#### **Origins** 1

N OCTOBER 31ST 2008, a paper authored bankers¹: (pseudonymously) by Satoshi Nakamoto was posted to a cryptography mailing list. Its title was "Bitcoin: A Peer-to-Peer Electronic Cash System", and it proposed a solution to the problem of secure transfers of value over the Internet without having to rely on third parties for trust. What is meant by that, is that before blockchain you needed to go through a bank, or a trusted service like VISA or Paypal to guarantee that a transfer of money would go through to a merchant when you purchased something online. Bitcoin allows us to do that without requiring such trusted third parties. The date of release leads us to suspect that the authors of the paper intended it to be more than just a technology to transfer money. In the climate of occupy wall street and similar movements across the globe, it is likely that the crypto-anarchists who started bitcoin intended it to be an alternative to incumbent fiat (government-issued) currencies. To get into the spirit, let us first revisit traditional fiat currencies and their problems to then be able to discuss how crypto-currencies propose to solve these in the next chapter.

#### 1.1 **FIAT CURRENCY**

A *fiat currency* is a legal tender whose value is backed by a government that issues it. Both USD, RMB, and EURO are examples of fiat currencies. The notion of currency usually evokes an image of physical money (cash), but it should come as no surprise that in this digital age, most money only exists virtually. More specifically, fiat currency is usually classified in the M's by

- M0: the amount of cash in circulation (bills and coins)
- M1: immediately available money: checking accounts, overnight deposits, and M0
- M2: savings accounts, short-term time deposits, and M1
- longer-term time deposits, institutional accounts, money market funds, shares, securities, and M2

Economists call M0 "narrow" money and M3 "broad" money. Regardless of the region, physical money is just a fraction of all the money in circulation<sup>2</sup>:

Indicator	US	Europe
M1	\$5,447 billion	€10,397 billion
M2	\$18,412 billion	€3,453 billion
M3	\$19,670 billion	€14,603 billion

#### **CENTRAL V.S. COMMERCIAL BANKS**

Where does this money come from? In most countries, a central bank (e.g., the Federal Reserve, BoJ, BoE, ECB) is responsible for controlling the supply of fiat currency. The bank that you likely use is a commercial or local bank,

<sup>&</sup>lt;sup>1</sup>The exact definition of an M differs from region to region, we adopt the U.S. standard here.

<sup>&</sup>lt;sup>2</sup>Non-seasonally-adjusted data for Feb 21, 2021. Source: FED, ECB

which takes direction from the central bank, but has some degree of autonomy. Somewhat surprisingly, banks do not need to have 1-to-1 collateralization of all their assets and balances (narrow banking). Instead, most world economies use the principle of fractional reserve banking where money is created through loans that are issued to customers (the most familiar being a consumer real estate loan). Consider the following example:

- 1. You deposit 100 dollars.
- 2. The bank puts 30 dollars in its reserves (30%).
- 3. 70 dollars are lent out to someone else
- 4. There are now 100 dollars + 70 dollars in circulation.

The bank is not fully collateralizing its liabilities (100 dollars) with assets (30 dollars). In this system, if a *bank run* were to happen, there would not be enough money for everyone to withdraw. What's more, the customer who took on a loan for 70 dollars can now go to another bank, which in turn can store 21 dollars (30%) in its reserves and borrow 49 dollars to another customer. The *money multiplier* is the total amount of money that can be created for every dollar spent in this way. It is easy to prove that it's equal to 1/r where r is the reserve ratio<sup>3</sup>. The total amount of money that can be created in this way for an initial deposit of 100 dollars is therefore 333.33... dollars.

Technically speaking issuing money is as simple as issuing a command to "create" a number in a bank's computer system. Of course, the

commercial bank has to report its daily deposits and lending activity to the central bank for oversight and record-keeping. Does this then mean that any bank can just print money? Yes and no. First, bank licenses are incredibly hard to obtain and banks that have licenses are strictly regulated by the central banks. Second, the overall amount of money that is created in such a fashion is closely monitored and manipulated by increasing/decreasing the cost of creation through a.o. minimum reserve ratio requirements.

#### **POLICY-MAKING**

Central banks are government-owned but are to a certain degree decoupled from day-to-day politics to ensure stability and conflicts of interest. Their monetary policies work with macroeconomic targets like "keep inflation at 2%" or "reduce unemployment at 5%". Furthermore, they are in charge of regulating local banks and providing financial services to them. Through their policies, they have the power to dynamically change the supply of money to incentivize economic growth. For instance, they may decide to make borrowing money cheap (as described before) which encourages people to invest more. If they make money too cheap, however, they risk causing high inflation which burns people's savings among other things. Governments themselves can also influence growth and inflation directly by enacting fiscal policies. For instance, a government that wants to stimulate economic growth could reduce taxes to incentivize spending, or even create large investment projects itself to create a demand for goods and services which ultimately should lead to an increase in jobs. While such fiscal policies were initially championed by Keynes as a reaction to the 1930's depression, the underlying philosophy is still very much alive as is evidenced by the U.S. post-corona fiscal policies.

This works great when governments have great foresight and act with prudence. For instance, we know from economic literature that

<sup>&</sup>lt;sup>3</sup>This result stems from the underlying geometric series  $\sum_{i=0}^{\infty} (1-r)^i D_0 = \frac{D_0}{r}$ , where  $D_0$  is the initial deposit.

Country	Central Bank	Reserve Ratio (2022)
China	People's Bank of China	10.00%
<b>United States</b>	Federal Reserve	0.00-10.00%
Kenya	Central Bank of Kenya	4.25%
Euro Area	European Central Bank	0.00-1.00%

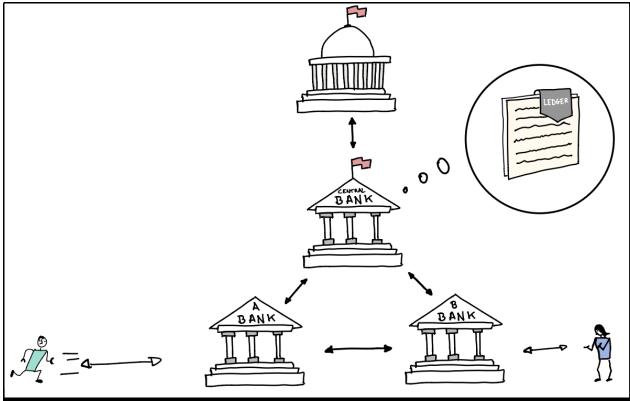


Figure 1: Simplified, schematic overview of how fiat currency transactions work. When person A transfers money to person B, their banks will interact to do the transfer on their books. At a set time of the day, both local banks will propagate their books to the central bank which stores them in their central ledger. The central bank can manipulate the ledger to enact policies.

commensurate spending on education can yield double-digit returns on investment thereby benefiting the nation as a whole. We know from history, however, that governments are not always as flawless as we would like them to be. Countries with high inflation (e.g., Venezuela), high political risk (e.g., Argentina), or low access to traditional banking (e.g., Zimbabwe) are plagued with currency problems making life for citizens very hard. At the height of the Weimar republic's inflation around 1922 the cost-ofliving index increased from 41 in June to 685 in December, a more than 16-fold increase! (Figure 2). In this way, governments harm their reputations by - in Hayek's words - "constant concessions to the expediency of the moment at the price of destroying the whole system" Its therefore only natural that informed citizens whose savings suffer from bad policy look elsewhere for their stores of value. Indeed, if you know your currency is going to be worth half of what it is worth now next month, the best move is to exchange it as soon as possible for a more stable store of value such as the USD, or the EURO. Sadly, a classical riposte of governments is to then outlaw foreign exchange of their local currencies.

#### The Iraqi dinar (Harvey 2021)

After replacing the Indian Rupee in 1932, Iraq finally go its own currency. For a time, the Iraqi dinar creation process was outsourced to Switzerland (printing plate manufacturing) and the U.K. (printing). As the war in Iraq erupted, the U.K. was no longer allowed to export to Iraq due to the economic sanctions put in place. In reaction to this, Saddam Hussein decided to change to lower-quality paper currency printed locally (the Saddam dinar). Despite the central bank no longer backing the old Swiss dinar, it was still used in the North Kurdistan region as the official currency.

Following the Kurd's reluctance to follow the new dinar system, a dual system remained in



Figure 2: Children playing with stacks of hyperinflated currency during the Weimar Republic, 1922 the depicted stack of bills was worth less than 1 dollar.- Rare Historical Photos

place. The Saddam dinar start inflating rapidly as Saddam decided to turn on the printing press to fund the war efforts. The total circulation increased from 22 billion in 1991 to 584 billion in 1995 (250% year-over-year inflation). The Swiss dinar supply remained constant and even decreased a little bit due to notes being taken out of circulation (no new notes were printed after 1989). Ten years after the start of the dual system, the Swiss to Sadam dinar ratio was 100:1. It further ballooned to more than 300:1 as the invasion ensued in late 2002.

The issues with a policy are not limited to just a handful of "problem countries". Even in the "developed" Western world, manipulation of currencies is widespread. In the next section, we cover Quantitative Easing, a modern experiment in monetarism where policies now focus on the volume of money instead of its price. It is educational to understand how money works in modern economies.

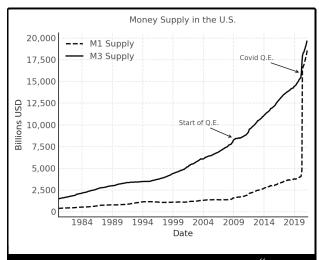


Figure 3: In crypto-maximalist terms: "Money Printer Goes Brrr".

#### **QUANTITATIVE EASING**

Quantitative easing is a monetary policy tool that originated in Japan but has become a popular instrument since the 2008 financial crisis. Under traditional QE, the central bank buys pooled debt (bonds or so-called mortgage-backed securities) from local banks. E.g., if the FED "buys" \$1 trillion dollars in bank deposits, it puts those assets on its balance sheet and gives the original owner a note stating that they are owed \$1 trillion dollars in return (aka a "liability"). Therefore, the central bank does not actually pay money to the local banks but changes a virtual balance number in their own records. This is, of course, the same as increasing the total supply of money. Figure 3 shows the effect of Q.E. in the US <sup>4</sup>.

The original purpose of Q.E. was to spur economic growth and avoid defaults by making cash cheaper, and more accessible to businesses and investors. Indeed, asset prices tend to go up and long-term government bond yields down. Moreover, increasing the supply of money makes it a potentially interesting time for foreign investors to invest in U.S. markets. The belief of policymakers is that these benefits, when taken to-

gether, will eventually "trickle-down" to the rest of the economy. In summary, there is some evidence that Q.E. can help in averting crises.

What's not to like then? Some critics say that it has created asset bubbles because things have been bought on cheap money (thereby kicking the real issues further down the road). According to the laws of supply and demand, more money created should mean that every unit is worth less (but it seems that that effect has been somewhat limited due to the dollar hegemony on oil markets). Of course, the crux of the matter is not how much money has been created, but what happens with the money that has been created. As mentioned before, a savvy government may get a good return on investment on every dollar created thereby benefiting citizens. Unfortunately, the way that Q.E. and Modern Monetary Theory (the 2020 incarnation of Q.E.) have been set-up, always seems to lead to the well-off reaping all the benefits because they already own certain asset classes that are targeted (stocks, bonds, properties, ...). People who live from paycheck to paycheck or with a little bit of savings in hand have probably seen their wealth decrease due to Q.E. The end effect is, therefore, a financial crisis avoided at the expense of largely increased wealth inequality. Is there a better way?

#### **PROBLEMS WITH CEFI**

In order to understand what solutions cryptocurrencies offer, we must first systematically review what problems centralized finance has beyond misdirected policy making due to centralization.

#### **Limited access**

In most banks that have originated in developing economies, access is limited by banks to profitable (rich) consumers. For instance, if you are poor you may not be allowed to open a bank account in some countries. An eye-opening historical example of this is the practice of "redlin-

<sup>&</sup>lt;sup>4</sup>https://fred.stlouisfed.org/series/M2SL

ing" in the U.S., where predominantly black areas where marked in red ink on mortgage lenders' maps. This practice caused lower investments in Black people areas which exacerbated existing inequalities. While such practices are generally frowned upon and nowadays even illegal, this type of discrimination remains in other segments of the services and in more covert ways. In many countries, you will be declined access to a brokerage account or credit if you do not meet strict requirements imposed by the bank. The result is that about 1.7 billion adults remain unbanked as of 2021. The leader is Morocco with 71% of its adult population being unbanked. Surprisingly, even well-developed economies like the U.S. (7% unbanked) and France (6% unbanked) are largely underserving their poorest constituents thereby severely limiting upward mobility and basic human safety.

#### Inefficiency

When you issue an order to transfer money using a traditional bank, the bank changes your balance and signal to the other bank to increase the recipient's account using SWIFT, SEPA, and similar money transfer protocols. Despite the fancy names, traditional bank transfers are anything but swift. Balance updates are typically settled by legacy systems in the back-end at a set time of the day by all banks through centralized systems that communicate with the central bank (ACH in the U.S., RTGS in most countries). International transfers are much slower as local banks need to send these to their international branches which then do the forex, anti-money laundering checks, etc.

#### **Expensive**

Due to the inefficiencies and vulnerabilities to fraud, the traditional banking system has huge overhead costs. Credit card payments and wire transfers can easily cost anywhere from 2 to 10% depending on your bank and region.

#### **Lack of Interoperability**

Banks are typically monolithic institutions with decades-old IT infrastructures that are siloed off from other banks. It is challenging for banks to innovate or even communicate within their own systems, let alone communicate with other banks. Interoperability is non-existent or relies on hacks that are not sustainable.

#### **COBOL**

Today, 43% of all banking systems use the COBOL programming language that was developed in 1959. COBOL is used for 95% of all ATM card swipes, 80% of all in-person credit card transactions, and handles more than \$3 trillion dollars of daily volume. COBOL is no longer taught in CS classes and most COBOL programmers are retired or passed away by now.

#### **Opacity**

The banking world is opaque. Unless consumers have insider access and extensive knowledge of finance, it is impossible for them to know what is going on inside of the bank. Simple things like knowing the sustainability and health of the bank are difficult. Problematic processes like discriminatory onboarding, inequal treatment, and unfair advertising are hard to prove. The end result is an incredibly inefficient ecosystem of expensive audits and stringent regulations which bar new entrants.

#### 1.2 CRYPTOCURRENCIES

#### **HOW CRYPTO-CURRENCIES ARE CREATED**

The crypto-anarchists who developed the early cryptocurrencies believed that the supply of money should not be put in the hand of individuals, but rather in immutable code. At their core, cryptocurrencies like Bitcoin feature a transparent algorithm which governs the monetary policy of the currency. Bitcoin's monetary policy was originally published in Nakamoto's paper and goes as follows:

- fixed number k of Bitcoins
- 2. Approximately every 4 years (every 210,000 blocks), set k equal to k/2.

This is a simple enough algorithm that results in the money supply schedule shown in Figure 4.

On the left, you see that indeed every 210,000 blocks, the number of bitcoins that are released halves. This event is appropriately called a *bit*coin halving and usually goes hand-in-hand with high volatility and Youtube channels filled with "to the moon" -memes and questionable investment advice. More importantly, we see that unlike fiat currencies bitcoin is deflationary. Another way to see this is to juxtapose bitcoin's supply curve with the M2 curve from fiat currencies. Inflationary fiat currencies lead to upward curving supply curves whereas bitcoin's is flat at the end, because each year, fewer bitcoins are released. We can calculate the total number of bitcoins that can ever be minted in this geometric series as<sup>5</sup>:

$$M_{\text{bitcoin}} = \frac{\sum_{i=1}^{32} 210,000 \times \lfloor \frac{50 \times 10^8}{2^i} \rfloor}{10^8}$$

Bitcoin's monetary policy is reminiscent of commodities with a decreasing supply like gold (which is why some people like to call "digital gold" ). We will postpone the question of whether or not bitcoin is good money to later. For now, note that it is probably better to consider it an asset class in and of itself that is neither completely gold-like nor money-like. At the time of writing, 18.2 million such bitcoins had been released with a valuation of 9,689 USD for a total of 1176.37 billion USD. By the time you are reading this chapter, the valuation will likely have dramatically changed (you can access the latest data on https://coinmarketcap.com/currencies/bitcoin/).

1. Approximately every 10 minutes, release a Regardless of what the numbers are, they are sure to be mind-boggling. To put at least some perspective on these, it is still a small asset class that comprises only 0.5-2% of total narrow money in the world.

#### **SOLVING CEFI**

#### **Limited access**

Anyone, anywhere in the world can open one or more cryptocurrency wallets for free. Once opened, such a wallet can be used to access the full spectrum of financial services at favorable terms similar to "rich" segments of the population and large institutions in CeFi. There are no restrictions on the development of new financial products beyond technical knowledge. Those who lack the required skills are typically allowed to participate in the democratic governance of DeFi projects by buying a stake in the governance of the underlying protocols.

#### Inefficiency

Unlike CeFi, cryptocurrencies have low-to-none organizational overhead. Users control their own funds and monetary policy and transactions are mostly handled by the code automatically. It is inconceivable, for instance, to think that one can transfer money almost free of charge from El Salvador to the U.S. in less than 10 minutes using traditional banking. Novel programming languages allow developers to code opensource money protocols which can be copied, and improved upon in quick bouts of iterations. This model encourages innovation over monolithic structures with extremely competitive pricing structures.

#### **Lack of Interoperability**

As we will see later, cryptocurrencies and financial protocols that build on blockchain technology are by definition interoperable. Composability and standardization of assets is a key

<sup>&</sup>lt;sup>5</sup>Note the usage of the floor operator  $|\cdot|$  which rounds a number down. E.g., |3.2| = 3.

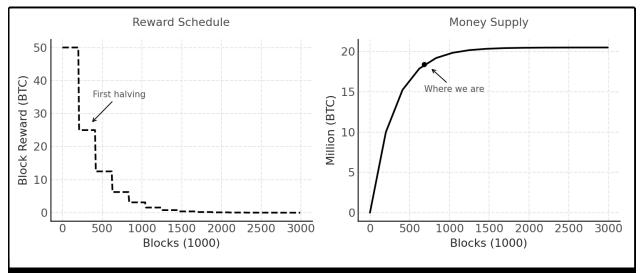


Figure 4: The bitcoin supply schedule (right) is determined by the reward schedule of its miners (left).

defining features of DeFi. Cryptocurrency finance is often referred to as money "Legos" in that many protocols can be stacked together to form complicated hybrid financial products. As the users are in control of the funds, they can choose to compose their portfolios in whichever way they want with whomever they want. They could, for instance, get a USD loan that is collateralized with a digital artwork that they purchased earlier to then invest in Bitcoin.

#### **Expensive**

By cutting out the middle management layer, financial products become much cheaper. Transactions are done efficiently requiring only an internet connection and a - typically - small transaction fee.

#### **Opacity**

Most crypto-currencies are transparent. Code that manages cryptocurrencies is open-source and transparent. Users are deterministically able to tell what the code will do under which circumstances to make an informed decision on whether or not they trust that code to handle their assets. Malicious behavior is discouraged by adding game theory and economic incentives to the protocols. All actions are logged and added to the underlying distributed ledger for everyone to see.

#### THE VALUE OF A CRYPTOCURRENCY

A natural question to ask is why anyone would want such a cryptocurrency? As F.A. Hayek "Some people apparently find it wrote in 1990: difficult to believe that a mere token money which did not give the holder a legal claim for redemption in terms of some object possessing an intrinsic value (equal to its current value) could ever be generally accepted for any length of time or preserve its value. They seem to forget that for the past 40 years in the whole Western World there has been no other money than such irredeemable tokens. The various paper currencies we have had to use have preserved a value which for some time was only slowly decreasing not because of any hope of ultimate redemption, but only because the monopolistic agencies authorised to issue the exclusive kind of currency of a particular country did in some inadequate degree restrict its amount"

1.3. WHAT IS MONEY?

(Hayek 1990).

A more positive answer is to consider all the new DeFi features that cryptocurrencies allow. The digital decentralized nature of cryptocurrencies makes transfers fast, cheap<sup>6</sup>, and secure. It allows us to bypass expensive banks and their legacy systems and keeps the user in control of their money. Most of the value of cryptocurrencies today is intangible (similar to the Swiss dinar), though as the ecosystem grows certain aspects have become collateralized - stablecoins being the prime example.

There are of course, also a couple of downsides that could impact such an intangible valuation. Precisely because there is no government backing them, the valuation is completely dependent on supply and demand by a heterogeneous group of people which makes them susceptible to bank runs and bouts of high volatility due to speculation. More importantly, you cannot pay your taxes using cryptocurrency as most governments only allow their domestic currency to be used for this purpose (this is probably one of the strongest reasons why traditional fiat currencies will never completely go away). Furthermore, it is perfectly possible for one coin to fall out of favor for another rendering the first valueless. While the top cryptocurrencies seem to retain their value, for now, their high volatility makes them unsuitable for making dayto-day payments<sup>7</sup>. Lastly, it is still a relatively new invention that requires some technological savviness to use. It is easy for people to get scammed or lured into pyramid schemes. In a similar vein, many novice crypto users use cen**tralized exchanges** (like Coinbase, and Binance) which (just like regular banks) keep your crypto

in an online account. Centralized exchanges offer more convenience at the expense of security with the user giving up control and potentially being vulnerable to hackers. Many of the more notorious hacks in the history of cryptocurrencies have been the result of attacks on centralized exchanges and led to the complete loss of user funds.

#### 1.3 WHAT IS MONEY?

We use money every day taking for granted the properties that make it a convenient means of storing and transferring value and wealth. We have seen that crypto aims to solve some of CeFi problems related to inaccessibility, inefficiency, etc. As many cryptocurrencies are explicitly positioning themselves as alternatives to fiat currencies (monies), let us think about what qualities money should have irrespective of the technology used.

Table 1 shows properties and a subjective ranking of both fiat and cryptocurrencies along desireable characteristics. Foreshadowing the later chapters, we can observe that (a) the fiat U.S. Dollar does not always score well on these properties, but (b) neither does crypto. In fact, a large part of the crypto community's experimentation efforts are currently directed at trying to overcome its shortcomings.

#### 1.4 FUD

A term you will see floating around once you follow crypto-channels is FUD (Fear-Uncertainty-Doubt). It is a colloquial term for misconceptions that keep coming regurgitated by critics. While some of these have a source of truth to them and it is important to understand why people mention them, many have by now been debunked. We will dive deeper into most of these in the later chapters, but let us already some comments that you may have come across before reading this book.

<sup>&</sup>lt;sup>6</sup>Note: recently transfers have become victims of their own success with transactions being quite expensive due to congestion of the networks. Improvements have been proposed including L2 solutions for Ethereum and Ethereum 2.0, and the Bitcoin Lightning Network. For reasons that are beyond this introductory chapter, bitcoin's core (L1) network is likely to stay expensive for the years to come.

<sup>&</sup>lt;sup>7</sup>This problem is being solved now, as we will discuss in the chapter on stablecoins.

Property	Description	Fiat	Bitcoin	Sheep
Durability	Not perishable	©	©	<b>P</b>
Portability	Easily carriable	<b>©</b>	<b>©</b>	
Divisibility	Smaller units easily possible	<b>©</b>	<b>©</b>	
Uniform	Same value for the same unit everywhere	<b>©</b>	<b>©</b>	
Limited Supply	Cannot easily create more		<b>©</b>	
Acceptability	Everyone recognizes and accepts it	<b>©</b>	<b>(</b>	
Stability	Value remains stable over time	<b>(3)</b>	<b>(</b>	©
Sovereignty	A holder remains in control of her money		<b>©</b>	<b>©</b>

Table 1: Desireable properties of money.

## Cryptocurrencies are mainly used for illegal purposes

While it is true that some cryptocurrencies have been used for illegal purposes, they are - in fact - a terrible choice for this purpose! Most of the main crypto-currencies are relatively easy to trace due to their transparent nature. Even though we may not know who is behind a crypto-currency wallet, authorities can figure it out once they try to cash out through a regular bank. By far, the number 1 asset used in illegal transactions is still cash. Does that mean we should abolish cash?

## DeFi is too difficult to use for regular consumers

DeFi is still early-stage and indeed too difficult to use for many mainstream consumers. Even so, any technology goes through a phase where it is difficult to use before it becomes easier. We see this as a positive thing as the more limited it is, the more value can be captured by those willing to make the effort. There is no technological reason why it should remain difficult to use in the long term. In our view, this argument favors the bull case for the DeFi.

## Governments will regulate cryptocurrencies rendering them illegal

While it is true that some governments are threatened by cryptocurrencies and regulation is on its way, it is certainly going to stay in at least some parts of the world. At the time of writing two nations have made Bitcoin an official legal tender, and many governments are starting to propose crypto-friendly regulations. What the situation will look like once the regulatory dust settles is hard to predict, but complete illegality seems unlikely.

# Cryptocurrenices are like tulips: a bubble that will pop one day or another / All of crypto is one big Ponzi

There have indeed been several pump-anddump schemes in crypto-currencies and there will be several more in the future. Even so, this does not mean that all of crypto is indeed a Ponzi scheme. Just as you do your due diligence when buying real estate or joining one bank or another, you also need to do your due diligence when investing in the crypto-space. Crypto should not be seen as a panacea to these types of bad actors. This book - while not financial advice - is a good starting point. 1.4. FUD 11

## Cryptocurrencies are not backed by anything and therefore will always tend to zero

funds to date were due to user negligence or centralized exchanges being insecure or reckless, not due to some flaw inherent in the technology.

History shows that it is possible to have value without being backed by some underlying asset or authority. Until the '70s the U.S. dollar was backed by gold, now it is not. The U.S. dollar is backed by intangibles (need to pay taxes, legal requirements to accept dollars anywhere in the U.S., etc.). Another example is the Iraqi dinar as shown before. These examples shows that a currency can indeed be backed by intangibles like what people think it is worth and the acceptability by the people as opposed to the strong hand of the state.

### Cryptocurrencies are an ecological disaster

Cryptocurrencies today have a relatively smaller footprint than CeFi. With new innovations such as Proof-of-Stake consensus protocols, the ecological footprint will be negligible. We will talk more about this point in the coming chapters.

#### Cryptocurrencies are too volatile and risky

Investing in this space requires investment discipline and knowledge. There are ways to reduce both the risk and the volatility to almost zero, but remember that most of finance is an exercise in trading-off risk and rewards.

#### Cryptocurrencies are not safe

Variants of this argument will refer to quantum computers or the fact that a lot of crypto was lost to date. Crypto-currencies use the same (and sometimes more stringent) encryption and hashing standards as CeFi and e-commerce. If these could be broken, all of the internet would be broken. When quantum computers become mainstream and more capable and e.g., Shor's algorithm becomes viable (used to break encryption), it would be easy to switch to quantum-resistant forms of cryptography. Most losses of

12

#### 1.5 FURTHER READING

- Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System" https://Bitcoin.org/Bitcoin.pdf
- Vitalik Buterin "A Next-Generation Smart Contract and Decentralized Application Platform"
- https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf
- http://fedguy.com/the-mechanics-of-quantitative-eas
- The Institutions of Monetary Policy The Ely Lecture 2004, Mervyn King. https://www.bankofengland.co.uk/-/media/boe/files/speech/2004/the-institutions-of-monetary-policy.pdf
- https://www.statista.com/statistics/1246963/unbanked-population-in-selected-countries/
- Campbell R. Harvey, "DeFi and the Future of Finance"