

Cryptofinance^{*}

Campbell R. Harvey

*Fuqua School of Business, Duke University, Durham, NC 27708 USA
National Bureau of Economic Research, Cambridge, MA 01234 USA*

First posted to SSRN: May 17, 2014

Cryptography is about communication in the presence of an adversary. Cryptofinance is the efficient exchange of ownership, the verification of ownership, as well as the ability to algorithmically design conditional contracts, all with security, privacy, and minimal trust without using centralized institutions. Our current financial system is ripe for disruption. At a swipe of a debit or credit card, we are at risk (think of Target's breach of 40 million cards). The cost of transacting using traditional methods is enormous and will increase in the future. Cryptofinance offers some solutions. This paper explores the mechanics of cryptofinance and a number of applications including bitcoin. Also attached is a slide deck that I use in my graduate course.

Keywords:

Cryptofinance, Bitcoin, Bubbles, Block chain, Blockchain, Cryptography, Mining, Proof of Work, Hash, Deflation, Nonce, SHA-256, Merkle tree, DSA, Private Key, Public Key, Key Pair, Wallet, BTC, Satoshi Nakamoto

JEL: A10, C00, D00, E00, F00, G00, H00, I00, J00, K00, L00, M00, N00, O1, P00, Q00, R00, Z00

^{*} Current version: January 14, 2016. I appreciate the many conversations with Matt Corallo, Ian Dew-Becker and Jameson Lopp. I have no financial interest in any venture related to bitcoin. I own one bitcoin which I purchased for teaching purposes.

"The world is not short of currencies, so what is this currency solving for?"

Ajay Banga, CEO Mastercard, February 17, 2014

Introduction

Cryptography is the science of communication in the presence of an adversary. The adversary can intercept, delay, block, or potentially alter the communication. This field encompasses encryption, decryption, authentication, and the distribution of keys. Cryptofinance is the efficient exchange of ownership, the verification of ownership, as well as the ability to algorithmically design conditional contracts, all with security, privacy and minimal trust without using centralized institutions.

Our current financial system is ripe for disruption. At a swipe of a debit or credit card, we are at risk (think of Target's breach of 40 million cards). The cost of transacting using traditional methods is enormous and it will increase. Cryptofinance offers some potential solutions. This paper explores the mechanics of cryptofinance and a number of applications. I analyze both the potential benefits as well as the risks.

In the 1980s, David Chaum¹ first proposed the idea of a cryptographically secure method of payment that would ensure privacy. In 1990, he launched DigiCash. The innovation was described at the time by futurist Nicholas Negroponte as "the most exciting product I have seen in the past 20 years". However, DigiCash and its successor, Ecash, failed. Thirty years later there is a flurry of new crypto-currencies with Bitcoin being the market leader. Are these crypto-currencies headed towards the same fate?

My paper will attempt to analyze both the pros and the cons of this innovation. Much of the focus is on bitcoin because it is the first mover in this second wave of innovation. However, it is important to realize that bitcoin might be a stepping stone to the future – not the future.

Bitcoin offers a way to exchange ownership on a peer to peer basis that substantially reduces transactions costs, eliminates fraud, ensures privacy, is largely unhackable (strong claim, but read on), is decentralized so anyone on the network can verify that a party has the bitcoin to spend, and is not subject whims and machinations of any central bank's monetary policy. In addition, bitcoin may offer something different than a usual currency; there is potential value of having a network that serves as a secure repository for the common knowledge of all transactions. On the negative side, there are significant concerns regarding this innovation being used for money laundering, there is regulatory risk, it is not so obvious that privacy can be maintained in the future, there is third party risk (think of Mt. Gox), there is no insurance, and it may be possible to hack the network if enough computing power is harnessed. In addition, value of bitcoin fluctuates so wildly that it may be too risky to serve as a credible store of value (historically, bitcoin has been seven times more volatile than investing in the stock market).

There is one thing that everyone agrees on -- the debate about crypto-currencies is hampered by a lack of understanding of the mechanics. Before having a discussion about the economics, it is necessary to understand how crypto-currencies work. This is where my paper starts.

¹ See Chaum (1982, 1985) and Chaum, Fiat and Naor (1990).

The mechanics

Debit Cards and Cash

Bitcoin was first proposed in a white paper written under the pseudonym of Satoshi Nakamoto in 2008. This paper describes a peer-to-peer method to exchange electronic cash. Usually, when we transact, there is a central clearing place, like a bank. When I use my debit card, my bank is the middle party. Bitcoin better resembles cash. When go to a retailer to pay for something, I check to see if I have the cash and then I pay the retailer directly.

When I use my debit card, there are risks. Someone can steal my debit card. The retailer may be hacked and my debit card information could be stolen. In this case, my bank assumes all of the costs associated with fraud. Even if my children run up unauthorized Internet purchases on my debit card, the bank covers all the charge backs. This greatly increases the cost of transacting.

Using bitcoin for a transaction is similar to cash with a few important differences. When I go to the retailer intending to transact in cash, I usually need to withdraw cash from a bank. The bank provides a central place to keep my cash safe and delivers the withdrawal technology, such as an ATM. The bank provides insurance if cash is withdrawn with a stolen debit card – and if the bank is robbed. The government also provides some insurance in regulating the amount of risk that banks can take and providing deposit insurance for my account.

There are also other issues with cash. It is possible to counterfeit currency. Also, while cash is unique (there are serial numbers on each, for example, U.S. Federal Reserve Note), it is not feasible to track of the serial numbers of each transaction. In addition, the paper money needs to be recycled every three or four years – so even if the serial numbers were tracked, they would provide a very short record. Finally, a government can indirectly tax citizens by printing currency and creating inflation.

Bitcoin

In contrast to the usual concept of currency, the history of every bitcoin is known. Think of a giant ledger existing in cyberspace. When I go to the retailer to pay for an item and use a bitcoin, the ledger can precisely determine whether I have the coin to spend. My transaction is then verified.

This giant ledger is called the blockchain in crypto-currency parlance. It represents the history of all transactions. It is called blockchain because blocks of new transactions are being added to the chain as new transactions happen. Think of it as a giant diamond necklace with new diamonds being added. Currently, a new block is added every 10 minutes.

There are two important features of this giant ledger. First, it is easy to look into the block chain and verify that I have the bitcoin to spend at a restaurant. Anyone connected on the Bitcoin network can do this. Second, the chain is secured with very sophisticated cryptographic functions. As a result, it is extremely unlikely that someone could hack into the chain and change transactions. To do so, you would need to harness an unrealistic amount of computing power (read on).

One further important point. Transactions are added to bitcoin blockchain every 10 minutes. This means that there are some transactions in limbo waiting to go into the chain. Limbo is known as the ‘memory pool’. When

I go to my retailer and pay in bitcoin, my retailer checks both the blockchain and the memory pool to make sure I have the bitcoin to pay. Nevertheless, the memory pool is less secure than the blockchain.

The Miners

The miners are the people or groups of people that add new blocks to the blockchain. They solve a difficult cryptographic problem to secure a block. The miners are rewarded for this service. However, this mining should not be confused with gold or diamond mining.

Most of the mining occurs in pools where people join forces. Think of people offering their overnight computing time for the SETI project. The biggest mining pool for bitcoin is called AntPool. Anyone can join as long as you have some computing power.

But not all miners are rewarded. Approximately every 10 minutes, a new block is “won”. This means that a miner or mining pool has solved the cryptographic problem. Currently, the winning miner gets the 25 bitcoins. The losers get nothing.

As a result, bitcoin mining has been called “competitive bookkeeping”.

Early on, someone realized that standard computer processors (CPUs) were not well suited to solve these problems. The mining was much more efficiently performed on graphics processors (GPUs). Currently, most miners are using special computers with “application-specific integrated circuits” or ASICs. Just as the name implies, the processor is specifically designed to efficiently solve the type of math problem necessary to “win” the block.

Miners have a large amount of computing power, currently about 9,800,000 petaFLOPs – that’s 9.9 sextillion (9.8 followed by 21 zeroes) operations per second.² Currently, the world’s fastest supercomputer is China’s NUDT Tianhe-2 which runs at ‘only’ 33.9 petaFLOPS. Hence, to match the distributed power, you would need nearly 300,000 of the world’s fastest supercomputers. However, as mentioned earlier, mining needs specialized processors. Indeed, there are no floating point operations. The power of the network is measured in a different metric called hashing power. Currently, the network capacity for hashes is enormous. To match the hashing power of the network would cost at least \$2 billion. The key insight here is that there is a purpose for the bitcoin computing power. In order to hack the chain, you need match the capacity – which seems very unlikely – at least for the average hacker.

In the end, the miners’ work ensures that the common knowledge of all transactions in the block chain is safe.

² See <http://www.bitcoinwatch.com/> also see Cohen (2013).

Securing the Block chain

To understand the security of the block chain, it is important to understand a cryptographic hash function. I will focus on one particular function, called SHA-256. SHA is short for “secure hash algorithm”. It is open source code and it was originally developed by the NSA.

Usually when we think of encryption, some data is scrambled and there is a key to unlock the encryption to get back to the original data. Hashes do not work like that. They are one way functions. You can feed a string of text or numbers to the SHA-256 program and it will spit out a 64 hexadecimal code. To really understand this, you need to do a hash (I am serious). Go to,

<http://www.xorbin.com/tools/sha256-hash-calculator>

and copy the phrase, “Hello, world!” (without quotations) into the data box. Then press the button “Calculate SHA256 hash”. You will get this:

315f5bdb76d078c43b8ac0064e4a0164612b1fce77c869345bfc94c75894edd3

This is a 256 bit (or 32 byte) hash. Now do it again, except drop the exclamation mark. You will get this:

4ae7c3b6ac0beff671efa8cf57386151c06e58ca53a78d83f36107316cec125f

Note that the two hashes are completely different.

So the hashes have a number of important properties: 1) changing just a small amount of the input produces a completely different output; 2) the output is always 256 bits but the input could be anything from a single character to every word in the Bible (actually the maximum length for input is $2^{64}-1$ which is a huge number); and 3) hashes only go one way. This last property is the most important. Think of it this way (apologies to the vegetarians). There is no way to reassemble a cow after it goes through a meat grinder.

The main risk with hashes is a “collision”. This occurs when two different inputs deliver the same output. Is this theoretically possible? Yes. The hash produces $2^{256}-1$ different outputs. There must be collisions if there are more inputs. However, this is practically impossible. Bruce Schneier argues that the main issue is the energy needed to run the calculations. He shows that if all of the energy of the sun was captured (literally by putting a ball around the sun) for 32 years, you only get to 2^{192} combinations – well short of the 2^{256} . So theory is far from reality and these hashes are secure.

Another way of thinking about hashes is that they are unique identifiers. Indeed, you use SHA-256 every day – but you don’t know it. Take any email and “view all headers”. You will see a reference to DKIM (DomainKeys Identified Mail). You will see at some point “a=” (“a” refers to the signing algorithm) and you should see a reference to SHA-256. More generally, this hash function (and others) are commonly used to provide communication security on the Internet.³

So hashes are important – but how do they relate to mining and the block chain?

³ These hashes are used in the current Transport Layer Security (TLS) and the previous Secure Sockets Layer (SSL) to allow for data/message confidentiality and message authentication.

Next Section ...

My paper is incomplete. My slide deck is well ahead of the paper. Hence, please go to the slide deck which is next.

I also have a number of teaching decks. None of these are publically available yet but can be requested.

- "Bitcoin Myths and Facts" explores eight common claims about bitcoin.
- "Crypto Disruption" introductory deck.
- "The Blockchain Identity" is a high level introduction to blockchain. Includes private and public blockchains
- "Why Money" the history of money from ancient times to today's fiat currencies
- "The History of Digital Money" history from 1982 to present focusing on digital money.
- "Cryptology" introduction to ciphers and encryption.
- "Hashing" exploration of SHA-1 and SHA-2
- "Transaction Mechanics" explores the details of bitcoin transactions
- "Anonymity vs. Privacy" details how anonymous blockchains are
- "Keys" private and public keys
- "Addresses" show how to get a public address from a private key
- "Cryptography 101" basic cryptography, RSA, Elliptic Curve
- "VISA vs. Bitcoin"
-

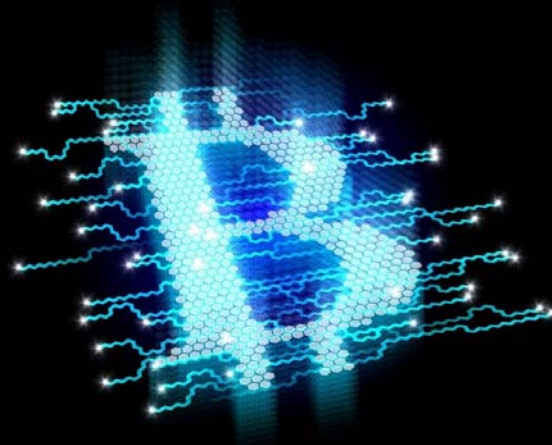
References

Chaum, David. 1983. Blind Signatures for Untraceable Payments. *Advances in Cryptology Proceedings of Crypto 82*, 3. 199-203.

Chaum, David. 1985. Security Without Identification: Transactions Systems to Make Big Brother Obsolete, *Communications of the ACM*, 28, 10, October.

Chaum, David, Amos Fiat and Moni Naor, 1990. Untraceable Electronic Cash. In S. Goldwasser (ed.), *Advances in Cryptology*, 319-327.

Cohen, Reuven, 2013. Global Bitcoin Computing Power Now 256 Times Faster than Top 500 Supercomputers, Combined! *Forbes*, November 28, 2013.



Cryptofinance

Campbell R. Harvey

Duke University, NBER and
Man Group, plc

Version: January 16, 2016

With material from Alex Meijer and Ryan Lanman.

Before Reading This Document

Go to this website:

<http://www.xorbin.com/tools/sha256-hash-calculator>

I would like you to hash the phrase: “Hello, world!” with a number appended. No spaces. Do it three times for three different strings.



Hello, world!0

Hello, world!1

Hello, world!4250

Notice the last hash. It should have some leading zeroes. The reason for this exercise will become apparent later.

Disruption 101

	
<p>Send warm wishes today.</p> <p>FOR ONLY \$5 / SEND UP TO \$50 <small>TRANSFER FEE</small></p> <p><small>FOR PICK UP WITHIN THE U.S.</small></p> <p>Find Agent Location »</p>	<p>Send warm satoshis today.</p> <p>FOR ONLY \$0.01 / SEND UP TO \$ANY <small>TRANSFER FEE</small> AMOUNT</p> <p><small>FOR PICK UP ANYWHERE ON EARTH</small></p> <p>Pick Your Wallet »</p>
<p><i>moving money for better</i></p>	<p><i>moving money <u>far</u> better</i></p>

Western Union, we fixed your ad for you.

In the news....

April 30, 2015 4:00 am

Goldman backs fundraising by payments company Circle

Stephen Foley in New York

[Author alerts](#) ▼



[Goldman Sachs](#) is backing the latest fundraising by Circle Internet Financial, a mobile payments start-up built on the bitcoin network.

Boston-based Circle has announced a \$50m cash infusion, led by Goldman and China-focused venture capital firm IDG Capital

Partners, to help fund its expansion beyond bitcoin and into other currencies.

In the news....

April 30, 2015 4:00 am

Goldman backs fundraising by payments company Circle

Stephen Foley in New York

[Author alerts](#) ▼



[Goldman Sachs](#) is backing the latest fundraising by Circle Internet Financial, a mobile payments start-up built on the bitcoin network.

Boston-based Circle has announced a \$50m cash infusion, led by Goldman and China-focused venture capital firm IDG Capital

Partners, to help fund its expansion beyond bitcoin and into other currencies.

March 10, 2015 11:02 pm

Masters joins cryptocurrency start-up

Tom Braithwaite and Ben McLannahan in New York

[Author alerts](#) ▼



[Blythe Masters](#), the former JPMorgan executive who helped pioneer credit derivatives in the 1990s, has re-emerged as chief executive of a cryptocurrency start-up.

Digital Asset Holdings aims to be a venue for buyers and sellers of financial assets to meet and transact, switching currencies into

bitcoin in order to cut the cost and time of settlement and make use of the decentralised "block chain" as a secure record of transactions.

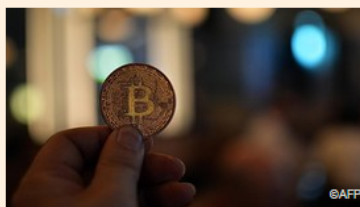
In the news....

April 30, 2015 4:00 am

Goldman backs fundraising by payments company Circle

Stephen Foley in New York

[Author alerts](#) ▼



[Goldman Sachs](#) is backing the latest fundraising by Circle Internet Financial, a mobile payments start-up built on the bitcoin network.

Boston-based Circle has announced a \$50m cash infusion, led by Goldman and China-focused venture capital firm IDG Capital

Partners, to help fund its expansion beyond bitcoin and into other currencies.

January 20, 2015 8:05 pm

Bitcoin company Coinbase lands \$75m investment from NYSE and BBVA

Sally Davies in London and Thomas Hale in Madrid

[Author alerts](#) ▼



Coinbase has become the world's most well-funded bitcoin company after landing a \$75m investment from high-profile backers, including the [New York Stock Exchange](#), Spanish bank [BBVA](#) and the former chief executives of Citigroup and Reuters respectively.

The funding round in the San Francisco-based start-up that lets people store, send and accept payment in bitcoins, was led by DFJ, the venture capital group. But it is the presence of traditional financial services companies and figures which will be interpreted as an indicator of growing investor interest in mainstream applications of the controversial digital currency.

March 10, 2015 11:02 pm

Masters joins cryptocurrency start-up

Tom Braithwaite and Ben McLannahan in New York

[Author alerts](#) ▼



[Blythe Masters](#), the former JPMorgan executive who helped pioneer credit derivatives in the 1990s, has re-emerged as chief executive of a cryptocurrency start-up.

Digital Asset Holdings aims to be a venue for buyers and sellers of financial assets to meet and transact, switching currencies into

bitcoin in order to cut the cost and time of settlement and make use of the decentralised "block chain" as a secure record of transactions.

In the news....

May 11, 2015 6:43 pm

Nasdaq adopts bitcoin backbone for stocks

Richard Waters in San Francisco

[Share](#) ▾

[Author alerts](#) ▾

[Print](#)

[Clip](#)

[Gift Article](#)

[Comments](#)



Nasdaq is to start using the technology behind the virtual currency bitcoin to handle transactions on its market, making it what is thought to be the first major financial market to adopt the idea.

The blockchain — the backbone on which bitcoin depends — has attracted wide interest in the financial world as a potentially revolutionary way to streamline many different types of transactions, though few alternative applications have yet been tried beyond bitcoin.

In the news....

R3CEV includes:

- Goldman
- JPMorgan
- Credit Suisse

September 15, 2015 12:42 pm

Blockchain initiative backed by 9 large investment banks

Philip Stafford

[Share](#) [Author alerts](#) [Print](#) [Clip](#) [Gift Article](#) [Comments](#)



Nine of the largest investment banks, including [Goldman Sachs](#), [JPMorgan](#) and [Credit Suisse](#), are planning to develop common standards for blockchain technology in an effort to broaden its use across financial services.

The group is looking to channel data, ideas and financial backing to a start-up called R3CEV, a New York-based group of trading and technology executives.

Campbell R. Harvey 2016

In the news....

R3CEV includes:

- Bank of America
- Deutsche Bank
- Citibank ...
- Now 42 banks (21 employees!)

Citi, HSBC Partner With R3CEV As Blockchain Project Adds 13 Banks

Pete Rizzo (@pete_rizzo_) | Published on September 29, 2015 at 15:54 BST

NEWS



Distributed ledger startup R3CEV has added 13 new banking partners, bringing the total number of banks involved in its activities to 22.

In a [release](#), R3 revealed Bank of America, BNY Mellon, Citi, Commerzbank, Deutsche Bank, HSBC, Mitsubishi UFJ Financial Group, Morgan Stanley, National Australia Bank, Royal Bank of Canada, SEB, Societe Generale and Toronto-Dominion Bank had signed on to [the project](#).





Campbell R. Harvey 2016



The Landscape

<http://coinmarketcap.com/>

- Bitcoin is the leader (approximate \$6 billion in market capitalization) founded in 2009
- Ripple is #2 with \$0.2 billion in market capitalization
- Currently, Coinmarketcap.com lists over 500 crypto-currencies. However, 98% of them are highly illiquid (and not secure as we will discover).

The Landscape

- Visa/Mastercard/Paypal are centralized and for profit businesses
- Bitcoin and others operate on peer-to-peer (P2P) networks, i.e. decentralized
- Bitcoin network is “guaranteed” by cryptographic algorithms rather than governments or corporations
- The currency “bitcoin” is a result of the Bitcoin network, i.e. Bitcoin is not just a currency.

The Innovation

- Crypto-currencies have been around since the 1980s
- The early ones, Digicash and Ecash failed because they did not provide a solution to the “double spend” problem. That is, with the same digital key you could spend twice or more.
- Bitcoin solves the double spend problem

Triple-Entry Accounting

- Usually, we think of a transaction as having a debit and a credit (double entry accounting)
- With Bitcoin, there is a third entry. Every transaction goes into a repository of common knowledge.
- This repository or public ledger is highly secure and maintained by everyone on the network
- The public ledger is the final word – so there can be no disagreement about the debits and credits and there can be no “double spending”
- The public ledger is called the “**blockchain**” (more later) or the “**World Wide Ledger**”

The Questions

- Is Bitcoin just a classic bubble?
- Alternatively, is Bitcoin an innovative, disruptive new technology that could be the next big thing?
- If Bitcoin is not just a currency what are the other applications?



The Founder

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

<https://bitcoin.org/bitcoin.pdf>

Published November 2008

Pseudonym or Dorian, Craig or Nick?

The Founder

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Electronic payment
system

P2P

Secure via
hash

No double
spending

Warning
about majority of
computing power

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

<https://bitcoin.org/bitcoin.pdf>

Published November 2008

The Beginning

- An Open Source Project, with developer mailing list and github repositories
- Satoshi remained a visible member of the community until December, 2010 before disappearing
- Satoshi handed over development to Gavin Andresen, lead developer
- Core development team maintains the reference client Bitcoin-QT (GUI) / bitcoind

Source: Brad Wheeler, Bitcoin: What *is* it?

The Beginning

- The network was “started” January 3, 2009 with the Genesis Block
- Bitcoin v0.1 was released January 9, 2009
- Latest version is v0.12 released May 19, 2015

<https://bitcoin.org/en/version-history>

Source: Brad Wheeler, Bitcoin: What *is* it?

Foundation/MIT Digital Currency Initiative

- Gavin Andresen (Lead Core Dev) and team moved from Bitcoin Foundation to MIT Digital Currency Initiative (April 22, 2015)

<http://gavintech.blogspot.com/2015/04/joining-mit-media-lab-digital-currency.html>

The Mechanics

How does it work?*

- Currently, 25 bitcoins are produced every 10 minutes
- Only miners get new bitcoins
- Size of each batch of new coins halves approximately every 4 years; coins divisible to 8 decimals places; 1 bitcoin=100,000,000 satoshi; bitcoin also known by BTC

Called "bits" →

Bitcoin	BTC	1
deciBitcoin	dBTC	0.1
centiBitcoin	cBTC	0.01
milliBitcoin	mBTC	0.001
microBitcoin	μBTC	0.000001
Finney ^[5]	-	0.0000001
satoshi	-	0.00000001

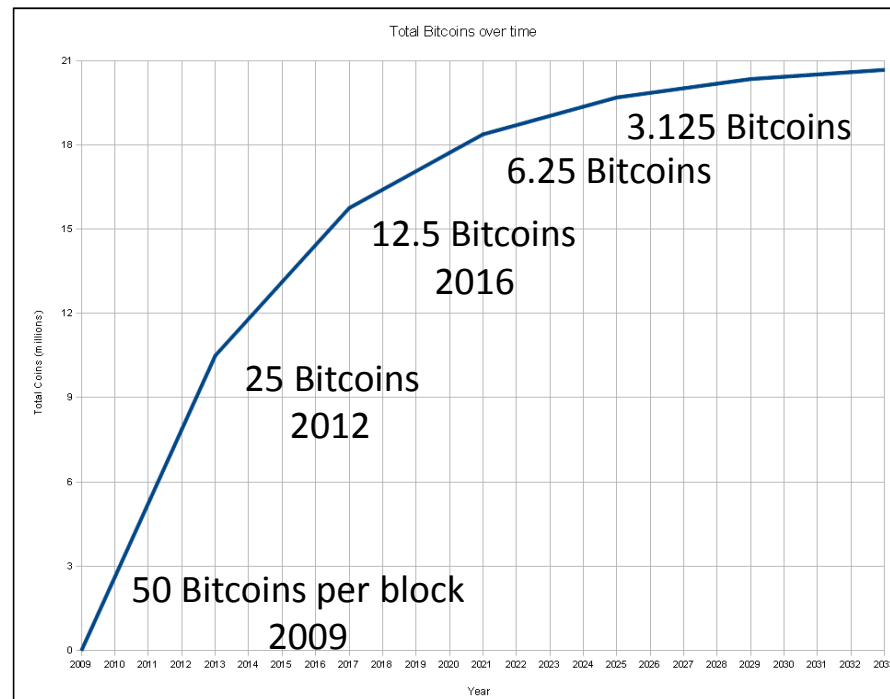
<https://en.bitcoin.it/wiki/Units>

*I have borrowed liberally from a number of sources, including, [King, Williams, and Yanofsky 2013, Quartz](#).

The Mechanics

How does it work?

- In the year 2141, new coins go to zero which caps the number of coins at near 21 million, but production slows



The Mechanics

Mining

- Miners are competitive bookkeepers
- Think of a huge public ledger containing the history of every bitcoin transaction
- Every time someone wants to send bitcoins to someone else, the transfer is validated by network
 - Make sure the person has the bitcoins to transfer
 - If the person has the bitcoins, it is added to the ledger
 - To secure the ledger, the miners seal it behind computational code
 - There can be no double spending and no counterfeiting

The Mechanics

Mining

- Miners are rewarded for their work in validating and sealing the ledger
- The miner rewarded is the first one to validate and seal

The Mechanics

Double spending

- Want to avoid spending the same currency more than once
- Traditional banks have networks to prevent this. For example, you have \$100 in your bank account and write two checks for \$100. The first person to cash the check gets the \$100 and the other bounces (and creates lots of fees)
- With Bitcoin, there is no bouncing. The ledger* is consulted to make sure the person has the bitcoin to spend
- Question: How do you ensure privacy and make the transactions transparent?

*Also, the pending transactions are checked, the so called “memory pool”.

The Mechanics

Bitcoin accounts?

- There is no traditional account, like a bank account where the bank can check your balance
- The ledger keeps track of all bitcoin transfers – not the balances

The Mechanics

Bitcoin basics

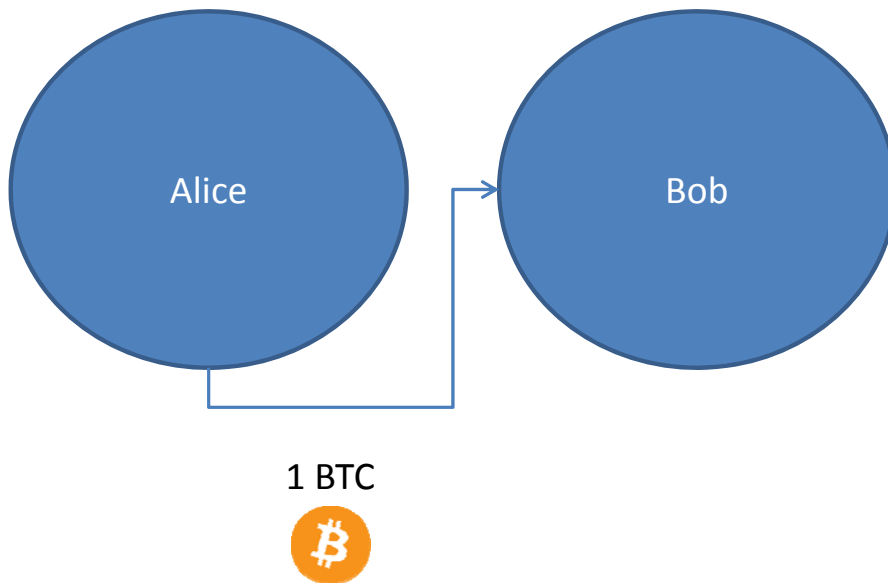
- Each bitcoin address has a public+private key
- Anyone can send to a public address
- However, you need a private key to send a bitcoin from any particular address
- Payments are irreversible



The Mechanics

Simplified example:

Alice buys something from Bob and sends him 1 bitcoin



The Mechanics

Examples: Alice 1 BTC → Bob

- Bob sets up a digital (public) address and sends it to Alice
- Like email account with password – except it (should) changes for every transaction.
- Alice adds Bob's address and the amount of bitcoins to a 'transaction' message.
- Alice signs the transaction (more later on this!)
- Alice broadcasts the transaction on the Bitcoin network for all to see.

The Mechanics

Examples

- Alice sends to Bob

Quoted in satoshi
so 50 bitcoins

```
Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

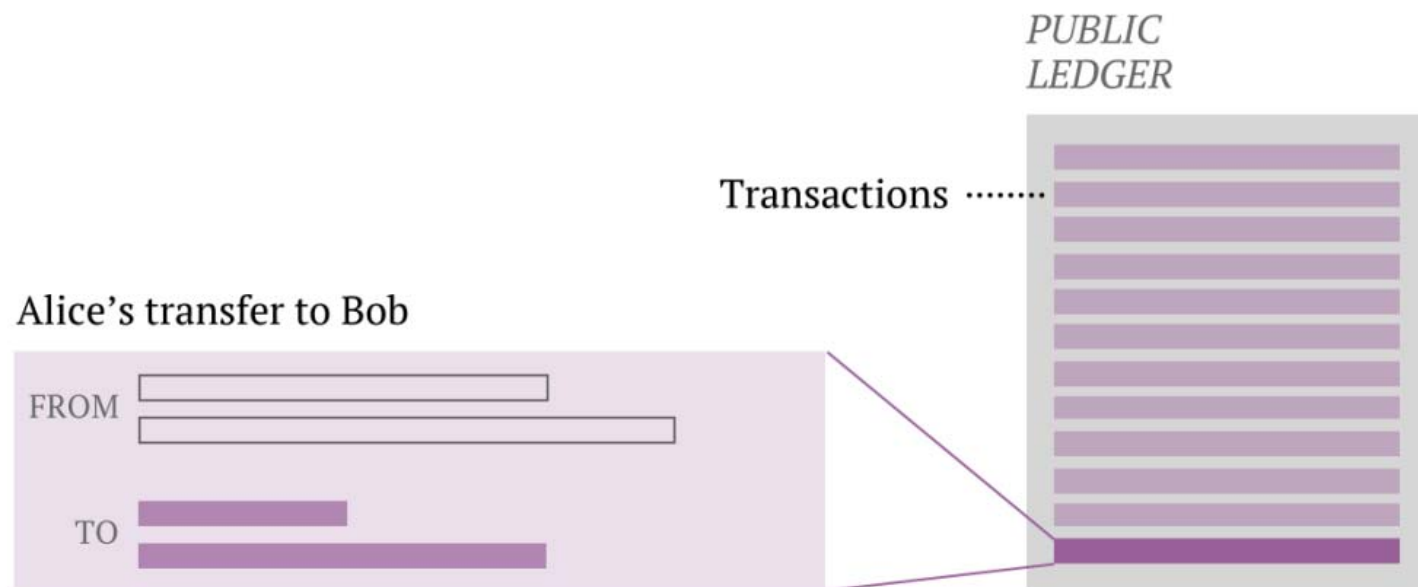
TRANSACTION RECORD



The Mechanics

Examples

- Transaction sent to every Bitcoin node on the Internet
- If the transaction is validated, it is added to the ledger

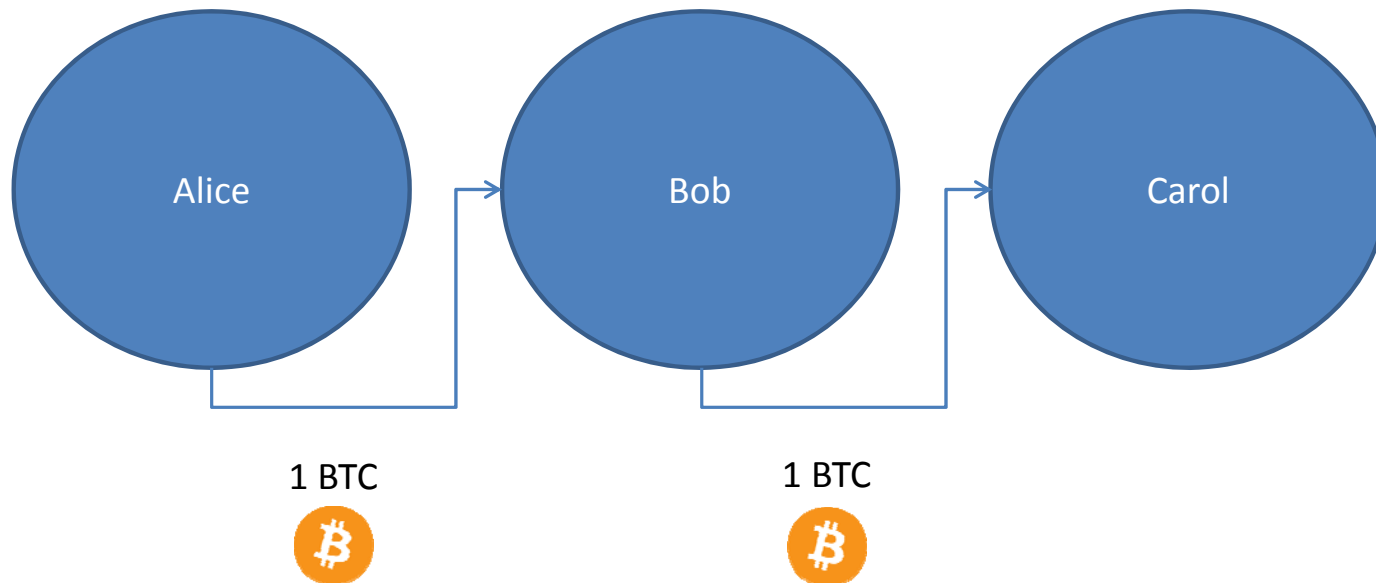


Graphics from King, Williams and Yanofsky (2013)

The Mechanics

Examples continue:

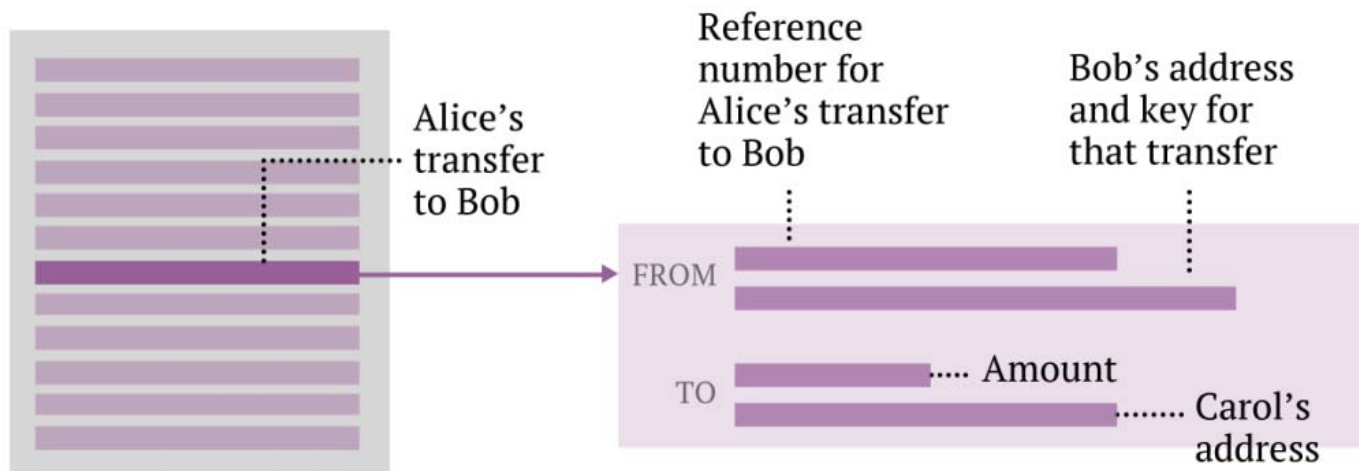
Bob buys something from Carol and sends her 1 bitcoin



The Mechanics

Examples

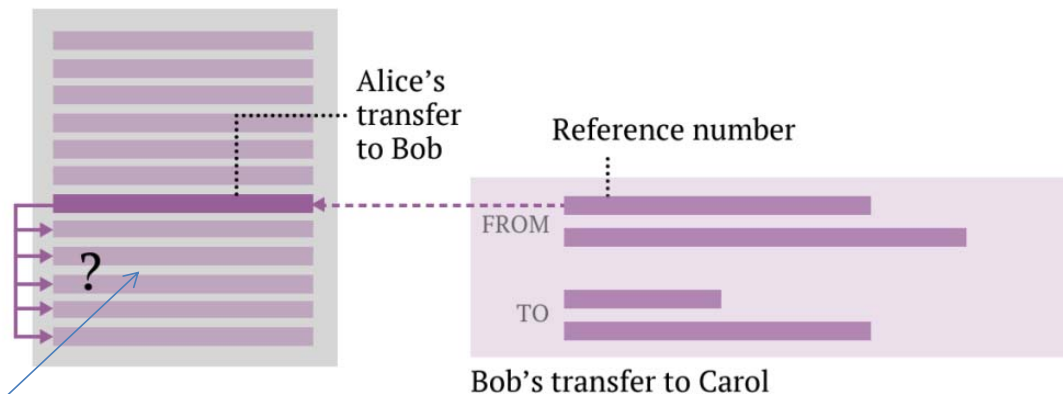
- Bob sends Carol 1 bitcoin
- Carol sets up an address and a key
- Bob takes the bitcoin he got from Alice, uses his address and key from that transfer to sign over to Carol



The Mechanics

Examples

- Proposed transaction gets sent to all on network to ensure Bob has not already spent the bitcoin from Alice



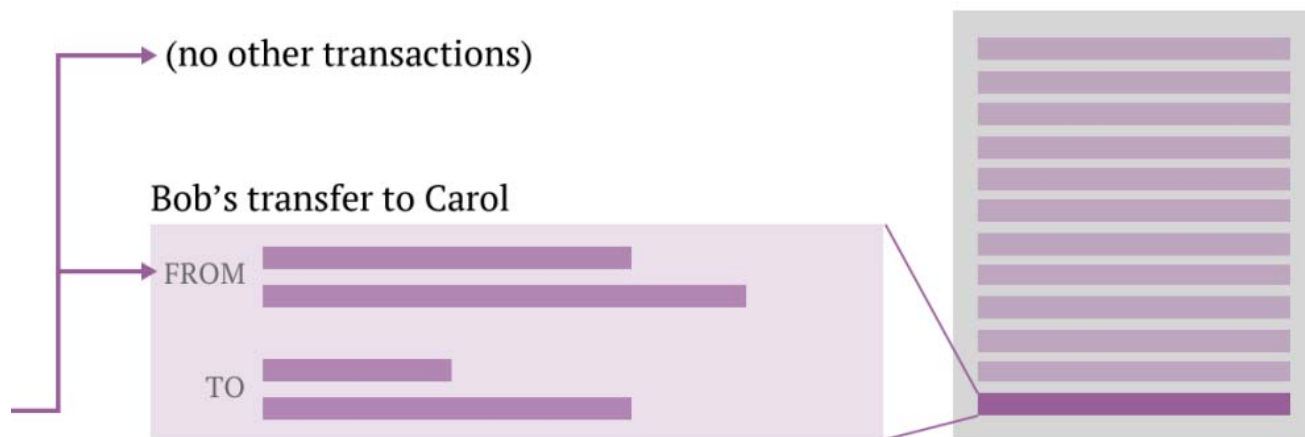
Other transactions that have occurred since Alice's original transfer to Bob

Graphics from King, Williams and Yanofsky (2013)

The Mechanics

Examples

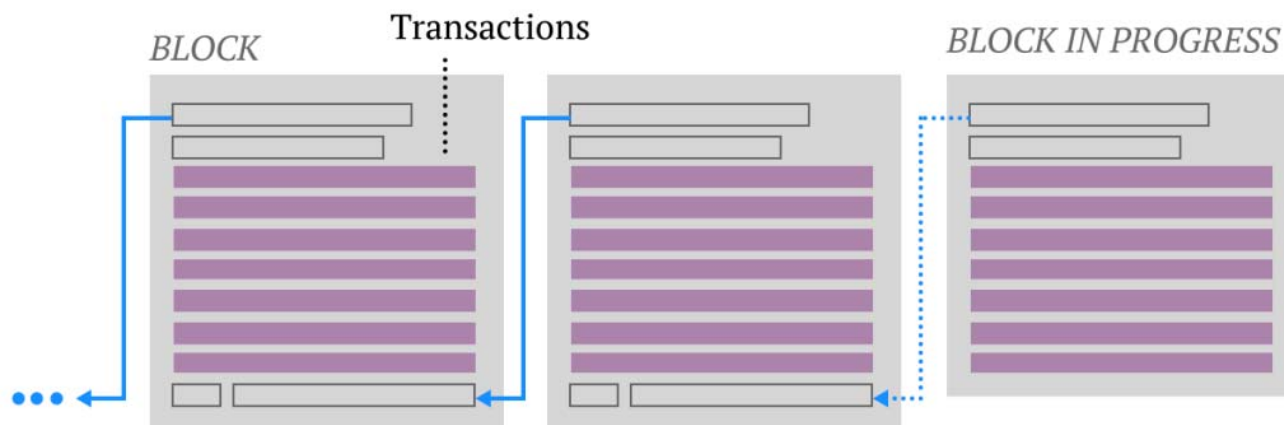
- If transaction validated, then added to the ledger



The Mechanics

The ledger

- Ledger broken up into 10 minute “blocks”
- Every block contains a reference to the block before it so you can trace every transaction all the way back to 2009



All of the blocks are called the “blockchain”

The Mechanics

The Blockchain

- All full nodes (running bitcoind or Bitcoin-Qt) (includes miners) have the complete block chain
- If a computer is turned off, when it starts up again, it will send a message to get the blocks created when computer was down
- Updates are provided by the system of miners

The Mechanics

Validation

- Miners compete to add a new block to the chain
- Need to complete a cryptographic “proof of work”
- Problem is different for each block and involves a cryptographic hash functions which take an input and delivers an output
- Each block contains the “Proof of work” (it is difficult to produce but easy to check)

The Mechanics

Hash (SHA-256)

- SHA-256 (Secure Hash Algorithm) developed by the NSA
- Output is 64 numbers/characters (called hexadecimal, a-f + 0-9) no matter how long the input it receives

The Mechanics

Hash (SHA-256)

- My I&E 550 syllabus

91efe4c1b83ce92a56007b15be0f700d3eb576718659d6321eaf55395d5c6abe

- My Finance 663 syllabus

6774deb9c313a3c87d4b1fadb69a9d1395cdbbc802b10707fa7e620ad722c0f63

- King James Bible (4.2mb)

47f63b8cd8470051acd3a3c0bd5c77c4aa9574d79cf5bfb3e576facabbc11491

The Mechanics

Hash (SHA-256)

- King James Bible (4.2mb)
47f63b8cd8470051acd3a3c0bd5c77c4aa9574d79cf5bfb3e576facabbcb11491
- King James Bible (4.2mb) – with 5 characters deleted
961c112581bd04e67285f56a354c98ad56cd65244dc768545cfde5bd8ef639c1

Note: You can hash the hashes

- King James Bible SHA-256 of SHA-256
0c8b120036a32525e9737fa8ed67b9af337affc7dae557d7244592c286b2cfd8

<https://archive.org/stream/thebibleoldandne00010gut/kjv10.txt> (without front and back matter)

The Mechanics

Hash

- It only goes one way. Once you have the output, you cannot go back to the input. Think of it as generating a unique identifier
- Even a trivial change in the input, produces a completely different hash
- On-line calculator example: <http://www.xorbin.com/tools/sha256-hash-calculator>
- SHA-512 at <http://abunchofutils.com/u/computing/sha512-hash-calculator/>

The Mechanics

Hash

- SHA-256 maximum input size is $2^{64}-1$ bits
- Large number? Suppose you put one penny on the first square of a chess board, two pennies on next, etc.
- How much is on the last square?



The Mechanics

Hash

- SHA-256 maximum message size is $2^{64}-1$ bits
- Large number? Suppose you put one penny on the first square of a chess board, two pennies on next, etc.
- How much is on the last square?
 - \$9, 223,372,036,854,780.00 (\$9.2 quintillion)
 - US GDP \$15,000,000,000.00
 - Hash allows for 18.5 quintillion bits of input

Importantly, we are only talking about the inputs. To break the SHA-256, you need to evaluate 2^{256} (See FAQs).

The Mechanics

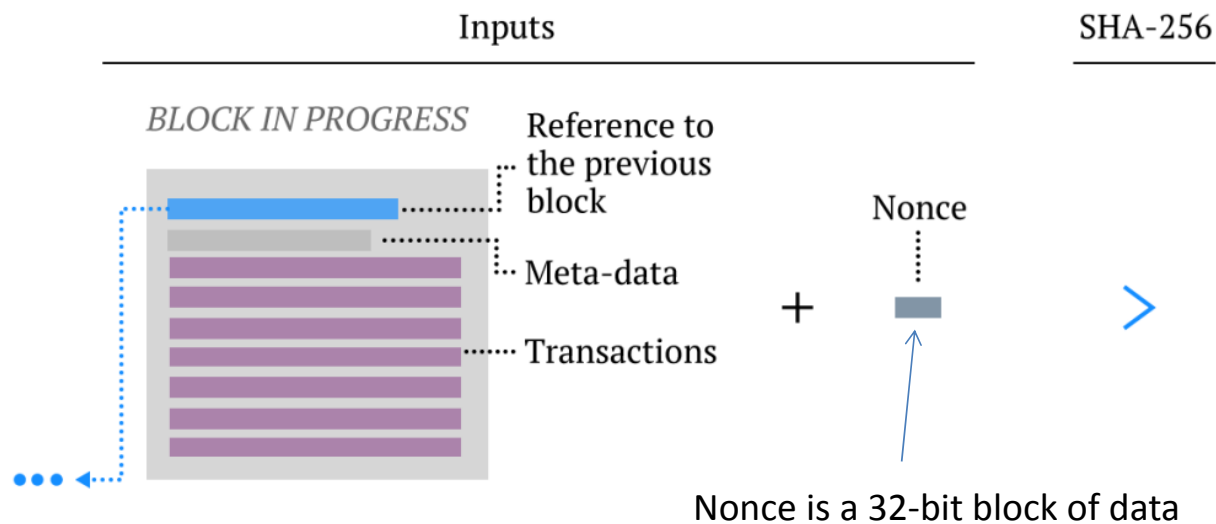
Hash

- Some previous hashes, SHA-1 and SHA-0 have been abandoned because of actual or theoretical “collisions”
- A collision is when two different inputs lead to the same output
- Note SHA-256 also used for SSL (Secure Sockets Layer)/TLS for secure traffic on the Internet
- Also there is SHA-512 which is in the category of SHA-2 (allows for 2^{128} - 1 bits) and a new class of SHA-3 which uses 5x5 arrays of 64-bit words

The Mechanics

What is the proof of work?

- Miners take a hash of the contents of the block they are working on (transactions, time stamps, reference to previous block) plus a random number called a “nonce”




Graphics from King, Williams and Yanofsky (2013)

The Mechanics

What is the proof of work?

- Their goal is to find a hash that has at least a certain number of leading zeroes, e.g.



00000eb9c313a3c87d4b1fadb69a9d1395cdbbc802b10707fa7e620ad722c0f63

- More leading zeroes means fewer solutions – and more time to solve the problem – it determines the “difficulty” (currently 17 zeros)
- Every 2016 blocks (two weeks), the difficulty is reset
- If it takes less than 10 minutes on average to solve the 2016 blocks, the difficulty is reset automatically

The Mechanics

Example of recent solution (January 14, 2016)

0000000000000000000011eae2aca0e002ed6d5fa1fb6a3755dbcaa8b0cab0ec3f6

See <http://blockexplorer.com>

0.0000000000000000000047703150496763649630755092963252383

[illegible]

49

The Mechanics

What is the “proof of work”?

- A target is set and you win if the number you draw is less than the target (leading zeros mean small numbers)
- Suppose the target=5. There is a lottery with numbers ranging from 1 to 1,000,000,000. There is a very small probability of drawing a 1,2,3,4 or 5.
- The current target has 17 leading zeros. See <http://blockexplorer.com>

The Mechanics

What is the proof of work?

Example. Try to find the nonce that turns the phrase “Hello, world!” into a hash with four leading zeroes:

"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7

...

"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfd65cc0b965

"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6

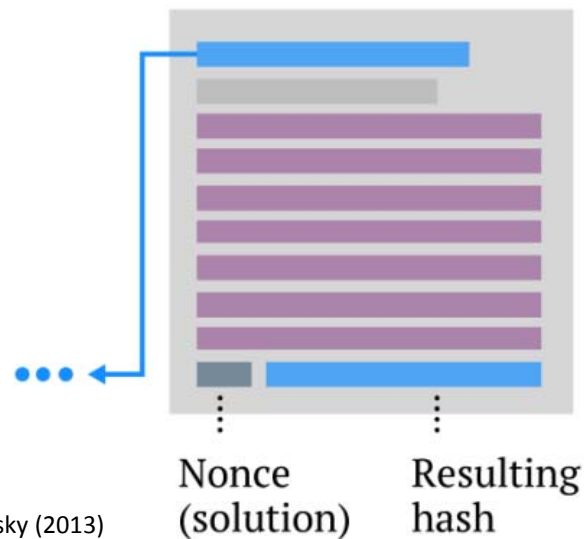
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

We get the leading zeroes after trying 4251 nonces.

The Mechanics

What is the proof of work?

- When the miner finds the nonce that works, they “win” the block.
- They provide the nonce with the block and everyone (not just miners) verifies

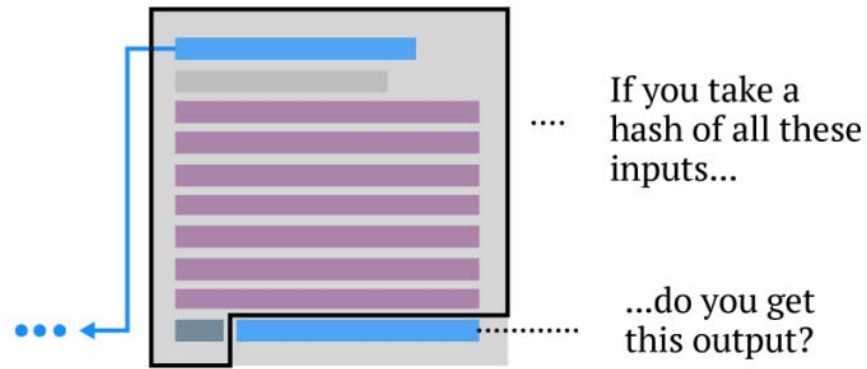


Graphics from King, Williams and Yanofsky (2013)

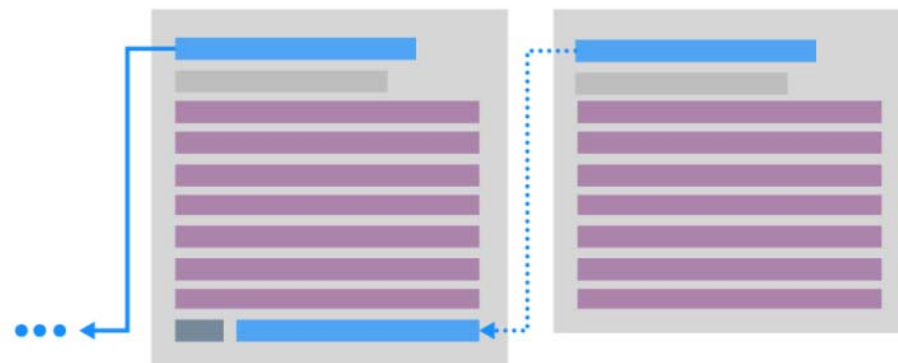
The Mechanics

What is the proof of work?

- The block gets sent to every miner
- They get the winner's nonce and verify the hash
- Work is hard to solve but easy to verify



If yes, then start a new block



Graphics from King, Williams and Yanofsky (2013)

The Mechanics

It is a little more complicated ...

- In previous example, there might be an incentive to have a small number of transactions in block
- This is solved by having all candidate blocks having the exact same size: 80 bytes (which is small – but what it represents is not small)
- The key is to understand what is in it

The Mechanics

80 bytes

- 4 bytes: version number (same for all miners)
- 32 bytes: previous block (same for all miners)
- **32 bytes: hash of the transactions in the candidate block**
- **4 bytes: time stamp**
- 4 bytes: difficulty of task (same for all miners)
- **4 bytes: nonce**

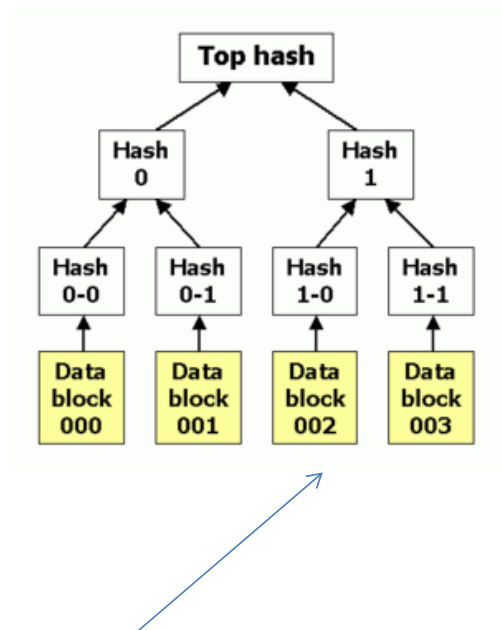
The Mechanics

Miner will vary the nonce – but a good machine can try all possible 32-bit nonce combinations in about 1 second (about 4 billion calculations)

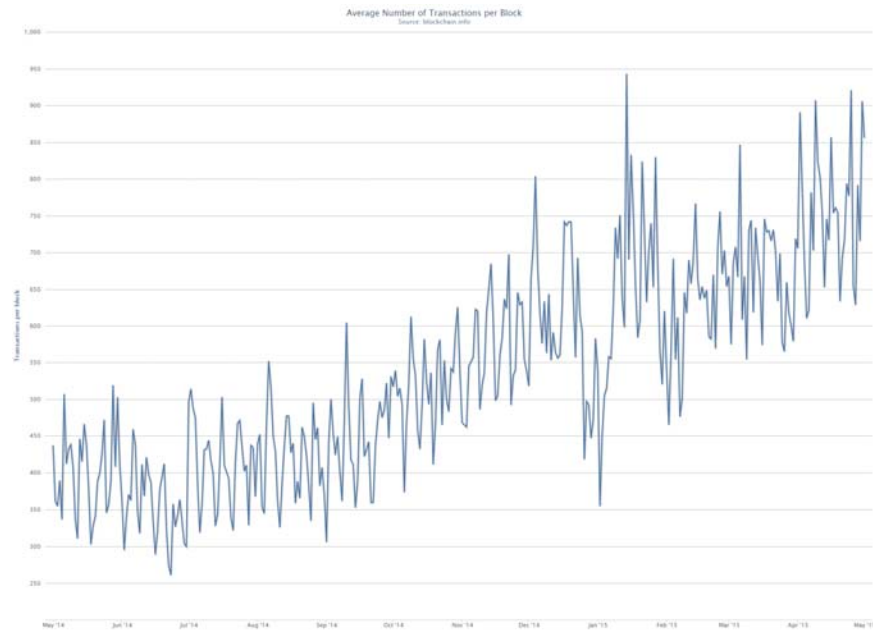
- Miner will also vary the order to which transactions are grouped (in a Merkle tree)
- Time stamp can also be varied

The Mechanics

Hash of the transactions is a Merkle tree (or hash tree) which includes multiple hashes



Each data block is a transaction

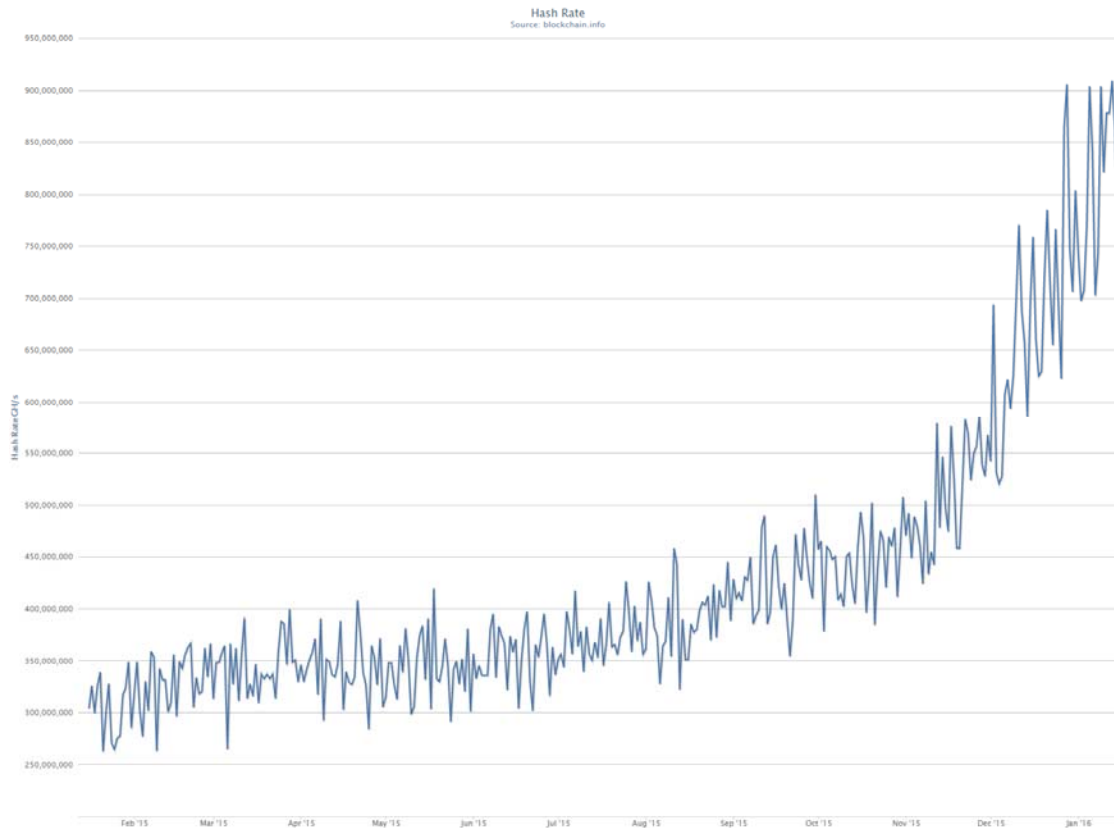


Block averages 700 transactions

<https://blockchain.info/charts>

The Mechanics

Lots of hashes! 800 million gigahashes per second!



<https://blockchain.info/charts>

The Mechanics

Miners' role:

- Mining code is open source
- Miners are competitive
- Miners pool resources

Miners' purpose:

- New bitcoins are distributed to those that are doing the work
- Miners provide proof of work that makes the network work (i.e. there is no double spending)

The Mechanics

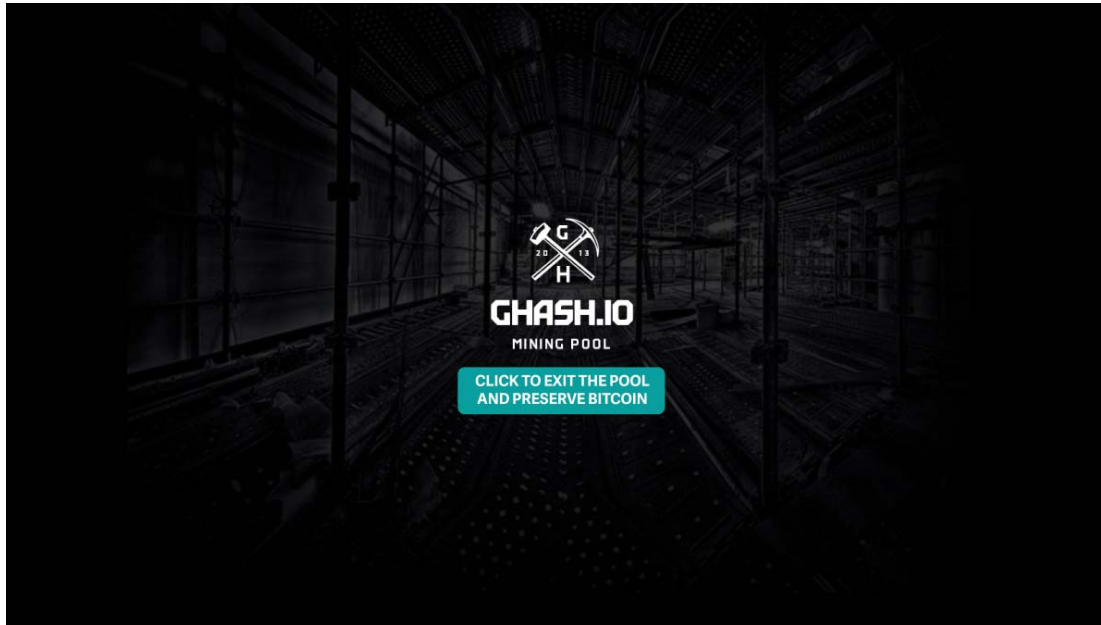
Vulnerability

- If a mining pool gains a large amount of computing capacity, they can attack the network
- Essentially, they can rewrite all the blocks and create a new block chain

The Mechanics

Vulnerability

- January 9, 2014 Ghash.io had 45% of all mining
- Had to appeal to people to exit the pool

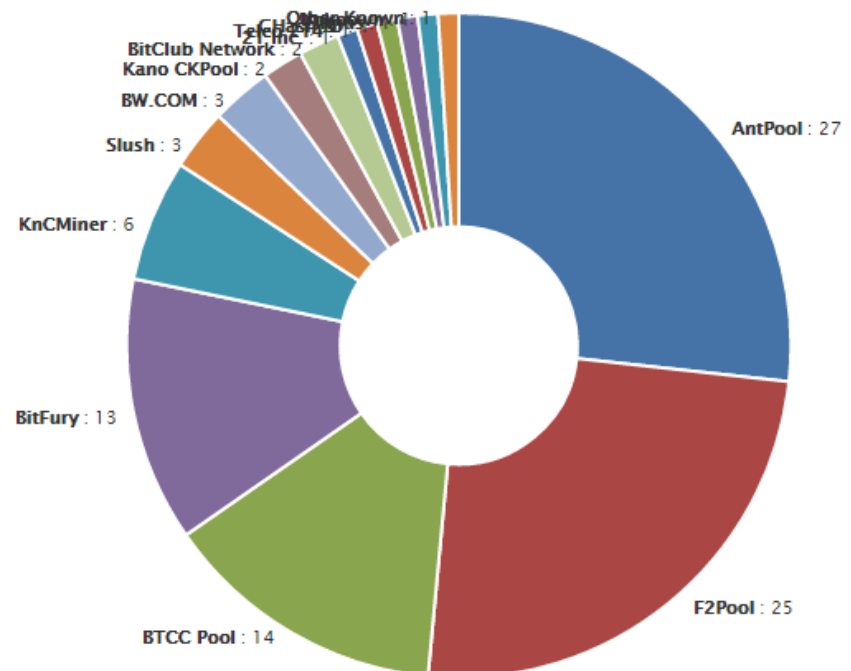


See their press release: https://ghash.io/ghashio_press_release.pdf

The Mechanics

Vulnerability

- Currently there are two pools that control nearly half the mining

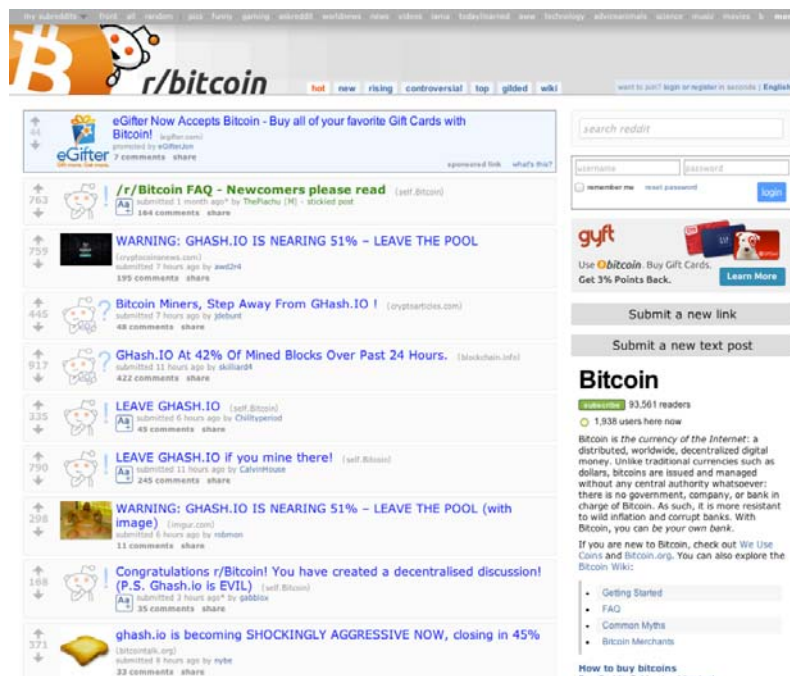


See <https://blockchain.info/pools>

The Mechanics

Vulnerability

- Not clear what the incentive is to “take over”
- If it ever happened, the value of the Bitcoin would disappear



The Mechanics

Private Key/Public Key:

- Bitcoin based on strong cryptography
- Usually we think of using a key to encrypt and decrypt
- It is possible to use two keys: private (secret) and public (give to anyone)
- You can sign a message using a private key such that the signature is unforgeably tied to the public key
- Two keys are known as the “key pair”
- Collection of keys is called a “wallet”

The Mechanics

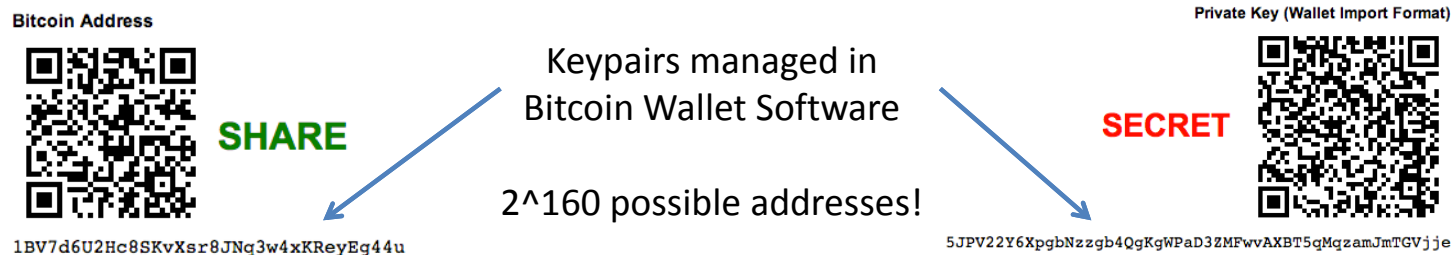
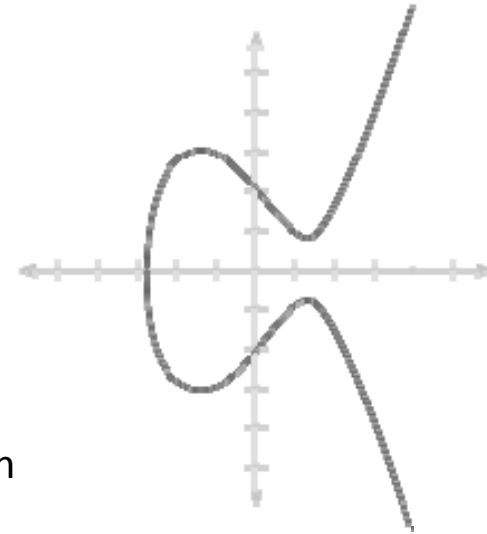
Signing:

- Signing involves your private key and a nonce
- Anyone can use the nonce and public key to verify that the message was created with the private key
- Creation of a transaction address is very secure, involves
 - Cryptographic “Elliptic Curve DSA” on curve secp256k1
 - Double application of SHA-256 hash
 - Application of RIPEMD-160 hash

The Mechanics

How it works:

- Users connect to the Bitcoin Network
- Client “wallet” (key management module) generates public/private key pairs based off of random number stream
 - Key pairs use Elliptic Curve Cryptography (ECDSA)
- Public key is encoded into a 27-34 character *address* string that can be shared to receive payments
- Private key is used to spend coins by digitally signing transaction messages that reference specific deposits sent to it



“Bank Account Number” Cheap, expendable, easy to produce

“Signing Key”

Source: Brad Wheeler, Bitcoin: What is it?

The Mechanics

Using Bitcoin:

- Open account on Coinbase.com (for example) many competitors in the works funded by VCs
- Register your mobile device using Authy
- You can then buy bitcoins by transferring from a bank account (may take a few days to verify your bank account)

The Mechanics

Using Bitcoin:

Show Them the Money

So you've got some Bitcoin in a wallet such as Coinbase, here's what it takes to spend it at a restaurant or retailer:

- ◆ Find a store that accepts Bitcoin. Coinmap.org now lists 3,000 places, plus online retailers.
- ◆ Call ahead to make sure the store accepts Bitcoin.
- ◆ Don't freak out if prices are only listed in dollars. The store's app will do the conversion for you when you pay.
- ◆ When you're ready to pay, tell your server or cashier you want to pay in Bitcoin. The employee will show you a phone or tablet with a QR code on its screen.
- ◆ With an Android phone, use the Coinbase app. Click on the QR code icon to bring up your phone's camera and hold it over the restaurant's QR code. Confirm your payment amount.
- ◆ For iPhones, you have to log into Coinbase's mobile website. Click "send money." On the merchant's device, click the QR code or ask the merchant to click "view address." Manually type in the Bitcoin address.
- ◆ The store then receives confirmation of your payment on their device.

Wall Street Journal, February 18, 2014

Currency?

Traditionally two types of currency:

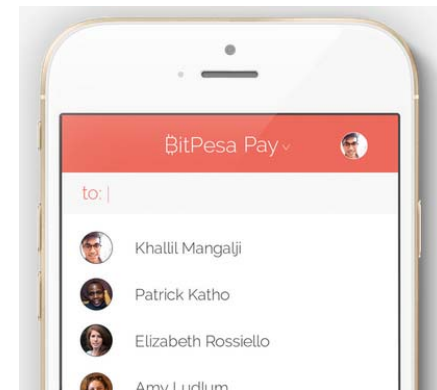
- Commodity: Has non-monetary use and is naturally scarce, e.g. gold, silver
- Fiat: No non-monetary use and scarce only by design, e.g. Federal Reserve's discretion
- Bitcoin: No non-monetary use and scarce by algorithm (reminiscent of Milton Friedman's computer controlled monetary rule)

See, George Selgin, "Synthetic Commodity Money", <http://ssrn.com/abstract=2000118>

Currency?

M-Pesa:

- Africans were transferring minutes to relatives and friends who were reselling the airtime
- Safaricom launched mobile phone-based payment system (deposit money stored in account on phone, send and withdraw it)
- 17 million users in Kenya alone
- 31% of Kenyan GDP flows through M-Pesa
- Different from Bitcoin because there is collateral but similar disruptive force for enabling transactions
- BitPesa now interfaces with M-Pesa



Currency?

M-Pesa:

- Many lessons from M-Pesa experience
- M-Kopa microcredit for a small solar panel



M-KOPA SOLAR

Currency?

M-Pesa:

- However, potentially we can learn from M-Pesa
- M-Kopa microcredit for a small solar panel



M-KOPA SOLAR

Currency?

M-Pesa:

- Kopo Kopo is like Bitpay
- M-Changa phone app to raise money for weddings and funerals
- UAP Group insurance for small farmers (crop failures compensated on mobile phone)



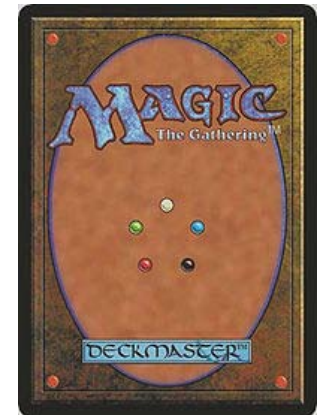
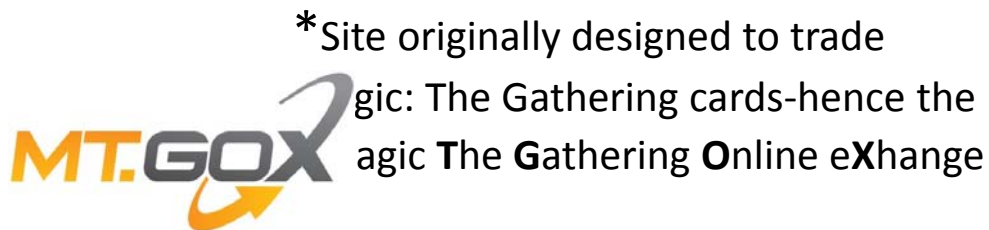
The Risks

- Uncollateralized fiat: Iraqi Swiss Dinar is a counter example.
- Confidence:
 - Could rules of the game change?
 - Could a competitive product dominate Bitcoin?
 - Could governments ban Bitcoin?
 - Could reputation for being used for illegal transactions damage confidence?
 - Given limited supply of bitcoins, could industries using Bitcoin fall into a deflation spiral

Some materials drawn from Reuben Grinberg, 2011, "[Bitcoin: An Innovative Alternative Digital Currency](#)"

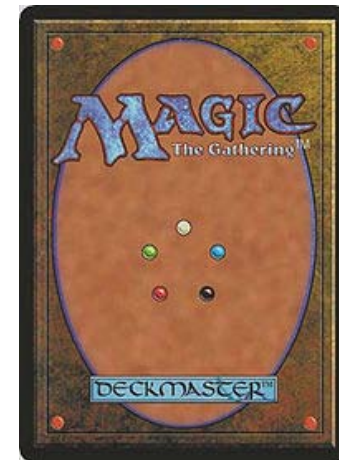
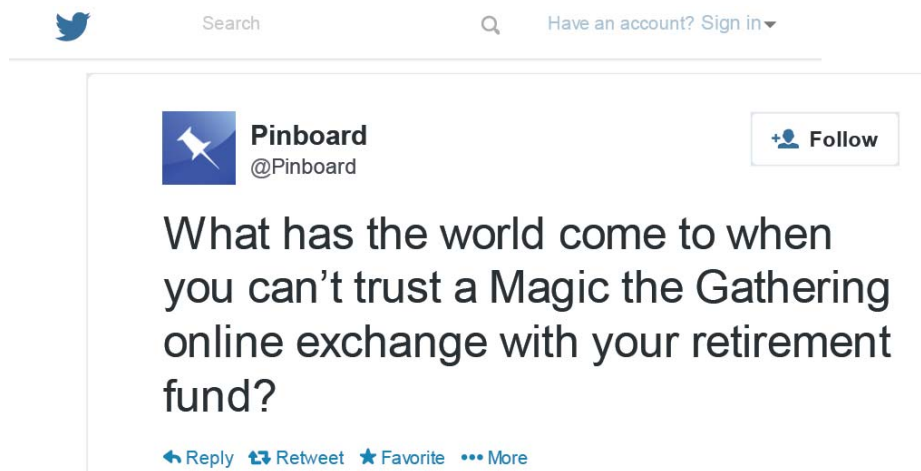
The Risks

- Technology:
 - Anonymity Failure (mainly due to people posting their on-line public keys and repeatedly using the same key)
 - Flaws in code
 - DoS. It is possible that a mining pool could turn against Bitcoin
 - Theft (stored on computer or mobile device which is subject theft). Mt. Gox* hacked in June 2011 where 25,000 bitcoins were stolen. The price went from \$17.50 to \$0.01 in one hour after the stolen bitcoins were dumped on the market (note the only seller at the price point was the hacker!)



The Risks

- Technology:
 - Mt. Gox II. On February 24, 2014, the site shut down with 850,000 bitcoins “missing”



The Risks

- Technology:
 - Bitstamp.net different. On January 4, 2015, the site shut down with some wallets compromised and 19,000 bitcoins “missing”
 - During shut down time, they implemented new hardware, Bitgo multi-signature, and Amazon cloud
 - All bitcoins guaranteed
 - They had “cold storage” backup

The logo for Bitstamp, featuring the word "BITSTAMP" in a sans-serif font. The "BIT" is in green and "STAMP" is in grey.

The Risks

- Technology:
 - Take over 50% of mining
 - Even if you do, what are you going to put in the block? Perhaps a bunch of non-transactions?
 - Block chain would fork and ignore the new block
 - Nevertheless, a 50% attack would cause problems

The Risks

- Legal:
 - *Stamp Payments Act* (1862) – makes U.S. government monopolist in issuing currency. But Act very old, last opinion in 1898 and digital currencies have been around for over a decade
 - *Liberty Dollars* case (2011). Founder issuing coins and notes backed by gold, silver and other precious metals. Not applicable to Bitcoin because there is no metal coin or note that resembles US or foreign currency
 - *Securities Act* (1933). Bitcoin does not look like a security because no enterprise is trying to raise money. In addition, it does not pay any dividend.
 - *Money Laundering Control Act* (1986). Biggest threat!

More details in Reuben Grinberg, 2011, "[Bitcoin: An Innovative Alternative Digital Currency](#)"

The Risks

- Regulatory:
 - Russian Central Bank, [January 27, 2014](#).

On the use in transactions "virtual currency", in particular, Bitcoin

...The Bank of Russia warns citizens and legal entities, primarily credit institutions and non-credit financial institutions, the use of "virtual currency" for them in exchange for goods (works, services) or cash in rubles and foreign currency.

According to article 27 of the Federal Law "On the Central Bank of the Russian Federation (Bank of Russia)" issue in the Russian Federation monetary surrogates prohibited.

...

The Bank of Russia has warned that Russian legal entities providing services for the exchange of "virtual currency" in rubles and foreign currency, as well as for goods (works, services) will be considered as a potential involvement in the implementation of suspicious transactions in accordance with the legislation on counteraction to legalization (laundering) proceeds of crime and financing of terrorism.

FT February 9, 2014. "Russian authorities are preparing to crack down on Bitcoin and have warned that those who use "crypto-currencies" are breaking the law..."

The Risks

- Regulatory:

- India, RBI, December 24, 2013

Issued advisory that prompted some Indian bitcoin traders to suspend their operations, even as regulators seek clarity on digital currencies and ways to regulate them. The RBI's worries include taxation, security risks, losses due to the volatility and money laundering.

While regulators have not deemed virtual currencies illegal, India's law enforcement agency, the Enforcement Directorate, raided the offices of a few companies that operate bitcoin trading websites.

The Risks

- Regulatory:
 - China, December 6, 2013
 - The People's Bank of China said financial institutions and payment companies cannot provide pricing in Bitcoin, buy and sell the virtual currency, or insure Bitcoin-linked products.
 - January 8, 2014 Alibaba bans Bitcoin

The Risks

- Regulatory:
 - [U.S. Federal Reserve Chairman Bernanke, September 6, 2013](#)
 - “Federal Reserve monitors virtual currencies and other payments system innovations, it does not necessarily have authority to directly supervise or regulate.”
 - “... while these types of innovations [digital currencies] may pose risks related to law enforcement and supervisory matters, there are also areas in which they may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system”

The Risks

- Regulatory:
 - [U.S. Internal Revenue Service, March 31, 2014](#)
 - Bitcoin should be treated as “property” and any capital gain is taxable
- This means if you bought a coin for \$100 but it appreciated to \$500, you are taxed on the capital gain
- Positive is that bitcoin is officially recognized and treated no differently than if I bought Euros or Yen to speculate on appreciation
- Negative is that it adds complexity. However, given the algorithmic nature of bitcoin, it is relatively simple to calculate all of the tax reporting.

The Risks

- Regulatory:

The biggest risk is Anti-Money Laundering (ALM)

Case study is E-gold

- Founded in 1996, users could open an account based in gold or other precious metals
- You could make instant transfers to other E-gold accounts
- 5 million users by 2009

The Risks

- Regulatory:

The biggest risk is Anti-Money Laundering (ALM)

Case study is E-gold

- Charged with illegally transmitting money
- E-gold showed up as a common method in a number of criminal investigations
- Founder found guilty of money laundering
- Sentence was lenient because judge realized that the founders did not intend to engage in criminal activity

The Risks

- Regulatory:

The biggest risk is Anti-Money Laundering (ALM)

Case study is E-gold

- Emphasizes the greatest risk is ALM
- Solution for companies using bitcoin is to have a clear KYC policy (Know Your Customer)
- In the U.S., it is also important to have state-specific money transmitting licenses

Dogecoin

Case study

- Doge is a famous meme. The word is originally used in Homestar Runner puppet show June 24, 2005
- Homestar calls Strong Bad his “doge” when trying to distract his work on “3rd quarter projections”
- See:
 - http://www.youtube.com/watch?feature=player_embedded&v=tLSgRzCAtXA



Strong Bad a.k.a. Doge

Dogecoin

Case study

- February 23, 2010 Japanese teacher posted photos of her dog



Dogecoin

Case study

- Turns into meme in 2012



Dogecoin

Case study













- December 6, 2013 Dogecoin introduced



Dogecoin

Case study

- Higher number of coins – capped at 100 billion and encourages new breed of mining technology
- Initial coin supply 7 billion
- December 14, 2013 value was \$400.80 per dogecoin

#	Name	Market Cap	Price	Total Supply	% Change (24h)	Market Cap Graph (7d)
1	 DogeCoin	\$ 2,842,549,645,462	\$ 400.80	7,092,187,181 DOGE	+88286715.40 %	
2	 Bitcoin	\$ 9,780,577,688	\$ 806.23	12,131,250 BTC	-6.81 %	
3	 Litecoin	\$ 697,469,784	\$ 29.06	24,003,892 LTC	-6.28 %	
4	 Peercoin	\$ 85,191,140	\$ 4.07	20,923,970 PPC	-7.55 %	
5	 Namecoin	\$ 39,232,217	\$ 5.23	7,497,892 NMC	-10.59 %	
6	 Quark	\$ 38,502,363	\$ 0.16	246,405,841 QRK	-2.42 %	

Dogecoin

Case study

- December 14, 2013 value was \$400.80 per dogecoin

Dogecoin

Case study

- December 14, 2013 value was \$400.80 per dogecoin
- December 15, 2013 value was \$0.0002 per dogecoin
- January 14, 2016 value was \$0.000176 per dogecoin (#6 on coinmarketcap.com)

Camcoin

What your own altcoin? [Coingen.io](https://ssrn.com/abstract=2438299)

Coingen

Build a New Coin

Check Status

Basic Information

Details

Advanced Settings

Coin Name (one word, case is ignored)

Camcoin

Coin Abbreviation (exactly three letters, eg BTC)

CAM

Coin Icon (256x256)

Choose File

No file chosen

☒ Remove Coingen branding on splash screen (0.10 BTC)

☒ Include source (+0.05 BTC)

☒ Do not display my coin on the public status page (I understand that if I lose my private link, I will lose access to my coin).

Details

Proof of Work Algorithm

SHA256 (like Bitcoin)

Block Rate (in seconds)

600

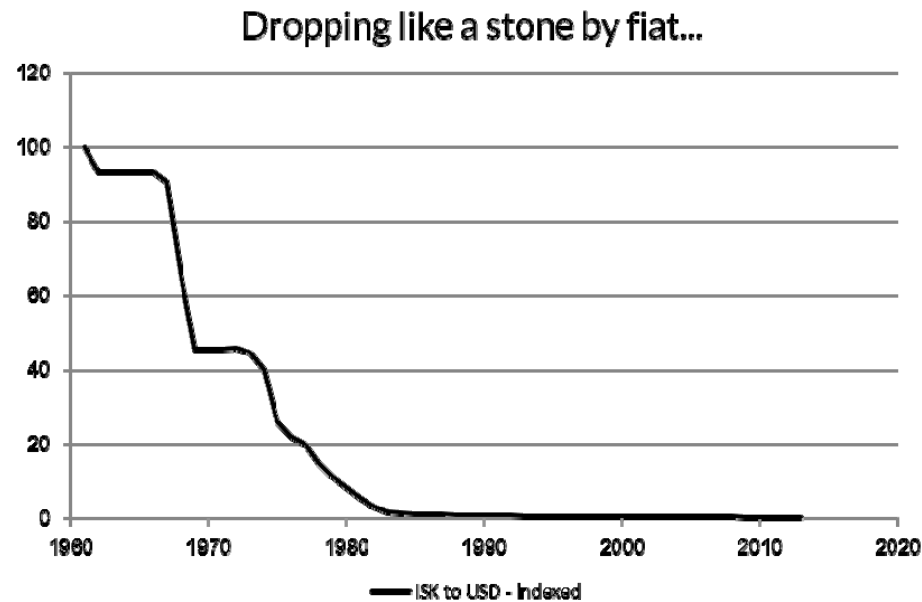
Camcoin

However,....

- Most of the altcoins have no or almost no mining power.
- Keep in mind that their protection from double-spends only exists as long as they have enough mining power.
- Given the small mining power, there are many individuals that could easily double-spend or cause damage to their network.

Auroracoin

Iceland fed up with fiat currency. Krona has lost 99.5% of its value versus USD since 1960.



Auroracoin

Auroracoin is 50% “premined”

- March 25, 2014 coins were “airdropped” to every citizen of Iceland (31.8 coins each)



Auroracoin

Auroracoin is 50% “premined”

- March 25, 2014 coins were “airdropped” to every citizen of Iceland (31.8 coins each)



...But very little mining.
As a result, it was
attacked and failed.
Today the dropped
31.8 coins are worth
about \$0.63.

The Controversy



The Conscience of a Liberal
PAUL KRUGMAN

DECEMBER 28, 2013, 2:35 PM

Bitcoin Is Evil

WCEG | Washington Center for
Equitable Growth

Watching Bitcoin, Dogecoin, Etc...

By [Brad DeLong](#) | December 28, 2013, 1:24
pm

The Controversy

Con

- Fiat money without any backing
- USD is also fiat money – but USD is legal tender for all transactions in the US and it is backed by a government that has the ability to tax and incarcerate if you don't pay your taxes
- Gold has been around for thousands of years. It has some industrial uses. It also has uses in art and jewelry. Gold has lower bound (fundamental usefulness and upper bound, as it rises in value, new technologies will be discovered to mine more – asteroids!!)
- Potential to disintermediate central banks

The Controversy

Con

- Encourages construction of special technology to mine bitcoins and a bitcoin arms race.



SP35 Yukon Power Shipping from Stock

5.5TH/s Coin Miner, \$2,235.00

Application-specific integrated circuit, or ASIC, is a microchip designed for specific purpose

The Controversy

Con

- Encourages construction of special technology to mine bitcoins and a bitcoin arms race.



1.2TH/s Coin Miner, \$5,599.00

Buyer Beware!!

Dear AMT customers/clients/followers.

We write to inform you that due to the pending class action, Lenell et al. v. Advanced Mining Technology, Inc., No. 14-cv-01924 (E.D.Pa.), we will no longer be communicating on the Bitcoin Talk Forum per the advice of our attorneys. We are still working towards resolving all outstanding customer complaints in conjunction with our counsel. Please note that customers may still contact us directly to discuss issues with their orders, but we will be unable to use the forum as a means of communication regarding specific orders or the pending litigation. You may contact us by phone at 855-866-6463 or by email at josh@advancedminers.com. We will still handle Individual communications regarding orders within the ordinary course of business.

The Controversy

Con

- Will not replace credit cards because these cards provide “credit” as well as transactions
- Similar point for banks
- Currently, there is no way to earn interest
- What will happen when there are no bitcoins to pay the miners?
- Mining is a risky business (depends on value of Bitcoin and subject to technological shocks)

The Controversy

Con

- Decentralized nature of Bitcoin both an advantage and a disadvantage
- The decentralization makes changes in model difficult and it is unlikely that the founder got it right in 2009
- Some new crypto-currencies address specific issues
 - Example, Ripple, XRP, requires a minimum balance, an account reserve, (to discourage DDoS-like behavior)

The Controversy

Con

- There is no downside protection, no collateral
- The value is what people think it is worth
- These are the ingredients of a classic bubble!

The Controversy

Pro

- Holding bitcoins as a store of value focuses on only one part of Bitcoin
- bitcoin is an application of Bitcoin
- It is true a telephone handset has no value without a network. Bitcoin is the network and bitcoin is the handset.

The Controversy

Pro

- While the number of new bitcoins will go to zero, there will still be an incentive for mining via small transactions fees
- These fees exist today (you can pay a fee for faster verification)
- Fees controversial. Not clear they are needed because certain third parties, like merchants might support the miners

The Controversy

Pro

- The hash searching is not a frivolous use of computing time
- The more difficult it is to find the hash the more unlikely it is that Bitcoin can be double spent. That is, the computing difficulty ensures no double spending.
- Currently the Bitcoin network has the computing power of 50,000 of the world's fastest super-computers (4,300 exaFLOPS, compared to Tianhe-2 which has 0.03 exaFLOPS)
- Obviously hard to mount a takeover.

The Controversy

Pro

- Internet is an example of long-term value creation through network efficiency. The core innovation was a way to efficiently disseminate data over a network – far cheaper and faster than in the past.
- Bitcoin's core innovation is the ability to publicly verify ownership, instantly transfer that ownership, and to do that without any trusted third party. Bitcoin reduces the cost of transferring ownership.
- Bitcoin solves a fundamental gap in the Internet – the direct transfer of ownership

The Controversy

Pro

- It is true that there is no floor on the value of a bitcoin. The bitcoin will only be valuable if it is an efficient method for transferring ownership
- What is the value of Bitcoin?
 - Valuing bitcoin is difficult. One proposed approach is to determine the amount of savings. Given the volume of transactions, we could approximate the savings on, say transactions fees.
 - Suppose on average a bitcoin is used 20 times a year and the average transaction size is \$100 (hence \$2,000 of turnover)
 - Assume that the average savings of eliminating the third party is 3% per transaction.
 - That amounts to \$60 per year on average
 - However, this is all very rough. The difficulty in establishing a value has likely contributed to bitcoin's extreme volatility.

The Controversy

Pro

- It is true that there is no floor on the value of a bitcoin. The bitcoin will only be valuable if it is an efficient method for transferring ownership
- What is the value of Bitcoin?
 - Alternative method to value bitcoin would be to answer the question: how much would it cost to acquire 10% of the computing power of the network?
 - You could calculate how many bitcoins you would win over the period before the computer power become obsolete.
 - The bitcoin should not be worth less or people will not invest in mining.

The Controversy

Pro

- Is the current consumer/commercial payment system just one part of Bitcoin?
- Is bitcoin the equivalent to the initial application of the Internet, email?
- For example, could this technology eventually touch stocks, bonds, futures, options? That would be a big deal.
- Think of using the Bitcoin ledger as verifying ownership of physical items – with your key, you can start your car or open your house. It could be “an independent, secure and reliable host of financial and personal information.” [WSJ, February 18, 2014]

The Controversy

Pro

- Value of Bitcoin is derived from what it allows.
- 3% savings on a transaction is likely very conservative. Think of all of the money that is spent verifying transactions and dealing with third parties, whether at a corporation or a bank.

The Controversy

Pro

- Why not just use a debit card?
- Answer: Cost of Fraud. Surprisingly large charge backs in the US – and even higher outside the US
 - Debit purchases made by children are one of the main source of charge backs!

The Quotes

Ajay Banga, CEO Mastercard

- “The world is not short of currencies, so what is this currency solving for?”
February 17, 2014
- 2015. Mastercard recognizes digital currency as a material risk in 10K filing.

The Quotes

Meyer Malka, Ribbit Capital (VC firm backing bitcoin startups)

- “[Bitcoin] is the most disruptive thing I have seen in financial services in my lifetime.” February 17, 2014

Bitcoin beyond bitcoin

Bitcoin network can be used for “distributed contracts” via the blockchain

- Allows problems to be solved in a way that minimizes trust
- Human judgment is taken out of the loop
- Secure, private, and common knowledge

*See Nick Szabo, “Formalizing and Securing Relationships on Public Networks,
<http://szabo.best.vwh.net/formalize.html>

Bitcoin beyond bitcoin

Distributed Autonomous Corporations (DACs) or Decentralized Autonomous Corporations where a currency is backed by the services its miners perform – rather than real world commodities.



*See Stan Larimer, “Bitcoin and the Three Laws of Robotics” at http://letstalkbitcoin.com/bitcoin-and-the-three-laws-of-robotics/#.U0MCk_nCBGP

Bitcoin beyond bitcoin

DACs:

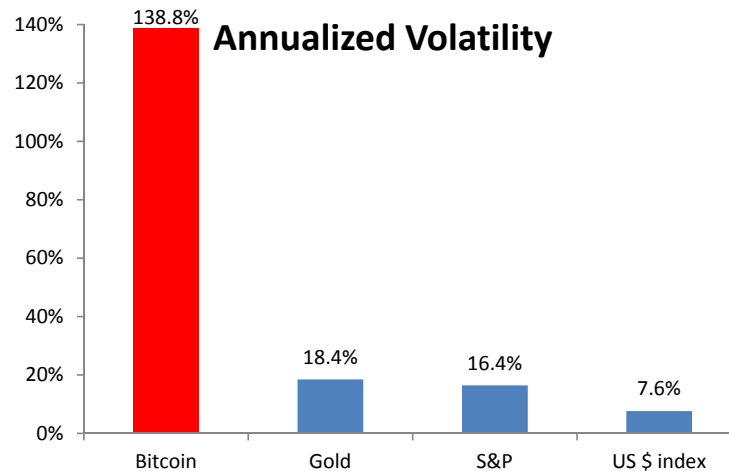
- **Corporations** – They are free and independent persons.
- **Autonomous** – once up to speed; they no longer need (or heed) their creators.
- **Distributed** – there are no central points of control or failure that can be attacked.
- **Transparent** – their books and business rules are auditable by all.
- **Confidential** – customer information is securely (and incorruptibly) protected.
- **Trustworthy** – because no interaction with them depends on trust.
- **Fiduciaries** – acting solely in their customers' and shareholders' interests.
- **Self-regulating** – they obey their own rules like, well, robots.
- **Incorruptible** – no one can exercise seductive or coercive influence over them.
- **Sovereign** – over their digital resources. They don't need governments to exist.

Bitcoin could be viewed as an early form of a DAC!

*See <http://invictus-innovations.com/i-dac/>

Too Volatile

Practically, it is too volatile to hold as store of value being 20x more volatile than USD



- Daily 95% confidence interval is +/- 10%
- 13 “Black Monday” like crashes (-20%) in last five years

Too Volatile

Currently bitcoin fails as a store of value:

- But bitcoin offers more than the “store of value”. Indeed, most merchants immediately translate their bitcoin into USD or other currencies
- More importantly, we care about tomorrow, not today.
- The key issue is:
 - Is the high volatility a result of lack of liquidity?
 - Is the high volatility a result of lack of collateral?

My Opinion

- Is Bitcoin just a classic bubble?
- Alternatively, is Bitcoin an innovative, disruptive new technology that could be the next big thing?

My Opinion

- Is Bitcoin just a classic bubble?
- Alternatively, is Bitcoin an innovative, disruptive new technology that could be the next big thing?

Bitcoin or any other cryptocurrency is a bubble – just like any fiat currency. Bitcoin has value because people find it useful and believe it has value. The key innovation is the blockchain. There are many types of blockchain with the strongest being the Bitcoin blockchain. Finance is the low hanging fruit – ripe for disruption by blockchain technology.

Postscript

Posted by Izzy Kaminska, Financial Times

<http://www.youtube.com/watch?v=hFHT5g75tZM&feature=youtu.be>

Conan O'Brien's take on bitcoin

<https://www.youtube.com/watch?v=Vd19SboRhVY>

FAQ

How did Bitcoin get started? If coins are awarded to mine, you need transactions to mine – but at the beginning there were no coins to pay for transactions?

- There is a 'genesis block' or a non-block. This includes an endowment.
- Block 1 contains a single transaction which is an award of 50 bitcoins to a miner (but not for any work). This is the genesis.

Do I need to wait 10 minutes to do any transaction (the time it takes to create a block)?

- No. The proposed transaction is broadcast to the network which includes miners and non-miners. The blockchain is consulted plus the 'memory pool' (those transactions not yet in the blockchain) to verify you have the bitcoin to spend.

FAQ

The SHA-256 hash has $2^{256}-1$ different outputs. However, you should be able to get a collision with just one more possible input, i.e. the $2^{256\text{th}}$ must cause a collision.

- “One of the consequences of the second law of thermodynamics is that a certain amount of energy is necessary to represent information. To record a single bit by changing the state of a system requires an amount of energy no less than kT , where T is the absolute temperature of the system and k is the Boltzman constant. (Stick with me; the physics lesson is almost over.)
- Given that $k = 1.38 \times 10^{-16}$ erg/°Kelvin, and that the ambient temperature of the universe is 3.2°Kelvin, an ideal computer running at 3.2°K would consume 4.4×10^{-16} ergs every time it set or cleared a bit. To run a computer any colder than the cosmic background radiation would require extra energy to run a heat pump.
- Now, the annual energy output of our sun is about 1.21×10^{41} ergs. This is enough to power about 2.7×10^{56} single bit changes on our ideal computer; enough state changes to put a 187-bit counter through all its values [i.e. $2.7 \times 10^{56} = 2^{187}$]. If we built a Dyson sphere around the sun and captured all its energy for 32 years, without any loss, we could power a computer to count up to 2^{192} [i.e. $32 \times 2.7 \times 10^{56} = 2^{192}$]. Of course, it wouldn't have the energy left over to perform any useful calculations with this counter.
- But that's just one star, and a measly one at that. A typical supernova releases something like 10^{51} ergs. (About a hundred times as much energy would be released in the form of neutrinos, but let them go for now.) If all of this energy could be channeled into a single orgy of computation, a 219-bit counter could be cycled through all of its states [i.e. 2^{219}].
- These numbers have nothing to do with the technology of the devices; they are the maximums that thermodynamics will allow. And they strongly imply that brute-force attacks against 256-bit keys will be infeasible until computers are built from something other than matter and occupy something other than space.
- ...Even a mythical quantum computer won't be able to brute-force that large a keyspace.”

From Bruce Schneier https://www.schneier.com/blog/archives/2009/09/the_doghouse_cr.html [my brackets]

Glossary

- BTC. Short-form for bitcoin
- Satoshi. Smallest bitcoin unit. 100,000,000 satoshi=1 bitcoin
- Hash. One way function that masks a message. SHA-256 is most popular.
- Collision. Two different inputs provide the same hash.
- To be completed!!

Reading

- Velde, Francois R., 2013. “Bitcoin: A primer” [Chicago Fed Letter](#).
- Perry, David, 2012. “[Explaining Bitcoin](#)”
- Larimer, Stan, 2014. “[Bitcoin and the Three Laws of Robotics](#)”
- Yang, Edward Z. “[The Cryptography of Bitcoin](#)”
- Reid, Fergal and Martin Herigan, 2013, [An Analysis of Anonymity in the Bitcoin System](#)
- Bitcoin wiki. [https://en.bitcoin.it/wiki/Main Page](https://en.bitcoin.it/wiki/Main_Page)
- Szabo, Nick. “[Formalizing and Securing Relationships on Public Networks](#)”
- Wheeler, Brad, 2014. “Bitcoin: What is it?”

Appendix: Rational Bubbles

Classic 1982 paper by Blanchard and Watson*

- Each period a bubble persists with probability p and bursts with probability $(1-p)$
- If the bubble continues, its price has to grow in expectation at the rate $(1+r)/p$, where r =interest rate
- If bubble bursts, price=0
- Expected return of the bubble is the risk free rate
- Risk neutral agents will play
- For small bets, agents are risk neutral or even risk loving
- Given Bitcoin is relatively small (\$6 billion) relative to the size of the economy, a speculative bubble can occur

*http://www.nber.org/papers/w0945.pdf?new_window=1

Above summary by David Hsieh

WSJ Debate

Con: says Bitcoins are a commodity, not financial instruments. Their value fluctuates widely in line with views regarding the usefulness of the bitcoin payment system—and the speculative manias surrounding those views.

Harvey: Bitcoin is not a commodity like gold. Bitcoin is not a fiat currency like the Euro. Bitcoin is a unit of account that is not backed by any central authority. Bitcoin exists because it solves problems and users assign value to it. This is not without historical precedent. After the first Gulf War, a currency was used in the Kurdish areas of Iraq called the Iraqi Swiss dinar (the printing plates were made in Switzerland). The currency was widely accepted although it was not legal tender and it was backed by no one. The legal tender was Saddam dinars. Again, it is possible to have a unit of account that is not backed by either a commodity or a government - as long as people are willing to accept it.

WSJ Debate

Con says bitcoins violate the basic rules of finance. There is no issuer, and thus no guarantor of its value, or promise to pay face value, the way there is with a traditional currency. Circulation at par, he says, is central to the stability of the entire financial system.

Harvey: Many argue that bitcoins “violate basic rules of finance” because there is “no issuer, and thus no guarantor of its value... the way there is with a traditional currency”. However, this argument is problematic on many dimensions. First, governments do not “guarantee” stability of the value of their currencies – recent examples are the ruble, the Swiss franc and the hryvnia. Second, the supply of bitcoin is determined by an algorithm – not a central bank. It is true that bitcoin is much more volatile than traditional currencies at this point in time. Much of this volatility is due to illiquidity – which is not unexpected given that the technology is so nascent. Recent innovations, such as a U.S.-based exchange that is regulated in the U.S., insured, and backed by the NYSE should add to liquidity and reduce volatility.

WSJ Debate

Con says bitcoins are completely impractical for use in servicing of debt. The fair price of bitcoins as measured by the discounted value of future cash flows is zero.

Harvey: Some argue that the “fair price of bitcoins as measured by the discounted value of future cash flows is zero”. This is not an argument against bitcoin but against any fiat currency. U.S. dollars are liabilities of the Federal Reserve Bank – yet no interest is charged. You lose money when you hold cash. This does not deter people from holding cash.

Harvey: Others argue that “bitcoins are completely impractical for use in servicing debt”. This does not make any sense. If the debt is in U.S. dollars, you can service the debt in bitcoin by translating the bitcoin into U.S. dollars at the prevailing rate. Currently, there is not much borrowing/lending going on the bitcoin space. However, a number of firms have entered this market. I doubt this market will grow for a very simple lesson from international finance. Suppose I notice that I can borrow a lot cheaper in Germany than I can in the U.S. (as is the case today). If I do that, I must pay back Euros in the future. However, if my revenues are in U.S. dollars and if the exchange rate fluctuates against me, then I might have to pay back much more than I borrowed. The same holds with bitcoin. If your revenues are in U.S. dollars, it is risky to take a loan in bitcoin. As more revenue sources arise in bitcoin, there will be increased borrowing/lending in bitcoin.

WSJ Debate

Lastly, Con says that with real currencies and banking systems, underwriting in the case of bank deposits, and budgetary procedures as well as monetary policy operations in the case of central bank instruments, put limits on the creation—and ability to acquire—currency. The bitcoin payment system doesn't do any of those things. He says the financial crisis of 2008-09, the collapse of Lehman etc., is what happens when underwriting falls apart.

Harvey: It is true that if bitcoin ended up being the world currency that there would be little or no role for central banks. There would be no monetary policy. There would be no QE operations. Would that increase the chance of another great recession – or a depression? Probably not. Central banks allowed commercial banks to take on extreme leverage before the global financial crisis. With \$2.50 in capital, you could borrow \$100. If markets moved 2.5% against you, you were wiped out and in need of a bailout. So much of what happened during the global financial crisis can be linked to flaws in the regulatory environment. Such extreme leverage is unlikely in a bitcoin world.

Harvey: In a future bitcoin world, you can imagine bitcoin banks with different fractional reserves. One bank might simply be bank that pays no interest and does not lend out your bitcoin. Another bank might offer a small interest payment and lend out only 25% of deposits (75% reserve ratio). Yet another might offer a higher interest rate but have a much lower reserve ratio. The banks would be transparent about the exact reserve ratios. Any borrowing by banks would be transparent too. No matter what, the reserves ratios would be much larger than the U.S. dollar banks. Remember, that within a few minutes you can transfer all of your funds from one bank to another with bitcoin. With traditional banks, this might take more than one day.