

## BitCoin and Digital Currency

*“There is a rule set up in Senator Edison’s Outlook account,” she pointed out. “All the emails he sends out are also forwarded to another address. Also everyone he receives is forwarded as well. I bet he doesn’t even have a clue it’s there.”*

*“What’s the other address?” Fabz asked.*

*“It is Mr.Casus.Belli@gmail.com,” Hannah reported.*

*“Let’s Google it,” Leon said. “People always use the same usernames in multiple places. I bet it poops up somewhere else.” Leon grinned at his pun.*

*They each began scouring the Internet for the Mr. Casus Belli email address on four separate laptops. To an outsider, it most likely looked like some kind of geek game show where contestants have to search for obscure trivia or the origination of urban legends. Bob was the first to buzz in.*

*“Found it!” Bob announced.*

*“Where are you?” Leon asked.*

*“On a discussion forum about bitcoin,” Bob said. “It appears to be affiliated with one Victoria Drazen.”*

*“I’ve heard that name before,” Hannah said, tapping something quickly on her keyboard. “Yes, that is the Senator’s Aid. His right hand man, so to speak... or in this case, woman.”*

Salt, gold, cash, and six-packs of beer have all been considered appropriate means of payment for goods by society over time. Many of society’s concerns revolve around the state of the economic system in any given country, with local currency in a volatile state depending on national prosperity and current relations with other nations. One of the most notable aspects to many forms of such currency is its anonymity. For example, if a \$100 USD bill was found within a residence, there would be no way to link it to its owner, nor to the person who gave it. In commercial shopping, there is no practical way to use money from a cash register to track who purchased a certain item.

While this level of anonymity may be beneficial to a regular citizen wanting to buy or sell goods in a local region, it doesn’t scale well across state or international lines. A citizen would have to jump through numerous hoops in order to anonymously donate money to a humanitarian charity located in another country. While cash can be couriered directly to its recipient, the exchange of money, especially larger amounts, is regulated and tracked. If someone wanted to send a payment for \$20,000 USD to a friend in another country, that transaction could be easily tracked by each respective government, and their law enforcement agencies, to determine the parties of the transaction and why the money was sent. Traveling with cash may seem to be a more anonymous form of sending money, but many countries require that this be tracked as well. The United States Customs and Border Protection agency requires that any travel out of the United States with over \$10,000 USD of currency be declared in writing.<sup>12</sup>

Not only are large transactions tracked, but currencies used in modern society all rely upon a central authority. These authorities, named Central Banks or Money Authorities, control the legitimacy and amount of currency within a market. The total amount of money available on the market is strictly controlled by a single organization, like the United States Federal Reserve.

In the early days of the Internet many online currencies formed, each competing for the ability to quickly send money afar. One of the early forerunners was e-gold, a service

incorporated in 1996 that provided online currency that was backed by physical gold. Until its closure in 2009, the online server grew to over 3 million accounts. However, in a move that led to the downfall of e-gold, its service did not verify the identity of user accounts as required by US law.<sup>13</sup> By not verifying those behind accounts, and not monitoring suspicious activity, the e-gold service became a core component to online crime and the sale of stolen credit card numbers. However, its creation shone light on large gaps within the US tax structure, as e-gold didn't consider itself either a money-transfer system or a bank, but instead as a payment system. Due to this confusion, its founder Douglas Jackson pled guilty to charges of running an unlicensed money transmitter business and aiding money laundering.<sup>14</sup>


Another idea then came forward by an identity known as Satoshi Nakamoto for a decentralized, online currency model unlike anything the world has seen. Named Bitcoin, this new digital currency would act independently of any central authority. The task of controlling growth and legitimacy would occur based on the cryptography algorithms used to generate currency, giving rise to a new class of money named cryptocurrency that put the power in the hands of the currency holders. Unlike e-gold, which was backed by an owner with a physical gold backing, Bitcoin did not have any centralized money store or ownership.

At a high level, Bitcoin appears to be a well-executed experiment into a decentralized money exchange. New Bitcoins are introduced into the market at a regular rate, though there is a set limitation of 21 million Bitcoins. However, at the rate of Bitcoin release, it will theoretically be over 100 years before this limit is reached.<sup>15</sup> The incredibly small amount of currency forces transactions to occur in fractions of a single Bitcoin, or BTC. The current small unit of currency in Bitcoin is 0.00000001 BTC, also known as a Satoshi. This is one hundred-millionth of a Bitcoin and, while comparable to an incredibly small amount of USD, allows for a large amount of inflation in BTC value.


In an early forum posting on [BitcoinTalk.com](http://BitcoinTalk.com), Satoshi made the following remarks as to the relative value of Bitcoin, challenging the concepts of traditional currencies based upon the physical characteristics, and rarity, of a tangible item.<sup>16</sup>

**satoshi**  
Founder  
Sr. Member  
●●●●●●

Activity: 364



Ignore

 **Re: Bitcoin does NOT violate Mises' Regression Theorem**

August 27, 2010, 05:32:07 PM

---

As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties:

- boring grey in colour
- not a good conductor of electricity
- not particularly strong, but not ductile or easily malleable either
- not useful for any practical or ornamental purpose

and one special, magical property:

- can be transported over a communications channel

If it somehow acquired any value at all for whatever reason, then anyone wanting to transfer wealth over a long distance could buy some, transmit it, and have the recipient sell it.

Maybe it could get an initial value circularly as you've suggested, by people foreseeing its potential usefulness for exchange. (I would definitely want some) Maybe collectors, any random reason could spark it.

I think the traditional qualifications for money were written with the assumption that there are so many competing objects in the world that are scarce, an object with the automatic bootstrap of intrinsic value will surely win out over those without intrinsic value. But if there were nothing in the world with intrinsic value that could be used as money, only scarce but no intrinsic value, I think people would still take up something.

(I'm using the word scarce here to only mean limited potential supply)

#10

In practical terms, Bitcoin is a digital currency that allows for money to change hands virtually, and without regulation, across the world. While local money would have to be exchanged, Bitcoin quickly and surprisingly became a standard method of payment for many online services and goods. By using specialized software to store a virtual wallet of Bitcoins, one has the ability to send or receive payments instantly to others, creating a means for instant commerce comparable to using cash.

In the years since its introduction it has become accepted and encouraged for online commerce and for shopping in select cities. Some service and restaurant industries were quick to latch onto the idea of Bitcoins to attract technologically savvy consumers, and to attract money that other businesses were not equipped to receive. In an experiment, a reporter for Forbes attempted to live solely on Bitcoin for a week in 2013 in San Francisco. While successful, there were many caveats found, such as the inability to pay to certain individuals and to large corporations.<sup>17</sup> A slow adoption rate amongst merchants was expected for a burgeoning currency, but it can be argued that Bitcoin is more relevant than other similar services. For example, Paypal is one of the largest money transfer services on the Internet but lacks a strong brick and mortar following. Through the use of a PayPal smartphone app, one can scan a QR code at a store to purchase goods, but only a small number of large-scale stores to accept such payments. In one informal study in early 2015, only a dozen national chains accepted the payment.<sup>18</sup>

At its best, Bitcoin is a system that is geared to change the way that many purchase goods and services. Its core importance was summed by the reporter Timothy Lee when he wrote that Bitcoin “allows wealth to be reduced to pure information and transmitted costlessly around the world”<sup>19</sup> The ability to transfer currency across the Internet, with verification, directly between two anonymous parties is feature that cuts the requirement for a third-party, such as Paypal or Western Union, to handle the transaction.

The true impact of Bitcoin was not noticed by regulators and governments until 2010, the year when U.S. Army Private Chelsea Manning (born Bradley Manning), leaked hundreds of thousands of classified government documents to an organization known as WikiLeaks<sup>20</sup>. As a non-profit organization designed to publish information leaked from internal sources, WikiLeaks existed long before the infamous leaks provided by Manning. However, it was this leak, which included classified international diplomatic messages that garnered a large amount of attention toward WikiLeaks. Released in a period where WikiLeaks was struggling financially,<sup>21</sup> the leak provided for a steady stream of attention, and donations, to help the organization.

As news spread about the leak of diplomatic cables, primary methods of donating money to the organization dried up. Visa Inc. suspended all payments to WikiLeaks,<sup>22</sup> while PayPal repeatedly froze WikiLeaks accounts.<sup>23</sup> Piece by piece, a virtual blockade was placed preventing the organization from receiving any money to continue operation. With careful attention, WikiLeaks was able to eventually bypass this blockade with the use of Bitcoin.

By creating a centralized Bitcoin address, WikiLeaks was able to provide a direct line of money transfer directly from senders.<sup>24</sup> Later, as form of greater anonymity, one-time use Bitcoin addresses were generated for each individual donor, masking the total amount of money being donated.

The initial visage of anonymity caused concern about abuse from terrorists and criminal groups, a concern that was noted in the public request by the US Department of Defense's Combating Terrorism Technical Support Office (CTTSO) for companies to monitor how the use of Bitcoin could be used to fund terrorism.<sup>25</sup> A CTTSO memo noted a concern that the "introduction of virtual currency will likely shape threat finance by increasing the opaqueness, transactional velocity, and overall efficiencies of terrorist attacks."<sup>26</sup> However, further research showed many of these fears are unfounded. For example, in a white paper written for the Combating Terrorism Center (CTC) at United States Military Academy at West Point, such research showed that "by analyzing the repeated use of specific public keys" investigators could "map user transactions across the network and pair them across datasets to find individual network users".<sup>27</sup>

As Bitcoin grew in popularity alternative currencies began to appear. These included services and currencies such as Litecoin and Namecoin. Over time, more fanciful currencies appeared based off Internet memes such as Dogecoin, based on a popular Internet meme of the "Doge" dog,<sup>28</sup> a currency infamous for later being sponsored onto a NASCAR vehicle.<sup>29</sup>

Additionally, the rise in popularity and common use has enticed large payment processors into supporting the use of Bitcoin. In late 2014, PayPal announced that it would be partnering with multiple Bitcoin processors to allow for peer-to-peer transactions, and eBay purchases to use Bitcoins.<sup>30</sup> Visa Inc. has made movement on allowing transitions between the Visa and Bitcoin networks and showing how its core is similar to that of Bitcoin when its CEO declared "Visa is not a currency, it's a network. We can process real or virtual currencies to the extent that it makes sense."<sup>31</sup> In a more neutral stance, the American Express network carefully considers Bitcoin as a competitor and one worth monitoring,<sup>32</sup> while MasterCard has publicly declared its distaste for the field of crypto-currency. In an interview with Channel NewsAsia, the MasterCard President of South East Asia criticizes the anonymous nature of cryptocurrency. "If it's an anonymous transaction that sounds like a suspicious transaction. Why does someone need to be anonymous?"<sup>33,34</sup>

Such a system of currency is ripe for abuse and attack. While many have tried to find loopholes in the implementation, as security researcher Dan Kaminsky found, the system was seemingly built on a secure core that was impervious to expected attacks or tampering. As Kaminsky noted, the construction of Bitcoin represents "an entirely alien design regime"<sup>35</sup> that differs from normal code development. While many applications have very clean and professional code there is always a likelihood of security vulnerabilities behind the code. Conversely, Bitcoin's frontend code appears very unprofessional and "hackish" but its core appears secure to many researchers.<sup>36</sup>

While the code and core components of crypto-currencies are currently thought to be secure against many attacks, they are weak to attacks against the coin holders. As with most technologies, the primary loss of data and money comes through human activity. The problem is compounded by the unencrypted virtual wallet files used by early versions of the Bitcoin software. Bitcoin is often compared to cash, and as such, requires the same

level of protection. In one incident in 2014 a Bitcoin entrepreneur lost nearly all of his Bitcoin cache, totaling nearly \$280,000 USD. The money was stolen while the victim was connected to a public WiFi hotspot during a vacation in Bali,<sup>37</sup> where his MacBook Pro was vulnerable to the newly discovered Shellshock exploit,<sup>38</sup> giving attackers full access to his system.

While there have been dozens of documented Bitcoin thefts performed, the majority of which are tracked on [BitCoinTalk.org](http://BitCoinTalk.org),<sup>39</sup> notable examples show the loss of Bitcoin through legal and accidental causes. In 2013, the infamous online drug market Silk Road was virtually raided by the US FBI for the seizure of Bitcoin assets of both Silk Road consumers and its owner, a 29 year old American who went by the moniker of “Dread Pirate Roberts”.<sup>40</sup>

Most notably however are the multiple attacks against the Mt. Gox service, a money exchange that handled 70% of all Bitcoin transactions by 2013.<sup>41</sup> In June of 2011, the service had 2,000 Bitcoins stolen when the account of a former administrator was compromised by an attacker.<sup>42,43</sup> In the same span of time, an SQL injection attack against Mt. Gox allowed an unknown attacker to retrieve a database of user accounts, emails, and hashed passwords from the exchange. This theft of data allowed for a secondary attack against the MyBitcoin exchange on the very next day. By exploiting users who used the same password on both services, attackers were able to exploit the weak accounts and steal thousands of Bitcoins.<sup>44</sup> While the users with shared passwords are the primary victims of such attacks, even those with secure two-factor authentication can be caught off guard. Notably, one victim who used Google two-factor authentication found himself robbed of thousands of dollars worth of Bitcoin. As his two-factor relied upon a text message containing an authentication code to be sent to his phone, an attacker who had previously gained access to his Google mail, and replaced the phone number, was able to gain access. Such access extended the attacker’s scope and allowed access to a Coinbase account containing 10 Bitcoin.<sup>45</sup>