What Are Cryptocurrencies?

Rasheed Sabar
Contact: Sabar@ellington.com
For Research Updates, Subscribe Here

Ellington Management Group, September 2017

1 Introduction

By now we've all heard of cryptocurrencies. But relatively few people own them, and even fewer people understand them. What exactly are cryptocurrencies?

In this paper, we aim to **explain cryptocurrencies clearly while keeping jargon to a minimum**. Cryptocurrencies are tough to grasp because they are novel on many levels: they are novel computer science and social engineering *technologies*, novel tradeable *instruments*, and novel monetary and political *phenomena*.

Having understood the essentials, we form a view on the merits of cryptocurrencies as an asset class. There is enormous disagreement on this point. Many people, especially in technology circles, believe that cryptocurrencies will prove to be as important as the internet itself. Others, especially in value investing circles, believe that they are an elaborate pyramid scheme.

Which view is correct? This paper will help the reader appreciate both sides and form an opinion. We start by considering the nature of money. Then, we show how Bitcoin works under the hood. We then survey the landscape of digital assets outside of Bitcoin. Finally, we weigh arguments for and against its investment merits.

2 What is Money?

Isn't it obvious? Money is what we use to buy things. Yet perhaps this perspective misses something essential. As the old proverb says, "If you want to know what water is, don't ask a fish." Money permeates our lives so wholly, it is difficult to grasp its **nature** above and beyond its everyday **use**. To understand money's roots, we consider theories of its origin.

One commonly held theory was developed by Adam Smith (and originally Aristotle): money originated to make barter more efficient.[1] Imagine a society before money. Imagine further that goods in this society are exchanged through barter. The baker has extra bread and wants meat. Hoping to trade bread for meat, he goes to the butcher. But what if the butcher doesn't want bread? Then there is no exchange, lacking a "coincidence of wants". In this setting, money originates to **scale up exchange**.

A different theory holds that society before money was based not on barter, but rather on gifts and debts.[2] Anthropologists have studied communities where people share items with others in need and expect reciprocation at some point in the future. Here there aren't strict one-for-one exchanges but rather a set of social norms: not "trading" so much as "sharing." As the size of tribes/communities grows, sharing becomes complicated to track and manage; it needs to be tallied to prevent people from being exploited. These quantified obligations are debt and, in this setting, money originates to **scale up social obligations**.

[1] See Adam Smith, *Wealth of Nations*, Chapter 4
[2] See David Graeber, *Debt: The First 5000 Years*, Chapter 3

Another theory holds that money, at its core, is a creature of the state.[3] Governments have the power to levy taxes. If only X is accepted as payment for taxes (it doesn't matter if X is gold, dollars, or seashells), then there will be demand for X by citizens; they will accept X as payments for goods and services, and they know that others will accept it as well. The ability to levy taxes gives government levers to direct economic activity (through choice of what to tax) and to expand its own scope (by acquiring new taxpayers through war, financed by taxes or newly created X). In this setting, money originates as a way for **states to scale up their power**.

So which theory is correct? We need not pick only one. Each perspective opens us to a different and important dimension of money. Indeed, the textbook definition of money as (a) a medium of exchange, (b) unit of account, and (c) store of value is a good list of **features** of money. But by considering narratives of money's origin, we can see that it is not only about exchange, but also about social obligations, trust, and power. Reflecting this intuition, Bitcoin as a money system emerged at a moment in time when trust in financial authorities was shaken, in 2008.

3 How Bitcoin Works

Satoshi Nakomoto[4] introduced Bitcoin to the world in a paper released on October 31, 2008. He tucked a message into the first Bitcoin transaction, on January 3, 2009: "Chancellor on Brink of Second Bailout for Banks". The note alludes to a UK Times headline from that morning and captures the climate of disillusionment with the financial system. Bitcoin[5] circumvents the financial system's plumbing; it is a system for exchanging digital "money" without the need for banks.

The system's rules are written in software that is open-source and owned by no one. A group of core developers maintains this software—some are volunteers and others are supported by donations. Any change to Bitcoin's software follows a democratic governance process described in Section 4.

In this section, we lay out the essentials of how Bitcoin works. Our exposition strategy is to start with a simple money system and progressively fix bugs and add features until we arrive at Bitcoin. The discussion is conceptual rather than technical, and certain nuances are ignored for brevity.

We start with a familiar, simplified money system. Imagine a hypothetical community that uses a fixed supply of coins as money. Community members start with 10 coins each and everyone is willing to exchange goods and services for coins.

3.1 A Centralized Money System

There is a single community bank. Rules for the money system, along with a diagram, are below:

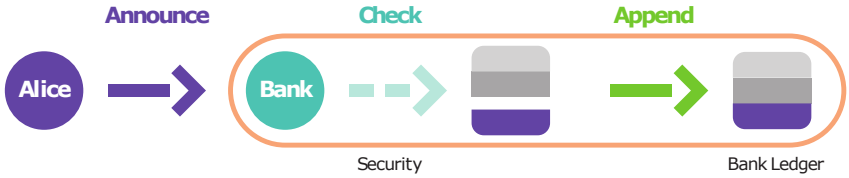
1. [ANNOUNCE] When someone wants to pay coins to someone else, she communicates the transaction to the bank. For instance, when Alice wants to pay Bob 2 coins, she tells the bank "Alice pays Bob 2 coins."
2. [CHECK] The bank checks if the transaction is valid by
    - Verifying that Alice authorized it
    - Verifying vs its internal ledger that Alice has enough funds
3. [APPEND] The process for adding the transaction to the bank's ledger is as follows:
    - If the transaction is validated by the bank, then the bank
        - Appends the transaction to its ledger, deducting from Alice and adding to Bob's account
        - Charges Alice a transaction fee of .01 coins

[3] See Abba Lerner, "Money as a Creature of the State", *American Economic Review* May 1947

[4] A pseudonym. The identity of the person or group that wrote the Bitcoin paper and created its protocol is not known.

[5] Common convention is to use "Bitcoin" with a capital B to refer to its underlying system, protocol, and community, and to use "bitcoin" with a lowercase b to refer to the tokens in that system. We will use the same convention in this paper.

Figure 1: Diagram of the Community's First System



In this system, the record of who-owns-how-many-coins is kept by the bank in its proprietary ledger (see Table 1 for sample ledger).

Table 1: The Bank's Ledger. Alice and Bob's Transaction is Appended.

From	To	Amount	Time	ID
Joe	Jane	5	3/21/17 10:30 AM	341
Chuck	Daisy	3	3/21/17 10:35 AM	342
Alice	Bob	2	3/22/17 10:30 AM	343

The system works well if people trust the bank. But suppose that community members are worried that the bank is tampering with the ledger for its own gain, or that it will freeze accounts, or that its transaction fees are too high. For citizens of Argentina, this situation is real. There is widespread distrust of banks and politicians, and people are not allowed to create competing banks. Their money is trapped.

The community decides to switch to a radically transparent, collectively managed money system.

3.2 A Decentralized System

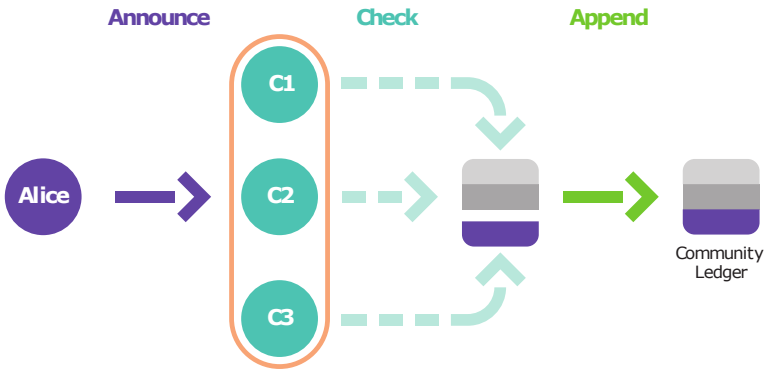
There is no longer a bank. In its place, the community has built a town hall. The bank's proprietary ledger is replaced by a **community ledger** which is managed according to the rules below. New items are marked in blue, and Figure 2 is the accompanying visual.

0. At the end of each day, community members gather in person at the town hall to conduct transactions
1. [ANNOUNCE] When someone wants to pay coins to someone else, she stands up and announces the transaction to everyone at the town hall. One person speaks at a time.
2. [CHECK] When a transaction is announced, everyone at the town hall checks if the transaction is valid by
   - Verifying that the payer authorized it
   - Verifying vs the community ledger that the payer has enough funds
3. [APPEND] The process for adding the transaction to the community ledger is as follows:
   - If the transaction is validated by a majority of community members, then a designated person
     - Appends the transaction to the community ledger

This system successfully eliminates the bank and gives the community control over the ledger. Note that, in passing from Figure 1 to Figure 2, the ledger is now open rather than proprietary. It is managed collectively rather than by an authority: it has become *decentralized*. This system is close in spirit to Bitcoin, though there remain a few key issues.

First, how is the community ledger kept secure? Is it physically housed at the town hall? If so, what keeps an adversary from breaking in and adding or deleting records from the official copy? If guards are installed, what keeps them from colluding with the adversary? **Second**, the labor of verification is shouldered by the community. It would be more practical to have dedicated laborers do this work. **Third**, there is no privacy: everyone can see everyone else's balances.

Figure 2: Diagram of the Community's Second System



3.3 Decentralized And Distributed

The community demolishes the town hall and implements three changes, one for each issue identified above. The first change is that there is no longer a single instance of the community ledger. Instead, the ledger is now *distributed*: everyone maintains **their own personal copy** of the community ledger, and rules are agreed in order to synchronize ledgers across members. This change makes it harder for an adversary to compromise the ledger: he would need to alter the many ledger copies. There is no single point of failure.

Second, community members no longer verify transactions themselves. Instead, they employ a group of "validators" to do this work. This is different from employing a bank because the ledger remains open and members can audit the work of validators at will. Validation is a paying job, and anyone who wants can become a validator. **Validators are paid for their work in the community's currency**.

The third change is that the system is now digital. Transactions are communicated over the internet, via email, rather than in person at town hall. To enhance **privacy**, transactions are now transfers between random email addresses ("public addresses") instead of actual identities. Members keep the passwords ("private keys") for their email addresses secret so that no one else can access their funds.[6]

The rules for the updated system are below (new items in blue), and the companion visual is Figure 3.

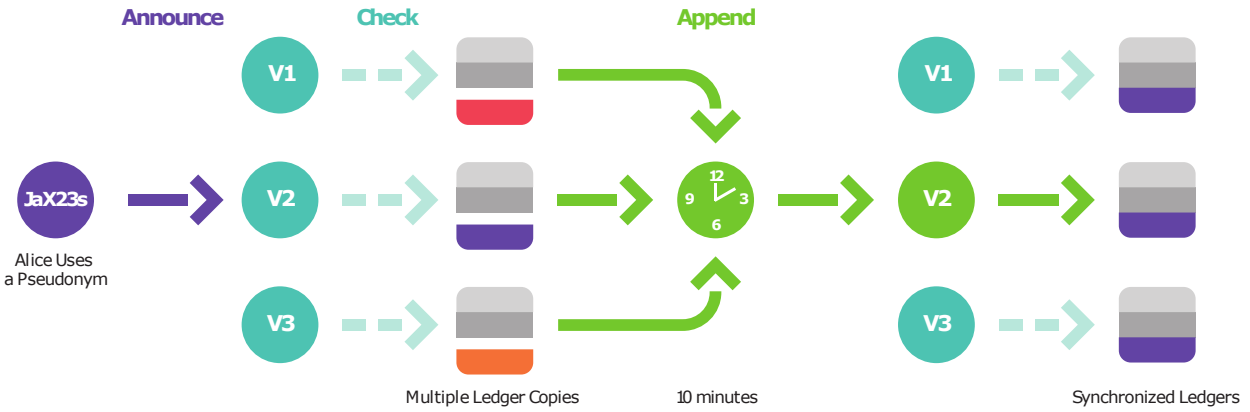
1. [ANNOUNCE] When someone wants to pay coins to someone else, she broadcasts the transaction to the community over the internet.
   - Anyone can broadcast a transaction at any time
   - Transactions contain public addresses rather than actual identities
   - Due to physical realities of internet lines, broadcasts are not heard by everyone in the same order
2. [CHECK] Validators pick an unconfirmed transaction that they've heard about and check validity by
   - Verifying that the payer authorized it (by checking its digital signature[7])
   - Verifying vs their copy of the community ledger that the payer has enough funds to cover the transaction
3. [APPEND] The process for adding to the community ledger is as follows:
   - Every 10 minutes, the network randomly selects a validator (V2) and that validator:
     - Appends his verified transaction to his copy of the community ledger, and
     - Broadcasts his updated community ledger to other validators

[6] We've described a public address as a random email address and a private key as its associated password. This is not literally correct but rather a good analogy that captures the concepts.

[7] A digital signature is a proof of access to public address. Its implementation uses cryptography. For details, see `https://en.wikipedia.org/wiki/Digital_Signature`.

- Other validators confirm that:
  - V2's ledger is valid, and
  - V2's ledger is longer than their own ledger (the "longest ledger policy")
- If confirmed, then validators update their ledger copy to match V2's and V2 receives .01 coins

Figure 3: Diagram of the Community's Third System



Comparing Figure 3 to Figure 2, note that the ledger has become *distributed*—each validator maintains a ledger copy and checks transactions against his ledger copy. The complexity of the "Append" process in Figure 3 is to synchronize these ledger copies.

The longest ledger policy in Rule (3) helps to establish a commonly agreed ledger. Suppose V1's ledger is not the longest (e.g., because it is stale) and he broadcasts his ledger to V2 and V3. They will reject his ledger. V1 can stubbornly continue to use his stale ledger but, per Rule (3), he won't get paid for verifying transactions. To receive payment, his ledger must be accepted by the other validators. Self-interest will lead him to use a ledger that others will accept. The longest ledger policy sets a shared expectation for what will be accepted.

The main problem with this system is the ease of subverting it. A malicious validator can create the longest ledger out of thin air. There is no way to tell if his ledger is the result of playing by the rules of the Append process or is simply manufactured. What's missing is anti-subversion logic.

3.4 Decentralized And Distributed; Dishonesty Is Costly

Bitcoin's brilliant anti-subversion logic uses ideas from anti-spam cryptography.[8] The mechanism, called **proof-of-work**, requires validators to expend lots of excess computation as part of the Append process. Proof-of-work can seem abstract and strange, like a ritual, but it will make more sense shortly.

After checking a transaction, validators are made to solve a cryptographic puzzle. Think of the puzzle as a number-guessing exercise. The validator's computer guesses random numbers until it happens to guess the right one. Each guess costs real-world resources (computing power and electricity), and validators are free to spend as much money on real-world resources as they like to maximize their number of guesses.

The first validator (say V3) to guess the right number is permitted to broadcast his ledger update to other validators. The other validators can easily check whether V3 guessed the right number.[9] If he did, they will update their ledgers to match his, and V3 will earn a reward in the community's currency. Then the process starts all over again for the next transaction with a new puzzle.

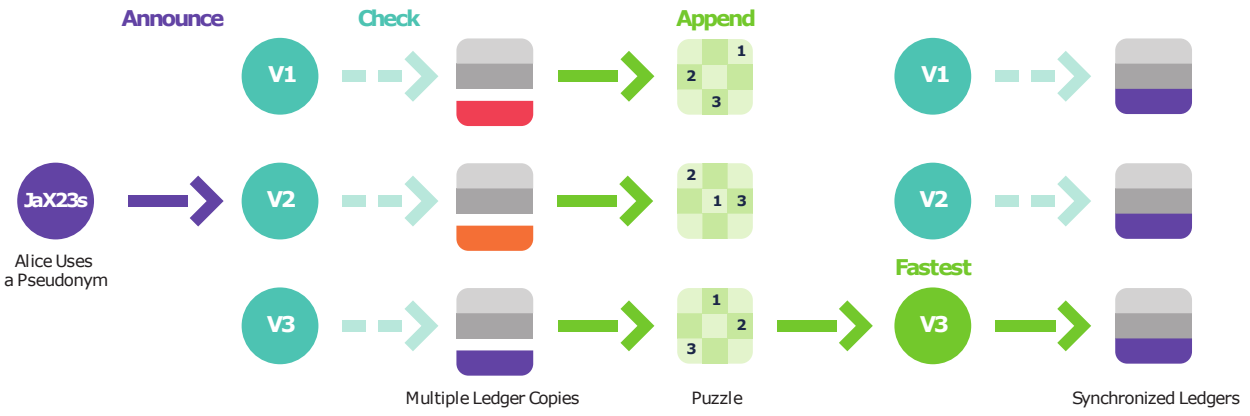
The rules of the new system are below (new items in blue, visual in Figure 4):

[8]Specifically Adam Back's hashcash, and Wei Dai's use of hashcash for digital money creation. See `http://www.hashcash.org/papers/hashcash.pdf` and `http://www.weidai.com/bmoney.txt`

[9]It is a neat mathematical property of the cryptographic puzzle that it is difficult to solve but easy to check.

1. [ANNOUNCE] When someone wants to pay coins to someone else, she broadcasts the transaction to the community over the internet.
    - Anyone can broadcast a transaction at any time
    - Transactions contain pseudonyms rather than actual identities
    - Due to physical realities of internet lines, broadcasts are not heard by everyone in the same order
2. [CHECK] Validators pick an unconfirmed transaction that they've heard about and check validity by
    - Verifying that the payer authorized it (by checking the digital signature)
    - Verifying vs their copy of the community ledger that the payer has enough funds to cover the transaction
    - Then they begin work on a cryptographic puzzle
3. [APPEND] The process for adding to the community ledger is as follows:
    - When a validator (V3) solves his cryptographic puzzle, that validator:
        - Appends his verified transaction and puzzle solution to his copy of the community ledger, and
        - Broadcasts his updated community ledger to other validators
    - Other validators confirm that:
        - V3's ledger is valid, and
        - V3's ledger is longer than their own ledger (the "longest ledger policy")
    - If confirmed, then validators update their ledger copy to match V3's and V3 receives .01 coins

Figure 4: Diagram of the Community's Fourth System



Passing from Figure 3 to Figure 4, the change is that proof-of-work is now part of the Append process. Validators do virtual jumping jacks, guessing numbers until one of them solves her cryptographic puzzle. Because each guess costs real-world resources, this procedure makes it **costly** to propose ledger updates.

Why? Because now when a validator proposes a ledger update with a puzzle solution, there is a baseline reason for others to believe him: *he has paid his dues*. Further, an adversary who wishes to tamper with the ledger would now need to amass *more resources than the other validators combined*.[10] Absent this, he is unlikely to win the guessing game and increasingly unlikely to maintain the longest ledger. Hence, the system becomes increasingly tamper-proof as more validators join and contribute resources.

[10]This is known as a 51% attack.

3.5 Putting It All Together

The protocol in Section 3.4 is essentially Bitcoin. Bitcoin calls validators "miners" and calls the community ledger the "public blockchain." A **blockchain** is a specific way to store data in which each new data element embeds a condensed copy of the prior element, all the way back to the first element. This makes it hard to alter past data without leaving traces on the most recent data.[11]

Bitcoin is a system for reliably and securely updating a distributed ledger without a central point of failure and no system owner. It enlists an impartial network of computers (owned by validators) to jointly manage and update the ledger. The ledger is open for anyone to check, is privacy-enabled and tamper-resistant, all without banks or central authorities.

Today, validators are rewarded primarily through the issuance of new bitcoins rather than transaction fees. The number of coins issued to validators is programmed to decrease over time, in such a way that the total number of bitcoins in circulation will plateau at 21 million in the year 2140 (versus the 16.55 million bitcoins in circulation today). Money supply increases are pre-programmed and transparent.

Bitcoin is called a "crypto" currency because it leverages cryptography in three places: in proof-of-work puzzles for anti-tampering, in digital signatures for anti-forgery, and via hash functions that link together elements of the blockchain itself.

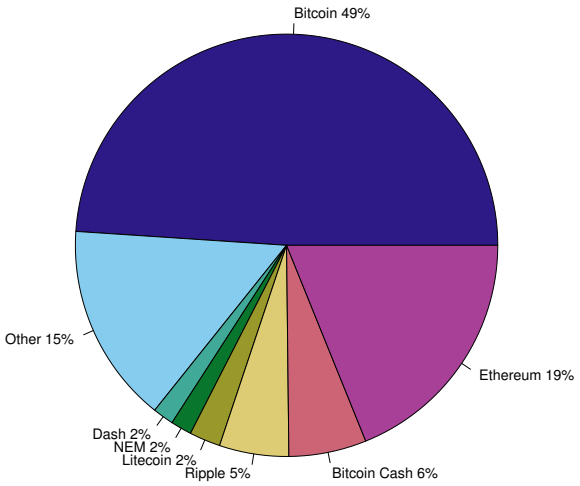
We turn now to the ecosystem of cryptocurrencies—also called "digital assets"—outside of Bitcoin.

4 The Larger Ecosystem (as of September 2017)

4.1 Overview

There are over 1,000 different digital assets today, and new ones are created each week. In aggregate, these assets have a market capitalization of around $140 billion. Seven assets account for 85% of this $140 billion and Bitcoin accounts for 49%. Figure 5 shows the market cap distribution by asset.

Figure 5: Cryptocurrency Market Cap Distribution



Why so many digital assets? Bitcoin is open-source, making it easy to copy and modify ("fork") its code. Naturally, some cryptocurrencies are born of greed and represent attempts by their creators to get

[11] For more details, see `https://en.wikipedia.org/wiki/Blockchain`.

rich quick. While forking Bitcoin's code is easy, building the community of users, developers and miners required to make the fork valuable is hard.

On a **micro-level**, cryptocurrencies differ in terms of features. Each cryptocurrency has its own ledger and its own rules for transactions. Each is a system unto itself. For example, Litecoin, worth over $3 billion, originated as a fork of Bitcoin's code and has faster transactions. Zcash has more privacy.

On a **macro-level**, cryptocurrencies differ in money supply issuance and tamper-resistance. Each has its own pre-programmed monetary policy. In Bitcoin, long-term supply is fixed at 21 million bitcoins; in others, issuance rates remain non-zero and supply grows forever. Bitcoin achieves tamper-resistance by forcing validators to solve cryptographic puzzles; some researchers are developing other tamper-resistance mechanics.[12]

On a **meta-level**, cryptocurrencies are a profound social experiment in how people agree on rules to govern themselves in the absence of central authority. Their **governance** structures are fascinating. In Bitcoin, only a handful of *core developers* can make changes to the code. However, only if the *miners* accept code changes do they become real. And if miners accept code changes that *users* don't like, users may stop holding bitcoin, which in turn hurts miners (since they are paid in bitcoin). There are implicit checks-and-balances in place between developers, miners, and users that discourages a change in rules benefiting only one group. When the community disagrees on a rule change, the ledger splits ("forks") and the separate groups follow different rules, with each ledger constituting a different currency going forward.[13]

Some cryptocurencies depart from Bitcoin's tripartite governance model. Dash, for example, adds a fourth constituency: *stakeholders*. These stakeholders ("masternodes") buy a certain amount of Dash in return for the right to vote on changes to its rules. Anyone can become a stakeholder. The idea is to position those most invested in Dash's success (i.e., stakeholders rather than miners or users) as stewards of the system. In contrast, the governance model of Ethereum is closer to de-facto benevolent dicatorship, with founder Vitalik Buterin wielding significant influence on community decisions in the face of conflicts. It is an open question which governance model is most efficient, fair, and sustainable. In equilibrium, there may well be a mixture of several models.

Via micro, macro, and meta-level differences, cryptocurrencies serve a variety of purposes and provide different kinds of utility. For the first time, it is possible to "vote with your feet" on monetary policy and governance structure. Some digital assets are not even money systems, but software platforms or services.

4.2 Ethereum and ICOs (This section is dense and can be skipped)

Ethereum, for example, is not a money system per se. It is the second largest digital asset with a market cap of $30 billion, and it is more abstract than Bitcoin. We saw that Bitcoin enlists a distributed network of computers (validators) to collectively **run a ledger**. Generalizing this, Ethereum enlists a distributed network of computers to collectively **run any computer program** (of which a ledger is but one example). The execution of these computer programs (called "smart contracts") is paid for with ether, its currency. Think of it as a system like Figure 4 where what is "announced" is not a proposed transaction but a proposed program execution.

Why is collective program execution useful? Say we want to run a political election online, and we write software to record and tally votes. The key issue is: who should run this software to administer the election? Probably not a private company, and probably not the government since incumbents have a vested interest in the outcome. It would be useful to have a computation engine that is owned by no one, that can run programs transparently. Enter Ethereum, a decentralized computation engine.[14] Developers can use it to run their applications when having a central authority run them is problematic or costly.

Ethereum is a platform that supports "decentralized apps" (dApps) like the voting app described above. dApps are compelling because—just as no one controls the ledger in Bitcoin—no one controls user data

[12] Currently the most popular is "proof of stake", in which validators contribute capital instead of computational resources.

[13] Figure 5 shows a 6% slice for Bitcoin Cash, which split from Bitcoin over a disagreement in August 2017.

[14] *Decentralized computing* on Ethereum is different from *cloud computing* on (for instance) Amazon. In cloud computing, nodes are rented in order to run a private program. In decentralized computing on Ethereum, all nodes run the same public programs at the same time. The latter is highly redundant and designed for tamper-resistance, not efficiency.

or program execution in dApps. This allows for the creation of (for instance) a decentralized version of Facebook in which user data is owned by the users themselves instead of by Facebook. Many dApps are being developed which are decentralized versions of common internet services.

Developers who build dApps create "tokens" to provision services in their applications. Token owners can use tokens to access the dApp. Because each token's supply is limited, tokens rise in value as demand for the corresponding dApp increases. The tokens constitute new digital assets, separate from Ethereum but dependent on its infrastructure. Ethereum's recent maturation has enabled the creation of hundreds of tokens over the last year.

Developers can sell tokens to investors in order to raise funds at various stages of dApp development. Though each token is unique, the lifecycle of a typical token is as follows: A team creates a white paper pitching their application. The application relies in some fundamental way on a corresponding token, which represents rights to future use of the dApp. Some of this token will then be sold and distributed through a crowdsale, raising money for product development.

This model is somewhat analogous to Kickstarter campaigns or crowd-funded equity, since the funds can be sourced globally, are raised as soon as feasible, and can resemble debt, equity, or hybrid structures. But unlike Kickstarter platforms, tokens are typically traded actively on exchanges *from their initiation*, giving a real-time price estimate to the projects they are tied to. Hence, the projects are like unregulated seed-stage companies doing an IPO. Following this analogue, the token crowd-sales are often called Initial Coin Offerings, or ICOs.

This year has seen over 100 ICOs raising a total of $1.25 billion, which is more than VC investments in the blockchain space. The majority of financing is from retail investors around the world, so much so that governing bodies like the SEC have issued warnings and guidance on how to avoid fraud. Chinese regulators banned ICOs in early September 2017. Clearly the regulatory framework is still evolving.

Now that we've surveyed the ecosystem of digital assets,[15] we turn to its investment merits.

5 Is It Worth Buying?

In the five subsections below, we lay out **five key arguments against** cryptocurrencies as well as counter arguments. Both the arguments and counter arguments have some merit. Given the variety of practical applications and governance structures discussed in Section 4, it is problematic to put all cryptocurrencies in one basket, but we do so anyway below for expedience.

5.1 It Has No Fundamental Value

In a recent and lively investor letter,[16] Howard Marks argued that bitcoins lack fundmental value. They provide no interest payments, no claim on profits or dividends, and no ownership of factories or other hard assets. Their price is based on demand which—absent intrinsic value or a real use case—is purely speculative. It's tulip mania all over again! According to JPMorgan CEO Jamie Dimon, it's even worse than tulips.[17] We offer three counter arguments.

First, Bitcoin differs from tulips in one crucial way: a positive feedback loop between **price and value**. When bitcoin **prices rise**, more engineers are attracted to the space and newly enriched Bitcoin entrepreneurs can afford to hire them. The dynamic is similar to a startup whose valuation is increasing: it can now attract more and better talent. This talent builds infrastructure and services—like easier payments, better user interfaces, more merchant support—that improves the Bitcoin ecosystem. This in turn drives more user adoption and **increases the value** for everyone through network effects. Higher prices also attract more validators which enhances ledger security. It is a classic case of George Soros' reflexivity,[18] in which an asset becomes more compelling as its price increases.

[15] We do not cover "private blockchains", which are enterprise-oriented permission-based ledger systems.

[16] See `https://www.oaktreecapital.com/docs/default-source/memos/there-they-go-again-again.pdf`.

[17] See `https://www.cnbc.com/2017/09/12/jpmorgan-ceo-jamie-dimon-raises-flag-on-trading-revenue-sees-20-percent-fall-for-the-t` `html`.

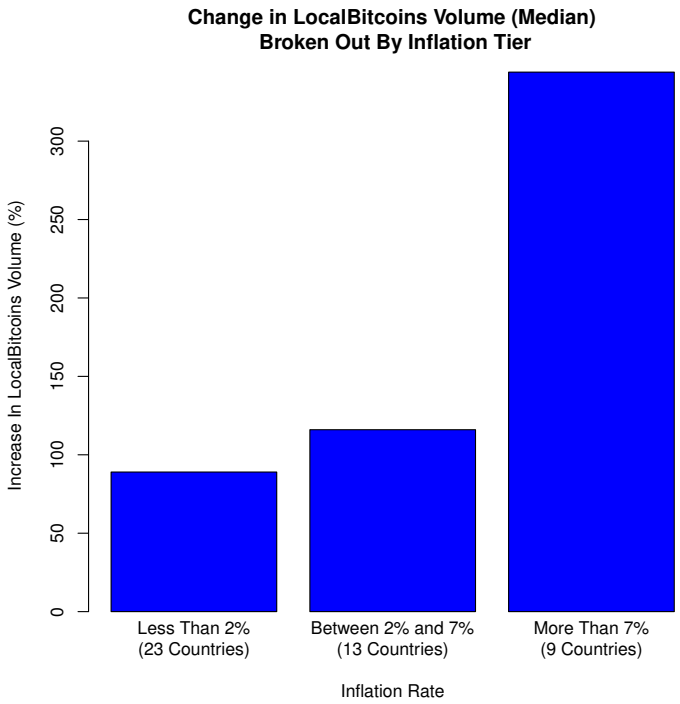
[18] A theory of markets developed by George Soros. See `https://www.ft.com/content/0ca06172-bfe9-11de-aed2-00144feab49a`.

Second, we've lived through many forms of money. In the 1970s, the US transitioned to a paper money system backed by trust in government. For much of history, trust in government was not worth much and citizens demanded gold or money backed by gold. Prior to 1913, money was a private affair: commercial banks issued money rather than the central government. Money systems derive value from social acceptance, which can evolve from generation to generation. Historically, this social acceptance has been based at various times on trust in central authorities, in the "intrinsic value" of gold, in the credit worthiness of commercial banks, or (with Bitcoin) in collective self-interest and cryptography.

Third, utility for Bitcoin exists today in parts of the world where trust in banks or currency is low. In Venezuela, inflation is over 100% per year and citizens are desperate to get out of local currency. They can't go to a bank and exchange bolivars for US dollars as that isn't permitted by the government. They can buy US dollars from black market dealers, but then those dollars have to be stored "under a mattress" and can't be used online. Or, they can buy bitcoin and have their holdings recorded in a secure global ledger; these assets can then be accessed anywhere there is an internet connection.

This is actually happening. Via data from Localbitcoins,[19] we examine how much local currency is being traded for bitcoin in a number of countries. The data consists of weekly volume for a set of 45 countries. For each country, we calculate the growth of volume in 2017 vs volume in the second half of 2016. This is a proxy for bitcoin demand-growth in that country. It turns out that **countries with the highest inflation rates have the highest growth in bitcoin demand**. Figure 6 illustrates. Among the 9 countries with inflation above 7% per year, median bitcoin demand growth is 350%. On the other hand, for the 23 countries with inflation below 2%, demand growth is only 90%.

Figure 6: Inflation Rate vs Bitcoin Demand



Bitcoin utility also exists in countries with **capital controls**: the same data shows that countries like China and Morocco have high bitcoin demand growth (1140% and 212%, respectively) despite having low

[19]The site localbitcoins.com is like a Craigslist for bitcoins in which people post offers to buy and sell bitcoins. Through the site, I can agree to meet someone at a local spot and exchange $20 for some bitcoin. Aggregated country-level volume data from localbitcoins.com is provided by coin.dance.

inflation rates.

5.2 Governments Will Crack Down On It

A second argument notes that Bitcoin, because of its privacy, is used by drug dealers, extortionists, tax evaders, and dark web users. It is used to evade capital controls. Imagine if terrorist organizations were to start financing their operations in bitcoin. Sooner or later, governments will crack down on Bitcoin. And there is historical precedent: Executive Order 6102 made it illegal for US citizens to hold gold bullion from 1933 to 1974. We now consider counter arguments.

A Bitcoin ban is difficult to enforce. Bitcoin is distributed and decentralized. There is no office building or company headquarters for the government to raid. So long as there is a single validator running somewhere in the world, the ledger continues to exist. Bitcoin is like a weed.

Governments can certainly make it hard for citizens to buy bitcoin by shutting down the private companies who act as on-ramps to Bitcoin (e.g. exchanges). This would curb demand and reduce bitcon's price. But it might also have unintended consequences. Some demand would shift to in-person black markets. Engineers and startups might migrate to Bitcoin-friendly countries.

In the end, a ban is unlikely. The CFTC is considering futures contracts on Bitcoin. This likely will pave the way for the SEC to approve cryptocurrency ETFs. A congressional caucus led by Jared Polis is advocating for blockchain technologies. Japan has legalized Bitcoin. The reality is likely to be evolving regulation that will require citizens to give up some privacy in exchange for continued free use of Bitcoin. Such regulation would decrease Bitcoin demand from criminals, and might increase demand from people who have stayed away due to uncertain regulation or perceived lack of legitimacy.

5.3 Central Banks Will Issue Their Own Cryptocurrencies

The third argument is that central bank issued cryptocurrencies will crowd out Bitcoin. In June, the IMF urged central banks to consider the merits of issuing their own digital currencies.[20] China has telegraphed many times its intention to issue a cryptocurrency. A few central banks are conducting pilot programs.

A central bank cryptocurrency is a representation of fiat currency on a distributed ledger. It is not a different currency but a different *implementation* of (e.g.) dollars. It could do useful things like instant taxation and real-time risk monitoring for banks. It could also significantly improve cross-border payments by uniting bank systems and ledgers.

But ultimately a **central** bank cryptocurrency is not **decentralized**. Bitcoin's value proposition of money that is "stateless" and free of inflationary monetary policy is not affected by the existence of central bank cryptocurrencies ("CBCs"). It is possible for CBCs and decentralized cryptocurrencies to co-exist. In fact, CBCs would legitimize cryptocurrencies and grow the pie of cryptocurrency users; Bitcoin would likely benefit. CBCs might even fuel incremental demand for their decentralized counterparts since CBCs would make surveillance of our money spending easier.

One related dynamic is next generation **currency wars**. In 2014 and 2015, Russia and China were enormous buyers of gold in a bid to reduce dollar reserves. In the future, we might have geopolitical chess in which central banks buy bitcoin to add a state-neutral, non-dollar asset to their reserves. Recently, a company in Russia connected to top politicians announced a large bitcoin mining operation that will exploit Russia's access to cheap energy.[21] Central banks may ultimately be buyers of cryptocurrencies.

5.4 The Reality is Less Glamorous Than the Theory

The fourth argument voices concern about a host of practical realities. How safe are funds in bitcoin? We hear about hacks in the news regularly. And how private is Bitcoin? Since the ledger is open, there is a risk of tracing public addresses back to actual identities. Finally, there is validator concentration risk: over 70% of mining power comes from China. We now consider counter arguments.

[20] See `http://finteknews.com/imf-central-banks-digital-currencies/`.

[21] See `http://www.zerohedge.com/news/2017-08-08/russia-launches-100-million-bitcoin-mining-operation`.

With respect to hacking, it is important to note that the Bitcoin blockchain itself has never been hacked. What has been hacked are private companies like exchanges that hold user funds. Some electronic wallet providers have also been hacked. While funds on the Bitcoin blockchain are safe, it is crucial for users to select safe vendors and safeguard private keys. Consensus has emerged which exchanges and wallets are safe.

With respect to privacy, Bitcoin's default privacy measures work for the majority of users. For highly active or high balance users, additional privacy is achievable through "mixing" services that further obscure public addresses. There also exist cryptocurrencies specifically optimized for privacy.

Miner concentration is a risk factor. If China outlawed bitcoin mining, Bitcoin's ledger would be backed by fewer validators and therefore less secure. In theory, Chinese miners could collude to tamper with Bitcoin's ledger, but this scenario makes less sense given miners' enormous investment in computational resources. They have a vested interest in seeing Bitcoin succeed. Researchers are actively investigating alternate validation mechanisms that are less subject to concentration risk.

In the end, the ecosystem is an **evolving** technology. Every identified practical issue has many technologists working on improvements. Today's practical risks put burdens on users to navigate the space carefully, and create opportunities for investors to spot and back technological improvements.

5.5 Bitcoin Is A Crowded Trade

Bitcoin is in the news every day and everyone has an uncle or grandma pitching it. It has gone up too much too quickly. A recent Bank of America survey showed that managers perceived long bitcoin to be a crowded trade.[22] No matter Bitcoin's merits, if it's crowded then it has significant downside risk.

Moreover, shorting bitcoin is not logistically easy. Skeptics have not been able to express their opinion in the market. If bitcoin were easy to short, its price would be lower. When futures markets do arrive, shorting will be easier and bitcoin's price will drop. We now consider counter arguments while noting that timing risks are very real, especially over shorter horizons.

First, absolute levels of bitcoin ownership are low, suggesting that we are early in the adoption cycle. We can see who owns how much bitcoin by looking at the public ledger. Only about 3 million public addresses have over $100 worth of bitcoin, and only 300,000 addresses have over $10,000 worth of bitcoin.[23,24] Reports using proprietary data have estimated the number of worldwide bitcoin holders to be on the order of 10 million.[25] A much larger number of people could naturally demand it: there are hundreds of millions of people in high-inflation and capital controlled countries, 2 billion people who don't have bank accounts, 500 million people who own stocks, and hundreds of millions of digitally native millenials.

Furthermore, bitcoin ETFs and futures don't yet exist. It is still a pain to access and store cryptocurrencies, especially more exotic ones. Hence, some would-be buyers are kept out, and there is pent-up demand.

Finally, there will be increasing demand from hedging and portfolio diversification needs. Bitcoin has exhibited low correlation to traditional asset classes (see Figure 7). Bitcoin has had negligible correlation (10%) to stocks. Interestingly, people often describe bitcoin as 'digital gold', but **in fact bitcoin has had zero correlation to gold**. This isn't to deny its merits as a safe-haven, but rather to suggest that the picture is more complicated. It has a safe-haven beta, but also other betas like sensitivity to adoption, high-profile thefts, and government regulation.

5.6 The Bottom Line

To summarize, cryptocurrencies can protect against high-inflation and capital controls. They get more secure and more developed as prices go up via price-value feedback loops. Central banks may legitimize them by issuing their own cryptocurrencies. And they may prove themselves as safe-havens in the next crisis.

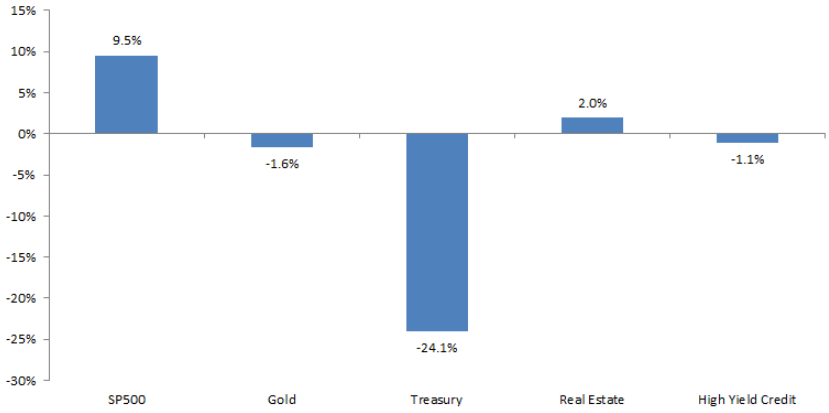
[22] `http://www.zerohedge.com/news/2017-09-12/its-official-long-bitcoin-most-crowded-trade-wall-street`.

[23] There isn't a one-to-one link between addresses and people: one person typically has multiple public addresses, and one public address (e.g, the address of an exchange) can hold the bitcoin balances of many people.

[24] For data on the distribution of bitcoin holdings by address, see `https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html`.

[25] See `http://research.ark-invest.com/bitcoin-asset-class` and `https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-cryptocurrency/`.

Figure 7: Correlations Based on Weekly Returns



At the same time, they may have gone up too far too fast. Most people in the US and the developed world have no need for them.

We can think of them as an insurance policy against low-trust states of the world. From that perspective, the prudence of buying depends not only on the price of the policy but also your portfolio's exposure to trust.

6 Conclusion

This paper began by asking: what are cryptocurrencies? In Section 2, we saw that money is about exchange, social trust, and state power. At their core, cryptocurrencies are a disruption of money. They decouple money from state power via decentralization. They decouple money from social trust via transparency and distributed validation. Their spirit is one of anti-establishment, of the freedom of money and, ultimately, the "sovereign individual". Price swings notwithstanding, the genie may be coming out of the bottle.

There remain many practical questions. How should one get exposure to the space? What are the trading realities? And the operational and financial risks? In a forthcoming paper, we discuss the practicalities of owning and trading cryptocurrencies; interested readers can sign up for it here.

Acknowledgments

Thank you to Arjun Balaji, Avichal Garg, Peter Green, Abe Othman, Charles Plager, Dave Rosen, Fatima Sabar, Steve Shadman, Tseno Tselkov, and Fabien Wang for valuable comments and insights.