manage value created by programs. Indeed, the original design of Bitcoin was to destroy and replace nation state currencies by being an alternate medium of exchange between people for goods and services - it was never meant to be an asset with a relative value INSIDE the system of government, or “fiat” money. But if people are not getting paid in cryptocurrency, how else can you get it to buy your Scooby Snacks in the dark markets if you can’t buy Bitcoin with cash? And even ornery libertarians can be tempted by a Lamborghini or a big house, and why stay on the crooked ladder if you can cash out and send your kids to school to climb the straight one? And so, if cryptocurrencies are to be of real utility in the real world, they have to be able to be exchanged for “fiat” currencies where the non-nerd wants Benjamin’s not Bitcoins.

The original exchanges were person to person – bitcoin holders would meet at informal meetups colloquially known as “Satoshi Squares” to buy and sell from each other, or just organize to meet in person. My first attempt at buying Bitcoin in 2013 talked me out of wanting to buy Bitcoin; it was too far to drive to a place I didn’t want to visit. But then slowly but surely online exchange services were created where you could transfer cash and get deposits made to your wallet (Bitcoin address). The early exchanges were, let’s kindly say, a mixed experience. The problem with exchanges is threefold – first you must trust that when you send your cash away the purchased Bitcoin will come back. Second, if you hold a balance of Bitcoin at your chosen exchange, you must trust that they are holding the cryptocurrency asset against your liability. And third, you must trust that they are good operators and not going to disappear through incompetence or malice. Every one of these risks were realized of course – MtGox famously had all its crypto stolen and so the accounts became worthless. One of my favorites is QuadrigaCX, which was a Canadian exchange where the operator died on a trip to India and because he ran the whole exchange from his laptop and personally managed the keys, the crypto was lost and every client’s balance with it (or did he die? That’s what Reddit is for). There have been various other stories such as exchanges being fronts for money laundering, and more recently, being taken offline by take down orders from governments for being facilitators of money laundering and crime. Some just stole their client’s Bitcoin.

The exchange that has made the category is Coinbase. Coinbase is a Silicon Valley VC funded crypto exchange that from the start wanted to be a good exchange and technology business, and they focused on the rules and the regulations as a core part of the business model. As well as paying huge dividends to its founders, I think the whole community got the dividend because the creation of a trustworthy exchange allowed trust to be established in the whole system in the largest market in the world – the USA. It also got cryptocurrencies a seat at the table inside established organizations by establishing itself as a reliable organization, and it could play an advocacy role. And so, with the emergence of well-behaved exchanges came the ability to buy and sell cryptocurrencies inside the “normal” financial system, and valuations could be formed and trusted.

INTEGRATED CRYPTO

I have explained the history and mechanics of cryptocurrencies, and I can now talk about how the cryptocurrency ecosystem we have today is not the cryptocurrency ecosystem envisioned by the original creators. But it’s still talked about in those terms – cf. Messrs. Buffett and Monger. Let’s put the old trope that it’s “inherently evil” to rest.

Governments and corporations never want technology innovations that disrupt the order (aka control and profit) of things. Music downloads were illegal until Steve Jobs convinced record labels with the iPhone that it was better to make music available online for a price than fight the inevitability of new technology. The reason why it was illegal to download music was because it was illegal to copy a work; no one envisaged a new peer to peer distribution mechanism that would turbo charge the illegal but tolerated use of a cassette copy of a vinyl record. So yes, all music downloads were illegal until the Jobs deal, because no one was allowed to hold a copy of a work. But now they do, and all is well.

The idea that crypto is “evil” is firstly, the same as saying cash is “evil” because it works for drug deals (and many in government are interested in state based digital currencies to remove cash citing that as a reason), and its usage in that realm does not mean that the technology is not valuable in other realms. For example, there is no real use for smart contracts in drug markets. Likewise, the weed that was purchased using Bitcoin five years ago is now legal in many states. In other words, technology innovations may start out illegal or be used illegally, but as they integrate into real world use the illegal gets dealt with like it always has, and the new technology gets adopted like it always has. To me, the name calling and harking back to the way it was started in the past can be left behind, like the young leave behind the attitudes of the old as the world changes in front of them. Buffett and Munger are free to listen to their digital music, get change in cash for their lunchtime burgers after a drug dealer paid cash for the previous one, and disparage Bitcoin on their zoom calls to investors. Meanwhile, technology adoption marches on.

But the transition from the "evil" and uncontrolled usage of cryptocurrency, which did make it money, means that cryptocurrencies are increasingly integrated into control structures and so the original purpose of it, which was to be free from nation state control, means that the cryptocurrencies that investors buy is "cleaned" from its original purpose. In a twist of irony, what this means to a cypherpunk is that it is corrupted by the system, but what it means to us is that it is cleaned by the systems that control them.

And so, investors now buy clean cryptocurrencies which I define as cryptocurrencies that are integrated into control systems and cannot serve any purpose in corrupt activities. So, let's explore why they are getting clean and what it means.

OOPS - CRYPTOCURRENCIES DON'T WORK

One of the key reasons why cryptocurrencies are becoming clean over time is because popular cryptocurrencies don't deliver the promise on the label; they don't keep you anonymous. Let's go back to the blockchain – that perfect and irrefutable record of transactions. The whole reason why gangsters kept two books was because they didn't want anyone seeing the real transactions, and now blockchains put them on every computer in the world. The blockchain provides a time stamped record of who did what from the year dot. Ah, you say, but no one knows who did what because the wallet addresses are anonymous. They're not; they are pseudonymous – which means that they are a pseudonym for the person doing the transaction and if you find out who they are, the whole chain of transactions gets revealed. This problem was known early in the dark market days – someone who was "turned" gave their addresses to law enforcement and then law enforcement had the first link in the chain – a known felon - and then they could build the graph to the next one and so on. This idea was so well known that a metric known as "coin taint" was developed which gave a Bitcoin address and the coins it controlled a score of the likelihood of disclosure. Companies are known to have created systems that law enforcement can use to track and trace Bitcoin blockchain transactions this way, and so the noose is slowly tightening over the whole system. It still works, but increasingly less so.

Of course, technology also iterates with new information, and cryptocurrency developers and dark markets haven't been sitting on their hands. The traceability of transactions on blockchains is a known problem and new methods have been developed to solve the problem. Dash and Monero are two cryptocurrencies that use different blockchain organization techniques so that you cannot link the data going into a block with what comes out. The peers that perform the transactions jumble them before they write them, so you don't know which output came from what input. A new signature approach charmingly called zk-SNARKs - Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (a name which also proves that nerds are still clever but also still nerds) has been developed and implemented in ZCash which allows for better anonymity. And so, the new dark markets have moved on from Bitcoin to use better technology. But here's the rub – the reason why you probably haven't heard of these clever coins is because they are largely not allowed on exchanges as first and foremost, the regulators know they work and are "watching," which discourages the thought of linking them to "fiat" exchange, and secondly, the customers that use them make a pain in the behind for the exchanges and so it's bad for business.

Services were also developed called "tumblers," where you could basically wash your crypto of taint by putting them through a service that took coins in and paid them out so that the link was broken. These services were available but are no longer as there is nothing like the threat of jail for being an enabler to make you stop doing what you are doing even if technically it can be done. There's a big difference between being in the business of dealing in clean crypto and laundering dirty crypto!

EXCHANGES ARE AGENTS OF THE GOVERNMENT

Here's a tip – crypto exchanges are participants in the bank transfer systems of the countries they are in, and they now must follow counter terrorism financing and anti-money laundering laws (CTF/AML), which means that they need to perform "Know Your Client" (KYC) compliance checks, and report transactions to financial tracking and tax authorities. This also means that investors that buy and hold cryptocurrencies are "standing there naked" inside the regulatory system just like any other banking service. The exchanges, as licensed operators, are also dependent on making sure you are either compliant or not a customer. All this information automatically goes into blockchain tracking systems, and if you have a cryptocurrency account at an exchange, you have entered the de-anonymized blockchain and all your blockchain transactions pre and post are now traceable, forever. The system becomes cleaner by the day, and that's the system you are in. If you want the "fiat" from your cryptocurrency investments, you have to live by the rules of the systems of government that give "fiat" it's value. You can't have your cake and eat it tax and oversight free, too.

The cryptocurrency exchange process also raises an interesting point often overlooked by investors – most cryptocurrency transactions don't occur "on chain." That is, they never occur on the blockchain; they are done inside the exchange system and never see the light of day. This creates two interesting points for investors. The first point is that transaction metrics gleaned from the analysis of blockchain data is largely irrelevant as the lion's share of trading is done against the crypto exchange's house account. Blockchain transactions are increasingly like the street side account of broker dealers on Wall St – they are wholesale transactions only seen by insiders. The transaction data is internal data that belongs to the exchange, and it is also reported to regulators. So, while there are no market rules in cryptocurrency land to stop you crossing your own trade and pumping on one side and dumping on the other, I don't consider it to be a long-term strategy as the monitoring of internal trade activities in exchanges increases. And the second point is that the price you see is not an international price such as what you see in real currencies traded through participant global trading banks. The price is the price inside the exchange, and the exchanges arbitrage (and profit) with the other global exchanges. So, the price of bitcoin in the USA is not the same as the price of Bitcoin in China, in USD terms. Cryptocurrency prices are local within countries and even within exchanges. Most exchanges make their trading data available via web service APIs, but nevertheless this data does not appear on the blockchain.

Not only are exchanges a way to control what happens within markets, exchanges allow control over what gets into markets. We have talked about how the popular crypto currencies don't work perfectly and how the new ones designed to be anonymous are not "allowed" into exchanges, and this same process also allows securities law to be applied effectively to control the way "smart contract" tokens are adopted. Recall that smart contracts allow anyone to make a token that represents anything. The SEC in the USA, and regulators in other jurisdictions have all made rulings about when token issuance falls under securities law. The founders of Ripple are inside a fraught legal process for the very reason that their issuance and control of the XRP token has been deemed by the SEC to be the sale of unregistered securities. Furthermore, regulators also make rulings about how cryptocurrencies and tokens are held inside securities, such as exchange traded funds (ETFs). At the time of writing this paper, the status of ETFs holding cryptocurrencies is still to be determined with the SEC in the USA still not approving Bitcoin ETFs. The combination of regulators controlling what is in ordinary exchanges (e.g., ETFs on the NASDAQ) and crypto exchanges coordinating with regulators about what should be included on the new crypto exchanges, all means that the crypto exchange mechanism is a tool for regulators to increase oversight and control which all adds up to the further cleaning of cryptocurrencies as an asset, and cryptocurrency trading as a process.

GLOBAL COORDINATION

Cryptocurrencies may be young, but they have got to the top of the list of topics in global financial discussions and the desire to control them. The global Financial Action Task Force (FATF), the global money laundering and terrorist financing taskforce has recently put out a guidance paper for member states (read instructions) on Virtual Asset Service Providers (cryptocurrency exchanges) in order to create a global standard to manage the regulation of cryptocurrency assets. This has the effect of legitimizing the asset class while also cleaning it up. But the geopolitics of cryptocurrencies is not just about ATF/AML; it is also about where it can be used, where it is banned, and who controls networks. All of this creates risk and uncertainty for investors in the asset class in the near term, while also creating certainty over time about what is approved and what is not.

CRYPTO CLEANED AWAY

I have made the case that cryptocurrencies are being adopted as a new asset class and regulators are responding to ensure that they fit inside old control processes. The cryptocurrencies available to investors are becoming "clean" and hence are available to be viewed as a legitimate investment, should an investor wish to take that risk given their mandates. At this point it's also important to note that investment decision makers (who are agent, not principal) should be careful to ensure that investing in cryptocurrencies is within their mandate, as regulators are also forming views as to whether some classes of investors, such as pension funds and in Hong Kong, individuals, should not hold the class and expose their beneficiaries to cryptocurrency risk at this time. But if it is okay to invest in the cryptocurrency class, I believe the class is a legitimate and clean asset that is there today to fit into an investment portfolio. But the question remains, what is the risk that cryptocurrencies get totally cleaned away? That is a risk with a probability far greater than zero.

Let's start with the technology risk. In my view, the market is a bit ahead of itself in its faith in the robustness of the crypto ecosystem. The Bitcoin developers and the Ethereum developers present as a robust community, but the actual group of "core" developers is quite small, and they are, let's kindly say, eccentric. No one controls these people, and their power is quite profound. Not because they are necessarily the best but because they control the write access to the official repositories from which everyone trusts to build and run their software. They have incredible power over the ecosystem. The risk of this power has been shown in both Bitcoin and Ethereum. I have already discussed how many Bitcoin developers are known as "maximalists" with a very narrow view of what Bitcoin can be and how it should work, and they fall on the side of ultra-conservatism and are largely immune to change. A classic example of how they use their power is that they refused to change the block size parameter of the bitcoin software, which meant that the number of transactions able to be processed at any one time in Bitcoin is fixed, and hence so is the scale at which it could operate. Rather than considering a pragmatic change, the developers nearly self-immolated with red hot righteousness from their view of the risk of changing the parameter, and so they went off on a very nerdy frolic around complex ideas like "segregated witness" (segwit) and creating "lightning networks" to move scale off the main blockchain. If you haven't heard of it, then you don't know the Bitcoin community. And because most people haven't heard of it, it proves most people don't understand the Bitcoin community. And that is a lot of risk for something that is appearing inside retirement funds.

The Ethereum network demonstrated the opposite dynamic. The first DAO created on Ethereum, and just called "The DAO," was a smart contract created by a company called slock.it that was trying to create smart locks on assets to enable an Airbnb style smart contract. The Ethereum foundation was behind this "revolution" as a demonstration of the amazing use case of the Ethereum system, and I remember sitting in a conference in Hong Kong where Vitalik himself was ebullient over the sunlit uplands of "The DAO" and all it meant for humanity to organize on the blockchain without the need for any legal frameworks other than rules in code. The problem was that it was a smart contract that ended up looking pretty dumb when some hackers worked out how to drain funds out of it. And so, the Ethereum developers changed the core software and rolled back time (called a "hard fork" of the Ethereum blockchain) so that the bug was removed. Once again, that is a lot of faith (also known as a lot of risk) invested by investors in the custodians of the network's software when they can rewrite history. And notwithstanding the crypto holdings of the founders, these open-source developers tend to work for free or inside small foundations, and that is a longevity and reliability risk. Then there is the geopolitical risk of the mining ecosystem. China was preeminent in the Bitcoin mining ecosystem because basically, they played unfair. I know this from firsthand discussions - European and American Bitcoin enthusiasts designed specialized hardware to mine Bitcoin faster, and they had them manufactured in China. The first batch off the production line would be installed in China, and by the time the second batch went to the customer, they were already behind the power curve and could not catch up. That, plus enterprising Chinese miners absorbing cheap power from Chinese anomalies like white elephant infrastructure projects and local handshake deals, meant that the Chinese emerged as the preeminent miners of Bitcoin.

The Ethereum developers were aware of this problem and so they created a mining algorithm that was "memory hard" and hence could not be easily accelerated with fast custom technology. Ethereum is mined best with graphics processing units (GPUs) such as those designed by AMD. This created a massive rush on GPUs and the specialized hardware to glue a whole lot of graphics cards into a single PC. My initial cryptocurrency work was in developing "mining rigs" that did this, but of course they are very hot and very power hungry. As the network grew rapidly and the number of units required to mine grew with the number of participants, Iceland ended up with the advantage because it's cold and its thermo power is cheap. So now Iceland uses more power for Ethereum mining than it does for anything else2, and nowhere else has air conditioning as good as theirs (they just open the door to let in frozen air to control the cooling of the red-hot GPUs). Without large monotonic increases in crypto prices, it is hard to compete with them on the cost curve.

Bitcoin and Ethereum are already at the mercy of how a few countries think about cryptocurrencies. The Chinese government has already largely banned cryptocurrency exchanges, and mining and exchange operators have control orders on them so that they can't even leave their city without government permission, and they have started to force the shutdown of mining enterprises. All of this creates instability in the ecosystem, but the system is resilient, and change creates opportunities for others. If mining moved back to the west, it may increase the attractiveness of Bitcoin and Ethereum as it becomes more distributed, and the risk of Chinese government meddling becomes less of an issue.

As crypto finds its way into funds, it will conflict with ESG and other environmental and social issues due to the proof of work mining algorithm. Ethereum is working on change with experiments in a new mining approach called "proof of stake" that does not require burning hot energy demanding calculations but instead puts miners' crypto stakes at risk if you don't mine correctly. Bitcoin is so ossified as a developer group, and can't do what Ethereum does out of principle, and so in my view it will struggle to change its mining algorithm and could increasingly be seen as an undesirable environmental pariah by users and governments alike.

And of course, governments are aware of the benefits of programmable money and are looking at the idea of "fiat" crypto (cryptocurrencies issued and controlled by central banks), which also goes by the acronym CBDC (central bank digital currencies). China has a live experiment with the Digital Yuan, and all other central banks including the EU and World Bank, have made various statements about the future potential of CBCDs. If CBCDs are realized, the central banks are 1) not going to want competition from unregulated cryptocurrencies, and 2) will be providing a legitimate alternative and be able to declare by fiat that the unregulated ones are inferior, unnecessary, and an environmental risk. Cryptocurrency advocates will say "let them try and the networks will just keep going," but I am not so sure about that. Look at illegal music downloads – they aren't worth the bother now there are easy legal alternatives. And once there is a legal and approved alternative, the Apple and Google app stores can simply remove the unapproved wallet apps people use, and because everything is in the "cloud," which really means it's in the data center of a very small number of large and compliant companies, they can just say you can't run cryptocurrency nodes just like they frown upon illegal download sites. Yes, the network can keep going at the fringe, but the fringe is not a good place to hold huge sums of investment value. And finally, if the government just said no, with all the lost coins and dormant crypto accounts, the actual real dollar value of floating crypto "capitalization" can be absorbed as a (albeit big) bankruptcy.

And finally, there is the plain old risk that the algorithms fail or are superseded by quantum computing, or a better mousetrap is invented. I am a cryptocurrency fan; I love the freedom experiment and the disruption of cryptocurrencies inside the progress of our money systems; but I also have my eyes open. All current cryptocurrencies could just be cleaned away.

CONCLUSION

I have left the burning question, "What is the value of a cryptocurrency?" for the conclusion. The reason is that no one knows from moment to moment, and the answer is it is worth whatever you get for it from the next person who buys it from you. It's on you to believe that what you get in return for the exchange is worth something too. What is the value of a randomly chosen large number created on a ledger? It can be worth zero if I do it on my computer, but it's become a medium of exchange for real assets from the history of what has happened to the number stored on Satoshi Nakamoto's computer. The value of all things is held between the ears of people. Even gold is worthless if there is no living human to value it in an exchange, and no one around is able to fashion it into jewelry and then exchange it for something to pay the bills with someone else who wants to wear it. Value is a very human and relative concept, and the concept of the intrinsic value of anything becomes fraught the more you look at it. With cryptocurrencies, it becomes deranging. The way humans value things is through the market, so clever tricks of sophistry explaining intrinsic value, and the opposite act of saying it is valueless out of hand, are all interesting conversations around the edge of the market, but the fundamental analysis of its value is made in the market, and the risk of the asset is relative to the other assets in the market.

I have mined, bought, sold, and transferred cryptocurrencies since 2015, and I have programmed and studied the Ethereum blockchain since it was first released. I have many friends with crypto, and I know others that create tools and protocols. It is definitely valuable, but after all this experience, I don't know what it's worth. To me, it always was and still is to this day, an experiment. To many, it is an experiment in personal freedom and that will continue while the "old" cryptocurrencies continue their value experiment on regulated exchanges. What the old and stable cryptocurrencies represent inside old and stable exchange mechanisms to old and stable investment processes, is yet to be determined. The best analysis and thinking of how to do this has been done by Dan diBartolomeo at Northfield.3 But when people ask me to put it into context, I use a comparison.

Cryptocurrencies are technology, and technology has step changes in both directions, and battery technology is my best equivalent. Lithium companies are now hot stocks because Lithium batteries became a new way of storing power that was better than nickel cadmium. Lithium mines create a horrendous environmental footprint, but people look past that to see the benefits of the technology. Maybe Lithium is the last word in power storage, but the history of technology innovation suggests it's not. Maybe the dominant manufacturers of Lithium batteries will last forever, but probably not. And maybe the control of Lithium will become so important that governments will want to control its use and its mining. Or perhaps not. Ask two Lithium experts for their narrative, and you will get three versions of the future, or maybe four. They may all be right, but usually not.

This human invention was weird from the start. Or maybe not.

ENDNOTES

[1] Nakamoto, S., 2008, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf.

[2] Fairley, Peter, "Ethereum Plans to Cut Its Absurd Energy Consumption by 99 Percent," IEEE Spectrum, 2019, https://spectrum.ieee.org/ethere um-plans-to-cut-its-absurd-energy-consumption-by-99-percent.

[3] diBartolomeo, Dan, "Risk Estimation of Cryptocurrencies, Northfield, April 2021,
https://www.northinfo.com/docs/cryptocurrencies.pdf.