

# Bits on Bitcoin!

Author: Jared Hall

Revision: 1.0

URL: <https://www.jaredsec.com/2017/11/01/bits-on-bitcoin>

Date: 11/01/2017

## Introduction

In the midst of the global financial crisis, a paper was anonymously authored in November of 2008. It described a peer-to-peer, distributed, electronic payment system without the oversight of a "*trusted*" central party, like a bank, PayPal, or the Federal Reserve. The paper was titled: "*Bitcoin*".

Bitcoin and other cryptocurrencies ensure that: **No bank is "too big to fail"**. It is believed that there are over 4000 cryptocurrencies active today.

Bitcoin works on an open, public, peer-to-peer network. Your transaction is announced to everyone. The announcement indicates the funds you wish to spend. The announcement is then cryptographically signed with the same key that is linked to those funds (validating that they are your funds). To prevent problems with competing announcements (the same funds spent twice), a timestamp is used to validate the transaction. This type of validation is called "*Proof of Work*". **It is incredibly important.**

To eliminate the middleman, your message is validated by a distributed process known as "*mining*". Mining is a power-hungry, CPU-intensive, cryptographic function that anybody can participate in. Miners are rewarded for their efforts by collecting a "*Block Reward*" when new Bitcoins are processed and by collecting Transaction Fees otherwise. "*Blocks*" are collections of transactions that are processed about every 10 minutes. The complexity of the cryptographic function changes to ensure that blocks are processed within this 10-minute window.

Since blocks may contain different transactions from different miners, the "*blockchain*" often "*forks*". So, after five more valid blocks are processed by the network, the monies are made available to the recipient.

- Within 10 minutes after sending money to a recipient, the network will have processed your transaction.
- It will be made available to the recipient within one hour after you submitted your transaction.

There are many sites that keep track of Bitcoin transactions and blocks. One site (Luxembourg) is: <https://blockchain.info/stats>

## NOTES:

1. **Blockchain** databases are "mined" in order to develop new blocks.

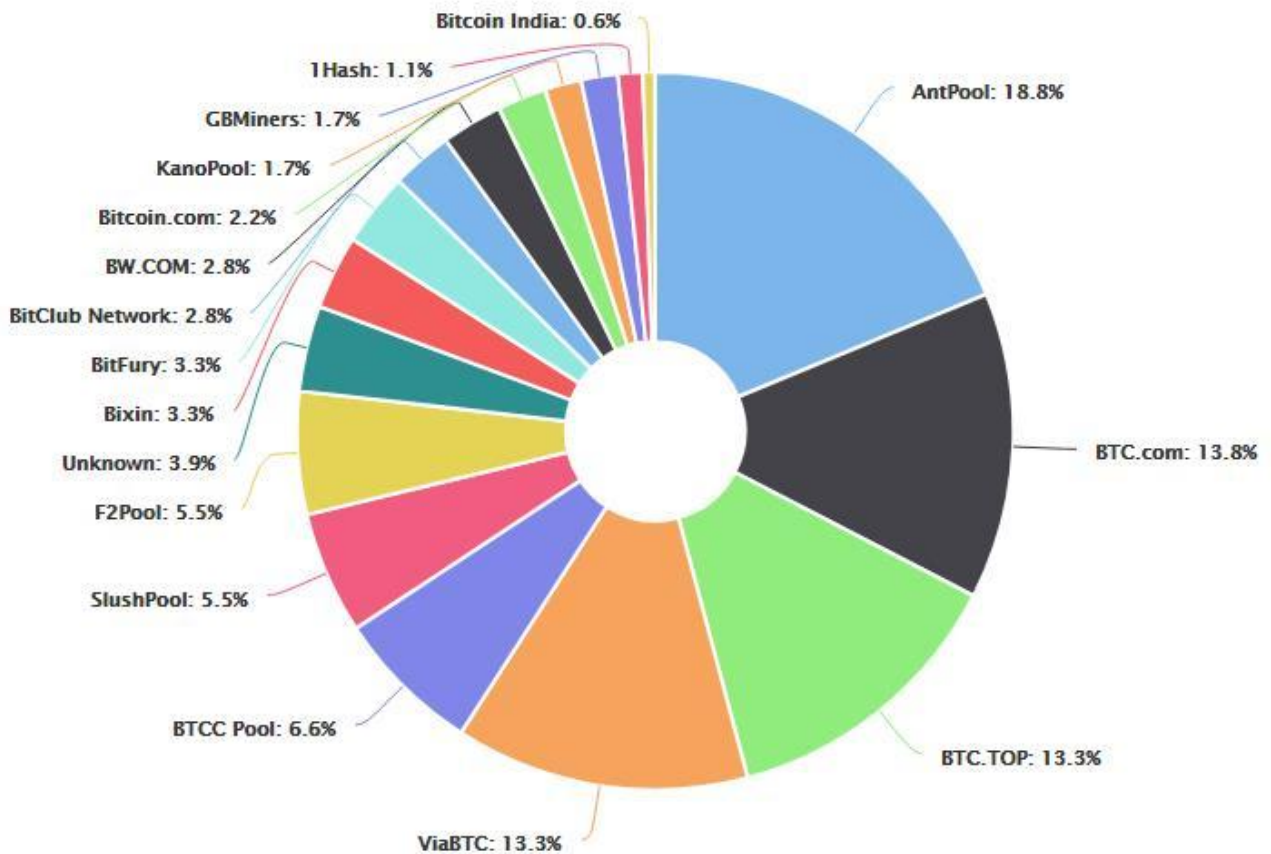
2. **Blockchain** databases **do not need** distributed miners or mining incentives. This is unique to Bitcoin's decentralized model.

### **About Mining**

When, and if, the network accepts a miner's block, the miner is rewarded in a two-fold fashion. The first is a Block Reward, which is presently 12.5 BTC. This started out at 50 BTC in 2009, then halved to 25 BTC in 2012, and halved again to 12.5 BTC in 2016. The Block Reward is actually paid, collectively, by the senders of money into the system. The block reward will stop altogether after 21 million BTC are in circulation. As you send transfer money into the Bitcoin system, it is common (but not necessary) to pay a transaction fee which is paid to the miner. This ensures that miners will continue to participate in system when all BTC are issued.

Back in the early days, a miner could exist with a standard, high-end, computer. Then processing shifted to software using high-end video cards, then specially-built ASIC cards. Over the last five years, Bitcoin's blockchain difficulty has increased by 350,000 times. Nowadays, a computer with a \$2000 ASIC (Application Specific Integrated Circuit) board would only represent about 0.001% of the network's mining power. The odds of getting a return on your investment are pretty small.

Successful Bitcoin mining costs money. You need a lot of computational horsepower to continually process and crank out encrypted blocks. That means that you're generating a lot of heat, and voraciously consuming electricity. An individual can buy mining hardware and join a pool; a collective whose revenues are shared between the members.



These days, about fifteen companies control most of Bitcoin's hashing power. China, which has the world's cheapest electrical power, is the dominant leader ("exporter") of newly minted BTC. In fact, **China mines about 60% of all Bitcoins, an obvious concern to many Bitcoin participants.** Being so dependent upon electricity, the top Bitcoin producers ("exporters") are, in order:

- China - 60%
- Georgia - 15%
- Sweden - 7.5%
- United States - 3%

For those with an interest in Bitcoin mining, here are some useful links:

- <http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/>
- <https://www.buybitcoinworldwide.com/mining/pools/>

### Alternative Cryptocurrencies

I think of Bitcoin being the "Genesis Coin"; the first of its kind. But in a blockchain database with multiple miners, block corruption can occur if a single miner has 51% of the mining power.

**If China nationalized the three biggest miners, this would represent a threat to Bitcoin.** If a single mining entity has a 51% share, then the blockchain can become corrupt.

Not all cryptocurrencies have the same administrative rules. For example, in Bitcoin, the "miners" have the authority to approve policy changes. There are a number of alternative cryptocurrencies available; each having slightly different rules of implementation. The majority of Bitcoin users favor "Miner Registration" policies, but approval of this policy has been thwarted by Chinese miners.

- Litecoin (LTC)
- Ethereum (ETH)
- Zcash/Darkcoin (ZEC)
- Ripple (XRP)
- Monero (XMR)
- Dogecoin (DOGE)

Litecoin came out shortly after Bitcoin and is the second largest cryptocurrency. Ethereum is intended to support software objects like *Smart Contracts* and *Distributed Applications* but they have their own monetary unit called "Ether".

Ripple uses a "*Concensus Ledger*" to provide a real-time global settlement network (Bitcoin would be like a "Near Real-Time" global payment network). XRP is gaining traction in the banking industry due to its low operating costs.

Zcash and Monero provide enhanced security and anonymity over Bitcoin.

Bitcoin's payment system supports two types of "*Contracts*". Addresses formats for these types are:

- **Pay-to-Public-Key-Hash** (P2PKH) addresses are 26-35 alphanumeric characters, beginning with the number 1. **This is the most common address.** You can get one online at any time and own multiple addresses. Bitcoin wallets will normally generate one for you. This address is a Base58-derivative of: RIPEMD160(SHA256(ECDSA\_publicKey)) where the *ECDSA\_publicKey* is a public key your wallet knows the private key for.
- **Pay-to-Script-Hash** (P2SH) addresses are 26-35 alphanumeric characters. These addresses all begin with the number 3. This address is a Base58-derivative of: RIPEMD160(SHA256(redeemScript)) where the *redeemScript* is a script the wallet knows how to spend

## **Privacy and Security**

**It is a myth that Bitcoin transactions are totally anonymous.** Blocks and the transactions therein **are visible**. The payment type and amounts associated with a transaction are also visible to anybody. You can view Bitcoin blocks at many sites, but here's a good URL:

<https://www.blockchain.info/blocks>. You will see a sequential listing of blocks. If you pick a block, and click on the "hash", you will see the individual transactions therein. Here's a listing of Block #491236:

3cb1c0b37545f6cc753e3dc2d324d5cb84739cebfb926aa293212b724865c93		2017-10-23 10:09:23										
1H6ZZpRmMnrw8ytepV3BYwMjYnEKWDqVP	→	<table border="0"> <tr> <td>18tZJVshW7Ui4mFTUVS81KgApniJvEB4t9</td> <td>0.0161 BTC</td> </tr> <tr> <td>1ECDkRMZk2rzwMdxMm8e8gKSa47QQd21Vw</td> <td>0.1123 BTC</td> </tr> <tr> <td>378auEeLLMP8btgWPoyP6nwSVZgL4VEhEp</td> <td>2.6583 BTC</td> </tr> <tr> <td>1LfxTGDfmQh1WMGRjachya1XCqoJ5kF4Mt</td> <td>0.0495 BTC</td> </tr> <tr> <td>1H6ZZpRmMnrw8ytepV3BYwMjYnEKWDqVP</td> <td>86.3563598 BTC</td> </tr> </table>	18tZJVshW7Ui4mFTUVS81KgApniJvEB4t9	0.0161 BTC	1ECDkRMZk2rzwMdxMm8e8gKSa47QQd21Vw	0.1123 BTC	378auEeLLMP8btgWPoyP6nwSVZgL4VEhEp	2.6583 BTC	1LfxTGDfmQh1WMGRjachya1XCqoJ5kF4Mt	0.0495 BTC	1H6ZZpRmMnrw8ytepV3BYwMjYnEKWDqVP	86.3563598 BTC
18tZJVshW7Ui4mFTUVS81KgApniJvEB4t9	0.0161 BTC											
1ECDkRMZk2rzwMdxMm8e8gKSa47QQd21Vw	0.1123 BTC											
378auEeLLMP8btgWPoyP6nwSVZgL4VEhEp	2.6583 BTC											
1LfxTGDfmQh1WMGRjachya1XCqoJ5kF4Mt	0.0495 BTC											
1H6ZZpRmMnrw8ytepV3BYwMjYnEKWDqVP	86.3563598 BTC											
		89.1925598 BTC										

## Transactions

aef7eb514d46e137ba1b49b743a1c035012f72e0ab87563c5036776323d2abca		2017-10-23 02:17:44				
No Inputs (Newly Generated Coins)	→	<table border="0"> <tr> <td>1PuTM8tUE6u8JLuZ4Yd6mFZ9qjBRsy79W</td> <td>12.5546147 BTC</td> </tr> <tr> <td>Unable to decode output address</td> <td>0 BTC</td> </tr> </table>	1PuTM8tUE6u8JLuZ4Yd6mFZ9qjBRsy79W	12.5546147 BTC	Unable to decode output address	0 BTC
1PuTM8tUE6u8JLuZ4Yd6mFZ9qjBRsy79W	12.5546147 BTC					
Unable to decode output address	0 BTC					
		12.5546147 BTC				

57f60e656a22ee85328e26cf9ed37f2d6dbc15c6eb23072769c673bca8ab75c		2017-10-23 02:17:24											
<table border="0"> <tr> <td>3NqWR1u9eyMrmV1HmZAhLK17SgSMTksSq1</td> <td rowspan="4">→</td> <td rowspan="4"> <table border="0"> <tr> <td>1H4LvJR8K5ciGyqQdFYQt8Rk2dtfH7Led</td> <td>2.999 BTC</td> </tr> <tr> <td>37wuWR8XxQhwvvy2X2SNT83un2DEFMIHuW</td> <td>0.01000005 BTC</td> </tr> </table> </td> </tr> <tr> <td>3KiRKJGPRjpH2xLr5YbxPR8XAFTSSXqkq</td> </tr> <tr> <td>3KdEeSKAQpLJCab85ay31VhtWxRnKqGt3V</td> </tr> <tr> <td>3J2CIXvL8kNXiavqkVUDUhrNe6xgvQ32pX</td> <td></td> </tr> </table>	3NqWR1u9eyMrmV1HmZAhLK17SgSMTksSq1	→	<table border="0"> <tr> <td>1H4LvJR8K5ciGyqQdFYQt8Rk2dtfH7Led</td> <td>2.999 BTC</td> </tr> <tr> <td>37wuWR8XxQhwvvy2X2SNT83un2DEFMIHuW</td> <td>0.01000005 BTC</td> </tr> </table>	1H4LvJR8K5ciGyqQdFYQt8Rk2dtfH7Led	2.999 BTC	37wuWR8XxQhwvvy2X2SNT83un2DEFMIHuW	0.01000005 BTC	3KiRKJGPRjpH2xLr5YbxPR8XAFTSSXqkq	3KdEeSKAQpLJCab85ay31VhtWxRnKqGt3V	3J2CIXvL8kNXiavqkVUDUhrNe6xgvQ32pX			
3NqWR1u9eyMrmV1HmZAhLK17SgSMTksSq1	→			<table border="0"> <tr> <td>1H4LvJR8K5ciGyqQdFYQt8Rk2dtfH7Led</td> <td>2.999 BTC</td> </tr> <tr> <td>37wuWR8XxQhwvvy2X2SNT83un2DEFMIHuW</td> <td>0.01000005 BTC</td> </tr> </table>	1H4LvJR8K5ciGyqQdFYQt8Rk2dtfH7Led	2.999 BTC	37wuWR8XxQhwvvy2X2SNT83un2DEFMIHuW	0.01000005 BTC					
1H4LvJR8K5ciGyqQdFYQt8Rk2dtfH7Led					2.999 BTC								
37wuWR8XxQhwvvy2X2SNT83un2DEFMIHuW					0.01000005 BTC								
3KiRKJGPRjpH2xLr5YbxPR8XAFTSSXqkq													
3KdEeSKAQpLJCab85ay31VhtWxRnKqGt3V													
3J2CIXvL8kNXiavqkVUDUhrNe6xgvQ32pX													
		3.00900005 BTC											

In this block, the first transaction is a block reward sent to the miner of Block #491235. The miner's "**Block Reward**" is always the first transaction of the next block. In the next transaction, monies from four Pay-to-Script-Hash addresses are sent to two other accounts. So, you can see the Bitcoin Addresses (Account Information), but **no other personal identifying information**.

The following transaction was snipped from Block #491297:



3cb1c0b37545f6cc753e3dc2d324d5cb84739cebfb926aa293212b724865c93		2017-10-23 10:09:23										
1H6ZZpRmMnrw8ytepV3BYwMjYnEKWDqVP	→	<table border="0"> <tr> <td>18tZJVshW7Ui4mFTUVS81KgApniJvEB4t9</td> <td>0.0161 BTC</td> </tr> <tr> <td>1ECDkRMZk2rzwMdxMm8e8gKSa47QQd21Vw</td> <td>0.1123 BTC</td> </tr> <tr> <td>378auEeLLMP8btgWPoyP6nwSVZgL4VEhEp</td> <td>2.6583 BTC</td> </tr> <tr> <td>1LfxTGDfmQh1WMGRjachya1XCqoJ5kF4Mt</td> <td>0.0495 BTC</td> </tr> <tr> <td>1H6ZZpRmMnrw8ytepV3BYwMjYnEKWDqVP</td> <td>86.3563598 BTC</td> </tr> </table>	18tZJVshW7Ui4mFTUVS81KgApniJvEB4t9	0.0161 BTC	1ECDkRMZk2rzwMdxMm8e8gKSa47QQd21Vw	0.1123 BTC	378auEeLLMP8btgWPoyP6nwSVZgL4VEhEp	2.6583 BTC	1LfxTGDfmQh1WMGRjachya1XCqoJ5kF4Mt	0.0495 BTC	1H6ZZpRmMnrw8ytepV3BYwMjYnEKWDqVP	86.3563598 BTC
18tZJVshW7Ui4mFTUVS81KgApniJvEB4t9	0.0161 BTC											
1ECDkRMZk2rzwMdxMm8e8gKSa47QQd21Vw	0.1123 BTC											
378auEeLLMP8btgWPoyP6nwSVZgL4VEhEp	2.6583 BTC											
1LfxTGDfmQh1WMGRjachya1XCqoJ5kF4Mt	0.0495 BTC											
1H6ZZpRmMnrw8ytepV3BYwMjYnEKWDqVP	86.3563598 BTC											
		89.1925598 BTC										

What's interesting about this transaction is that you see that the sender's address is also listed as the last one in the group of recipients. This is actually the "**Change**" returned from the account's balance. Yes, even that is a transaction unto itself. You can also see that this was sent from an individual Pay-to-Public-Key-Hash account to three other Pay-to-Public-Key-Hash accounts and one Pay-to-Script-Hash. Hopefully, this will give you an idea on how the system works.

Now, here's where privacy comes into play. I can click on that sender's Address/Account Number and view the current balance and all transactions associated with that address:

## Bitcoin Address

Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	1H6ZZpRmMnrw8ytepV3BYwMjYnEkWDqVP	No. Transactions	29194 
Hash 160	b08f46e4d21cd0547a8a1e2e43e5440284f710a4	Total Received	170,357.10645309 BTC 
Tools	<a href="#">Related Tags</a> - <a href="#">Unspent Outputs</a>	Final Balance	200.5262598 BTC 

[Request Payment](#) [Donation Button](#)



Holy guacamole! There's 200 bitcoins in there! There's 584 pages of activity, going back to December 2014. It comes complete with a QR code to make it easy to send money to, or request money from, that particular account. Hmm. I'm not too proud to beg.

This last example underscores the **difference between security and privacy**. Yes, the transaction was secure. Nobody can use that account to send money unless they know the private key associated with it. This is usually setup when you install your wallet. But anybody can see what is going on with the account.

In the interest of **privacy**, it would not be a good idea for this account number/QR code to be pasted on a website where there might be an association with personal identifying information. Naturally, there are sites that keep track of the *\*richest\** Bitcoin addresses: <https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html>

**Bitcoin is commonly used to pay remote employees and contractors in foreign countries.** These days, transactions over 1 million dollars (US) are quite common.

### A Blockchain Primer

A *Blockchain* is a type of immutable database. That is to say that once a record block has been entered, it cannot be changed without invalidating all subsequent blocks. **Accountants love Blockchain.**

What makes Blockchain immutable is the use of cryptographic signing of each block. Of course the term "immutable", like redundancy, is not perfect, but the math behind blockchain is the best thing we've got.

A blockchain database always starts with Record/Block #0, called the "*Genesis Block*". Here's a nice web page with a sample javascript command-line interface that creates and mines a sample blockchain: <https://medium.freecodecamp.org/how-does-blockchain-really-work-i-built-an-app-to-show-you-6b70cd4caf7d>

In the sample implementation, the Genesis Block looks like this:

🏆 Genesis Block	
⏪ Previous Hash	0
📅 Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
📄 Data	Welcome to Blockchain CLI!
🔥 Hash	0000018035a828da0...
🔨 Nonce	56551

Blockchain databases have a concept of "difficulty". This is usually the number of leading zeroes in the hash of new blocks.

Subsequent blocks are added with a Secure Hash Algorithm like this:  
SHA256(index + previousHash + timestamp + data + nonce)

The "nonce" value starts at 0 and increments until the desired difficulty is met (leads with 4 zeros). This is a lot of CPU-work to calculate these hashes. The more zeroes needed (higher difficulty), the more CPU horsepower needed.

Here's what Bitcoin's *Genesis Block* looks like:

# Block #0

Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893
Block Reward	50 BTC

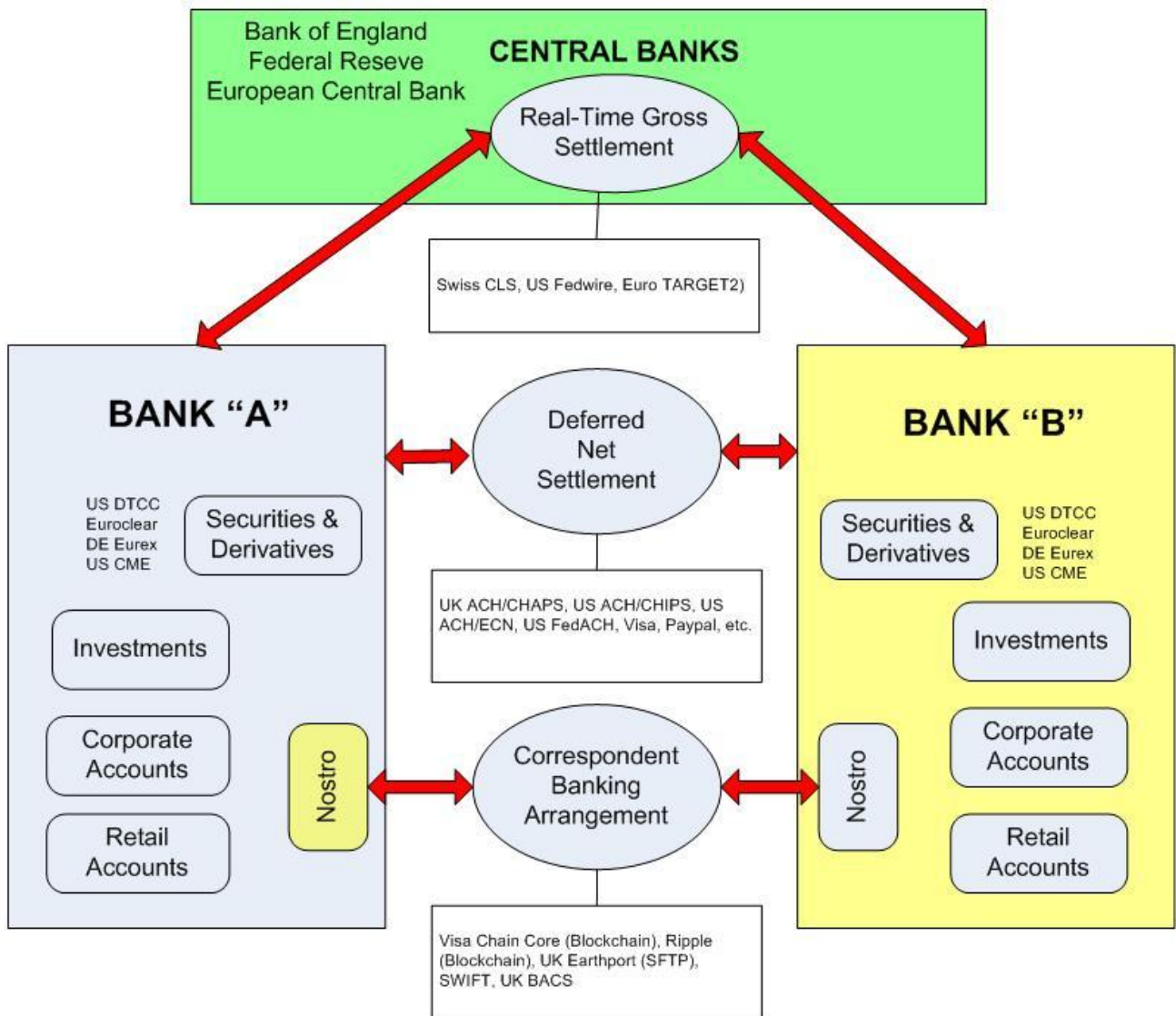
At the time of this writing, here is the current Bitcoin block:





## Banking Networks

The following diagram depicts typical Western banking topology and the types of networks used between banks.



**Correspondent Banking** is the simplest of arrangements between banks. It usually involves *Nostro/Vostro* accounts. *Nostro* means "our, as in "our money that is on deposit at your bank." *Vostro* means "your", as in "your money on deposit at our bank". Messages are interchanged between banks to the credit and debit of accounts. The SWIFT (Society for Worldwide Interbank Financial Telecommunication) network is the dominant entity here although it is facing heavy competition now from Blockchain systems, such as Visa's B2B-Connect "Chain Core" network and Ripple. Deposits are held in the currency of the holder of the Nostro account. There is risk in terms of the amount of money transferred and the relative size between banks (counterparty risk), so many systems will broker the transfer through the Central Bank system. This is especially true when transferring money between banks in different countries.

If banks do a lot of business with each other, a **Deferred Settlement Network** is preferred. Here, everything between the two banks is tallied up at the end of the day and the appropriate accounts debited or credited. Credit Card Merchant networks, Check Processing and PayPal are all examples of these types of networks. Again, a Central Bank will be used when the amounts are large or the banking entities are in different countries.

Finally, Central Banks provide a means to achieve both settlement finality and zero counterparty risk. They offer networks that do **Real-Time Gross Settlement**. There are no reversals (settlement) and there is no "netting" (otherwise it wouldn't be "*real-time*"). But there is a serious problem with Central Bank RTGS networks; **they are anything but real-time**. Anybody that has transferred funds to/from international entities knows to expect delays; around one day (at best). This is because of government intervention. In the US, for instance, the Treasury Department and Homeland Security are going to want to take a peek at what's going on.

Bitcoin represents a **Near-Real-Time Gross Settlement** network.

### **About Currency**

The fact is that most countries' currencies are "*fiat*", meaning that they are backed by nothing. A quote at [New Economic Perspectives](#) correctly asserts that "Money is nomos (custom, law, norm, rule), not physis (nature). The entity designated as money is just the embodiment of a social relationship, a relationship that can change because of an act of will or common agreement or by chance."

What makes the US dollar viable for trade is also answered therein: "Because there are 300 million Americans throwing a \$14T dollar denominated party every year and a dollar represents a piece of that action." That was a post written in 2011. It's a little more than that now. So the value of a dollar represents this country's collective GDP with the "common agreement" of law.

Consider the "shell-based" currency of the Solomon Islands. For **10 thousand years**, women have collected a certain type of shell, and then grind them into beads to form tradeable currency. They only produce as much currency as they need and the relative value is set by the **amount of work** needed to produce it. Ask yourself a question. What makes gold or diamonds, or any other substance valuable? It's not that they are rare metals. It's because of the **amount of work** needed to acquire them.

For a currency to remain viable, it must have trade value. The US Dollar is the legal tender of the United States and enforced, ironically, through the Internal Revenue Service and spending by the government itself. Disputed acceptance is fought in International courts, or war.

Cryptocurrencies, like Bitcoin or Litecoin, are no different. Overall viability is determined by their acceptance worldwide, while value is determined by both the amount of currency converted to them and the overall **amount of work** performed by the miners.

Here's a listing of the most popular currencies in play today.

Rank	Currency	ISO 4217 code (symbol)	% daily share (April 2016)
1	 United States dollar	USD (\$)	80.6%
2	 Euro	EUR (€)	37.4%
3	 Japanese yen	JPY (¥)	21.6%
4	 Pound sterling	GBP (£)	12.8%
5	 Australian dollar	AUD (A\$)	6.9%
6	 Canadian dollar	CAD (C\$)	5.1%
7	 Swiss franc	CHF (Fr)	4.8%
8	 Renminbi	CNY (¥)	4.0%
9	 Swedish krona	SEK (kr)	2.2%
10	 New Zealand dollar	NZD (NZ\$)	2.1%

All currencies today are *fiat* currencies. Of interest is that fact that the "*Five Eyes*" countries are all well represented on this list. **The use of fiat currencies is controversial.** Since fiat currencies can be somewhat arbitrary, the International Monetary Fund, headquartered in Washington DC, meets every five years to adjust currency valuation based upon a basket of five currencies. These five "Reserve Currencies" are known as "*hard currencies*". These are:

1. U.S. dollar 41.73%
2. Euro 30.93%
3. Renminbi (Chinese yuan) 10.92%
4. Japanese yen 8.33%
5. British pound 8.09%.

Regarding global standards, the US Dollar continues to be the preferred currency exchanged between Central Banks. The US terminated the convertibility of the dollar to gold in 1971, under President Nixon. Other currencies, which were loosely based upon gold became floating at that time.

Russia has been buying gold at a furious rate since 2009, followed by the Chinese, in hopes to develop alternative trade currency. The US Federal Reserve, in a type of economic detente, followed suit. In 2014, Russian and China did establish a private line-of-credit to accommodate unfettered trade between them.

Russia is also pursuing the development of a national cryptocurrency, nicknamed the "CryptoRuble".

### **Of US Banking and Bitcoin**

Jamie Dimon of JP Morgan has been an outspoken critic of Bitcoin, and some of his quotes were republished in the magazine, "American Banker". It did not go well for him. Here is one cryptonerd's critique: <https://blog.chain.com/a-letter-to-jamie-dimon-de89d417cb80>. I can easily see and understand Jamie Dimon's position. I can also see why sometimes *a company's CEO shouldn't be the Chairman*.

1)	•DIMON: THIS IS THE LAST TIME I TALK ABOUT BITCOIN	BN	13:30
2)	•DIMON: BITCOIN IS 'A GREAT PRODUCT' IF YOU ARE A CRIMINAL	BN	13:30
3)	•DIMON: GOVERNMENTS LIKE TO CONTROL THEIR ECONOMIES, CURRENCIES	BN	13:29
4)	•DIMON: GOVERNMENTS ARE GOING TO CRUSH BITCOIN ONE DAY	BN	13:29
5)	•DIMON: "WHO CARES ABOUT BITCOIN?"	BN	13:29
6)	•DIMON: PEOPLE WHO PURCHASE BITCOIN ARE STUPID	BN	13:28
7)	•DIMON: I DON'T UNDERSTAND THE VALUE OF SOMETHING WITHOUT VALUE	BN	13:28
8)	•DIMON: I COULD CARE LESS ABOUT BITCOIN	BN	13:27

### **I COULD CARE LESS ABOUT BITCOIN**

Well, that's a personal opinion. I respect his opinion, and even understand it. Still, he is the CEO of JP Morgan and he shouldn't have said it. Bitcoin doesn't provide much value to they typical bank.

### **I DON'T UNDERSTAND THE VALUE OF SOMETHING WITHOUT VALUE**

Like the Dollar, or any other fiat currency? Is a Rembrandt just \$2.00 of canvas and paint? That's just a foolish thing to say. A better thing for him to have said would be, "*I don't understand the value of something without protection and enforcement.*"

### **PEOPLE WHO PURCHASE BITCOIN ARE STUPID**

Well, that's just insulting. I know JP Morgan clients who've purchased Bitcoin. Jamie's own daughter has purchased Bitcoin. Again, he's more than a stuffed-shirt with an opinion. He's representing JP Morgan.

### **WHO CARES ABOUT BITCOIN?**

People and companies that want to transfer money internationally without delay, primarily. I'd venture to say that if Jamie's own daughter was ever erroneously locked-up abroad, he'd care about Bitcoin. Of course, he could always wait for that wire transfer to go through.

### **GOVERNMENTS ARE GOING TO CRUSH BITCOIN ON DAY**

Right now, Bitcoin is not a threat to any government. Even with all BTC issued, it will not be a threat. But Jamie is most certainly right. **Governments will probably replace it with their own cryptocurrency.**

### **GOVERNMENTS LIKE TO CONTROL THEIR ECONOMIES, CURRENCIES**

Yes, they do. That's why nobody uses the *Gold Standard* anymore. In some countries Bitcoin is illegal:

- Russia
- China (Banks and financial institutions. Personal use is OK)
- Bolivia

- Kyrgyzstan
- Ecuador
- Vietnam
- Iceland

### **BITCOIN IS 'A GREAT PRODUCT' IF YOU ARE A CRIMINAL**

Like cold, hard cash? **Bitcoin isn't totally anonymous** and hackers are likely to move on to Monero for their ransoms. Geez, back in the DOS days you had to get your data back with a Credit Card. Then it became an address for you to ship your trashed hard drive to with a wad of cash. Then it became payment with Walmart Gift Cards. On this point, Jamie comes off as ignorant.

### **THIS IS THE LAST TIME I TALK ABOUT BITCOIN**

For Jamie, this would be a good thing right now. As Chairman, he can express things in any way he wants. As CEO, he probably hasn't fairly represented JP Morgan.

A bank has three basic purposes:

1. Act as a secure place for your money.
2. Issues certificates of debt (loans).
3. Acts as an investment vehicle for itself, and possibly it's clients.

To that end, Bitcoin competes slightly with banks with regard to being a secure place for your money. PayPal is no different, and banks don't like PayPal either.

### **Bitcoin is not a debt vehicle.**

As for investment, like any Foreign Exchange market, **Bitcoin is risky**. Anyone that follows Bitcoin sees the volatility. Banks have enough trouble with their *Nostro* accounts as they have to constantly monitor exchange rates and deal with Capital Gains and Losses.

Here's a tip for reporters: *If you want to solicit opinions about currency and cryptocurrencies, don't seek out an investment banker.*

### **Getting Started With Bitcoin**

The fundamental components of Bitcoin, and other cryptocurrencies, are similar to those in traditional monetary systems:

#### **Exchanges**

These are locations where you can interchange large amounts of domestic and cryptocurrencies. They usually will give you a wallet for your currency and provide funds transfer to and from your regular bank; like PayPal does.

- Some Exchanges will allow you to purchase cryptocurrency with a credit card.
- Some Exchanges will accept Direct Deposit.

- Most exchanges have transaction fees but have no deposit or withdrawal fees.
- Different exchanges support different cryptocurrencies.

There are a lot of fraudulent exchanges out there, so try to stay with the larger, popular ones. In the US, some of these include:

Coinbase (San Francisco, CA): <https://www.coinbase.com>

Kraken (San Francisco, CA): <https://www.kraken.com>

Gemini (New York, NY): <https://gemini.com>

For the neophyte, I recommend Coinbase. They offer some financial protections and support the "*big three*" cryptocurrencies, Bitcoin (BTC), Litecoin (LTC), and Ethereum (ETH). Not all states will allow the operation of cryptocurrency exchanges and most require some type of financial disclosure to their residents. Here's the warning message displayed by Coinbase when setting up a new account:

## NOTICE: By the Florida Office of Financial Regulation

---

BY GRANTING COINBASE A LICENSE, THE FLORIDA OFFICE OF FINANCIAL REGULATION IS NOT ENDORSING THE USE OF DIGITAL OR VIRTUAL CURRENCIES.

- U.S. currency is legal tender backed by the U.S. government.
- Digital and virtual currencies are not issued or backed by the U.S. government, or related in any way to U.S. currency, and have fewer regulatory protections.
- The value of digital and virtual currencies is derived from supply and demand in the global marketplace which can rise or fall independently of any fiat (government) currency.
- Holding digital and virtual currencies carries exchange rate and other types of risk.

POTENTIAL USERS OF DIGITAL OR VIRTUAL CURRENCIES, INCLUDING BUT NOT LIMITED TO BITCOIN, SHOULD BE FOREWARNED OF A POSSIBLE FINANCIAL LOSS AT THE TIME THAT SUCH CURRENCIES ARE EXCHANGED FOR FIAT CURRENCY DUE TO AN UNFAVORABLE EXCHANGE RATE. A FAVORABLE EXCHANGE RATE AT THE TIME OF EXCHANGE CAN RESULT IN A TAX LIABILITY. PLEASE CONSULT YOUR TAX ADVISOR REGARDING ANY TAX CONSEQUENCES ASSOCIATED WITH YOUR HOLDING OR USE OF DIGITAL OR VIRTUAL CURRENCIES.

## **ATM Machines**

Bitcoin ATMs provide a fast, mobile-friendly way to put money into, or take money out of, your Bitcoin wallet. The following details the countries with the largest amount of ATM machines:

- United States (1073 locations)
- Canada (271 locations)
- United Kingdom (90 locations)
- Austria (78 locations)
- Spain (36 locations)
- Switzerland (22 locations)
- Finland (22 locations)
- Czech Republic (21 locations)
- Australia (20 locations)
- Japan (16 locations)

You would figure that deployment of Bitcoin ATM with individual states in the US would correlate to the state's population count. That is not the case. Here are the states with the most amount of cryptocurrency ATMs:

- California, CA: 192
- Florida, FL: 119
- New York, NY: 117
- Illinois, IL: 108
- Georgia, GA: 90
- Texas, TX: 66
- New Jersey: 55
- Michigan: 44
- Washington, DC: 44
- Pennsylvania: 34

A useful website for finding nearby cryptocurrency ATMs is: <https://coinatmradar.com/>.

- Bitcoin ATM exchange rates vary between systems.
- The cryptocurrency support between ATMs vary.
- ATMs are In (Deposit), Out (Withdrawal), or both.
- For convenience and ease-of-use, many ATM providers have mobile app cryptowallets that make ATM use easy.

## **Wallet**

The wallet is your digital address for your funds. Your wallet is driven by your Bitcoin address which is a Base58-encoded string: RIPEMD160(SHA256(ECDSA\_publicKey)). The most common wallet is a "software wallet", held in your Exchange or mobile device. The "hardware wallet" is a USB-device that you may carry about with you on your person.



### **Mixers**

Mixers are sites that allow aggregate pooling of cryptocurrency. You can put money from your wallet into a mixer, and then transfer it from the mixer to another wallet.

Mixers don't seem to last long these days as their primary purpose is money-laundering. **You should avoid using Mixers.**

### **Currency Converters**

As I mentioned earlier, it is likely that ransomware miscreants will migrate from *Bitcoin*, *Litecoin*, and *Ethereum* payments to something even more untraceable, like *Monero*. Currency converters provide a way to convert between cryptocurrencies.

You will still need a wallet that can handle the cryptocurrency that you are **converting to**.

### **Don't Forget About Taxes**

Bitcoin and other cryptocurrency is treated the same as any other Foreign Exchange market. Holdings in Foreign Exchange currency markets must be reported, particularly if any amount held or traded exceeds \$10,000 USD. In addition, **all** Capital Gains or Losses must be reported.

If you run a business that has done any dealings with cryptocurrencies, there may be other IRS rules that apply.

I am not a tax expert. I recommend that anyone that uses cryptocurrency markets **consult a professional accountant or tax firm**. If you happen to be in the Tampa Bay, FL or Buffalo, NY metropolitan areas and seek such a professional firm, I'll be happy to refer you to one.