Innovation and Cryptoventures

Transaction Mechanics

Campbell R. Harvey

Duke University, NBER and
Investment Strategy Advisor, Man Group, plc

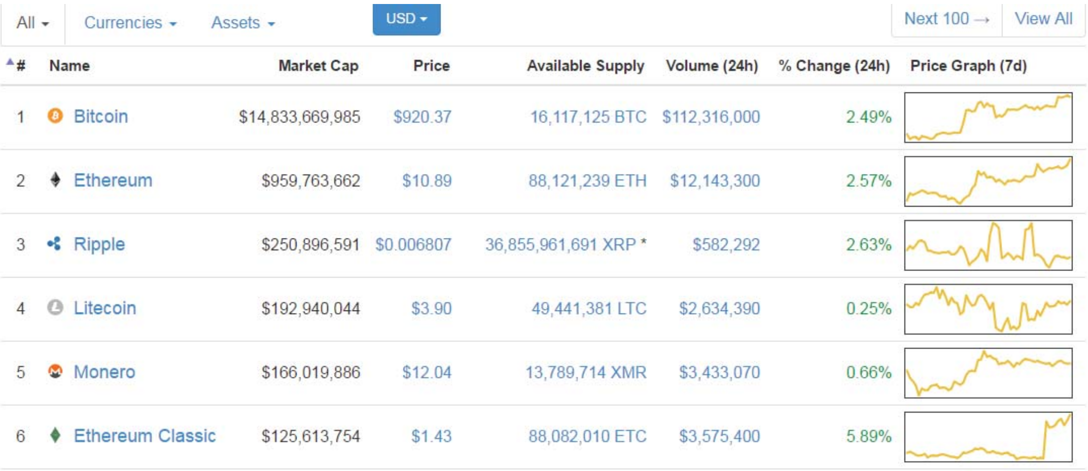
January 21, 2017

The Landscape

http://coinmarketcap.com/

- Bitcoin is the leader (approximate $13 billion in market capitalization) founded in 2009
- Ethereum is #2 with $0.9 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).

January 21, 2017 3:25pm



#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$14,833,669,985	$920.37	16,117,125 BTC	$112,316,000	2.49%	
2	Ethereum	$959,763,662	$10.89	88,121,239 ETH	$12,143,300	2.57%	
3	Ripple	$250,896,591	$0.006807	36,855,961,691 XRP *	$582,292	2.63%	
4	Litecoin	$192,940,044	$3.90	49,441,381 LTC	$2,634,390	0.25%	
5	Monero	$166,019,886	$12.04	13,789,714 XMR	$3,433,070	0.66%	
6	Ethereum Classic	$125,613,754	$1.43	88,082,010 ETC	$3,575,400	5.89%	

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.

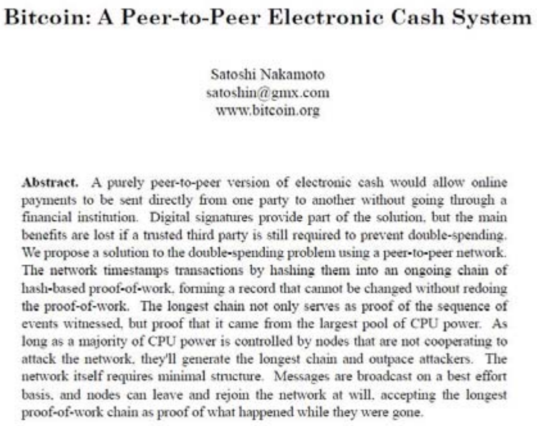
The Innovation

- Cypto-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 a "blockchain" (more later)

The Founder



Bitcoin: A Peer-to-Peer Electronic Cash System

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

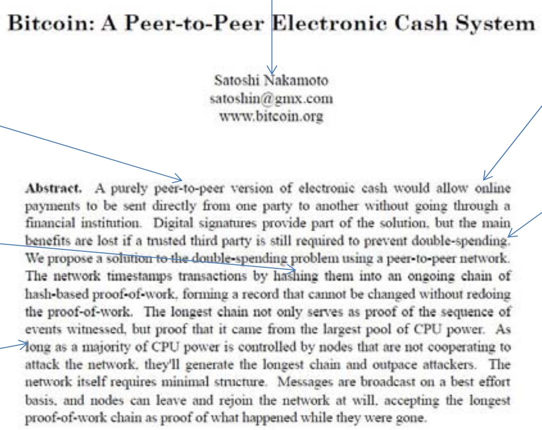
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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 on Internet November 2008

The Founder

Craig, Dorian or Nick Szabo?



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.

Electronic payment system

P2P

No double spending

Secure via hash

Warning about majority of computing power

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
- Core development team maintains the reference client Bitcoin-QT (GUI) / bitcoind
- There is are many competing proposals for the future of bitcoin – yet no centralized authority to decide on which one is the best

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

Competing Client Proposals

Bitcoin Classic:
Official Website: https://www.bitcoinclassic.com
Official Subreddit: https://www.reddit.com/r/bitcoin_classic
Official Github: https://github.com/bitcoinclassic/bitcoinclassic
Bitcoin Unlimited:
Official Website: http://www.bitcoinunlimited.info
Official Subreddit: https://www.reddit.com/r/bitcoin_unlimited
Official Github: https://github.com/gandrewstone/BitcoinUnlimited
Bitcoin XT:
Official Website: https://bitcoinxt.software
Official Subreddit: https://www.reddit.com/r/bitcoinxt
Official Github: https://github.com/bitcoinxt/bitcoinxt
Bitcoin Core:
Official Website: https://bitcoincore.org
Official Subreddit?: https://www.reddit.com/r/bitcoin
Official Github: https://github.com/bitcoin/bitcoin
The above list is not comprehensive and lists clients/proposals that seem to be being discussed/questioned most atm.

Genesis

- The network was "started" January 3, 2009 with the Genesis Block
- Bitcoin v0.1 was released January 9, 2009
- Latest version is v0.13.2 released January 3, 2017

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

Foundation/MIT Digital Currency Initiative

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

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

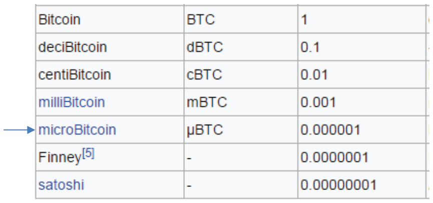
- Mike Hearn (senior developer) calls bitcoin a "failed project"

https://www.theguardian.com/technology/2016/jan/15/mike-hearn-senior-bitcoin-developer-says-currency-failed-experiment

The Mechanics

How does it work?*

- Currently, 12.5 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



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

Called "bits" → microBitcoin

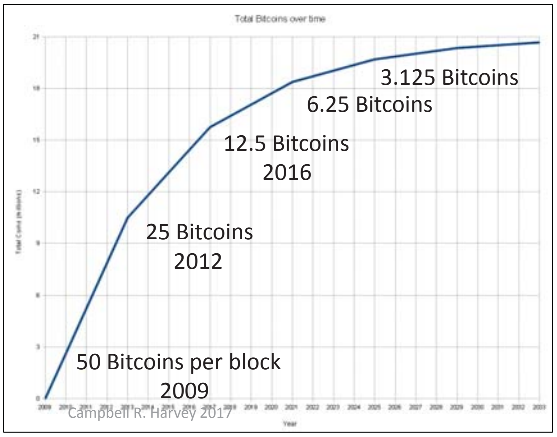
https://en.bitcoin.it/wiki/Units

*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

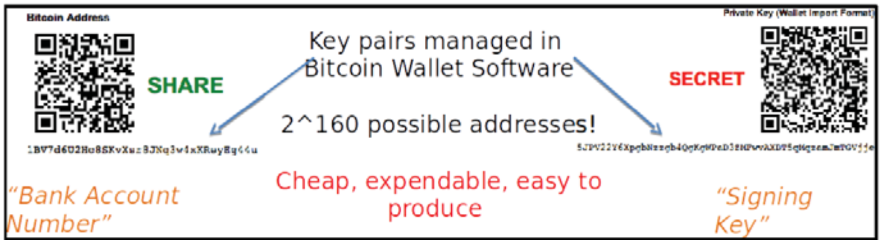
Bitcoin accounts?

- 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

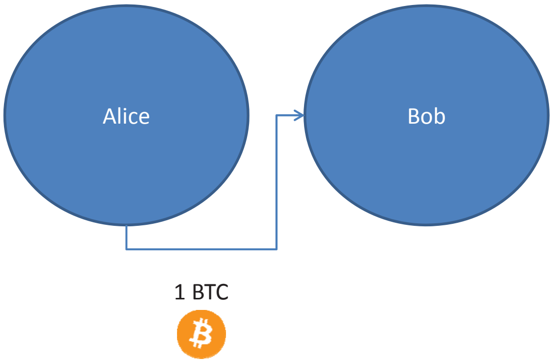
Bitcoin basics

- 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


Bitcoin Address
SHARE
1BV7d6U2Hu8SKvXuz8JNq3w4xXRuyEq44u
Key pairs managed in Bitcoin Wallet Software
2^160 possible addresses!
Private Key (Wallet Import Format)
SECRET
"Bank Account Number"
Cheap, expendable, easy to produce
"Signing Key"

The Mechanics

Simplified example:
Alice buys something from Bob and sends him 1 bitcoin



The Mechanics

Examples: Alice 1 BTC → Bob

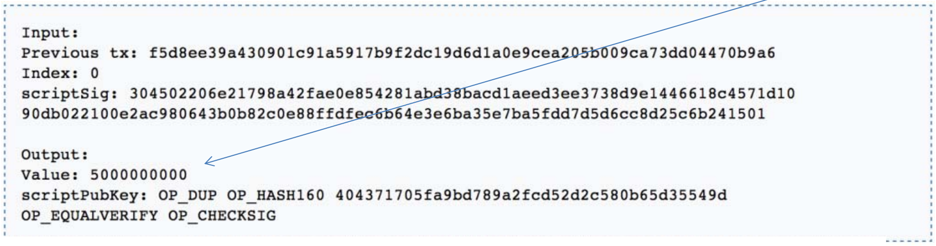
- Bob sets up a digital (public) address and sends it to Alice
- Like email account with password – except it (should) changes for every transaction.
- Alice adds Bob's address and the amount of bitcoins to a 'transaction' message.
- Alice signs the transaction (more later on this!)
- Alice broadcasts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

The Mechanics

Examples

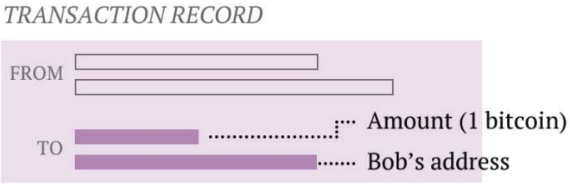
- Alice sends to Bob

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
```

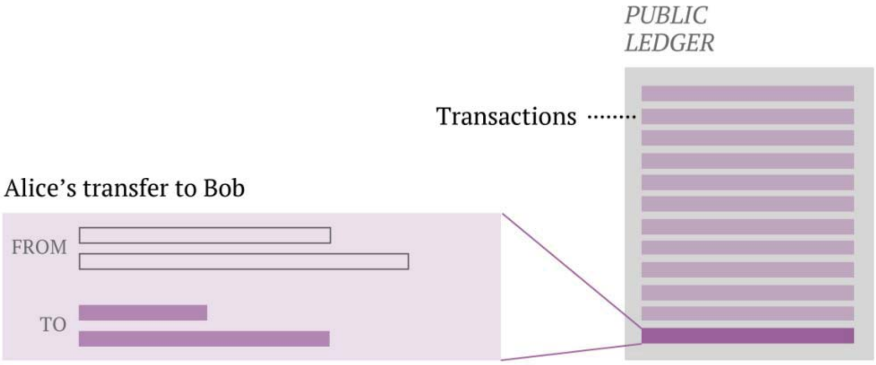


Graphics from King, Williams and Yanofsky (2013)

The Mechanics

Examples

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

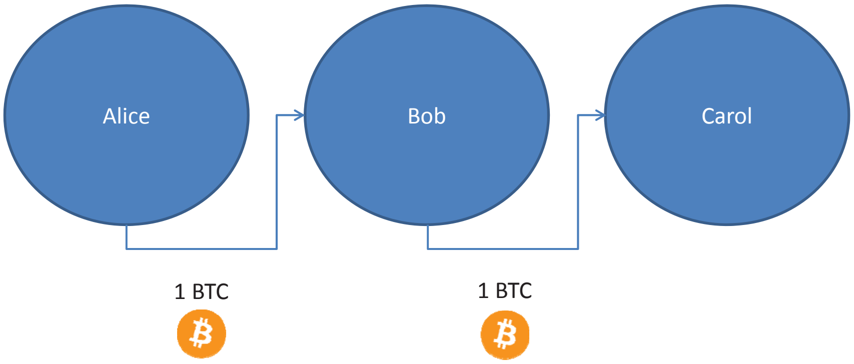


Graphics from King, Williams and Yanofsky (2013)

The Mechanics

Examples continue:

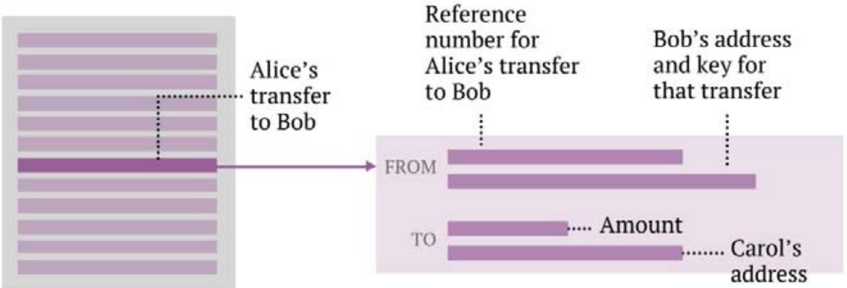
Bob buys something from Carol and sends her 1 bitcoin



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

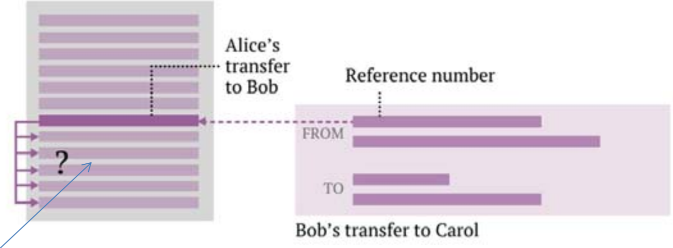

Alice's transfer to Bob
Reference number for Alice's transfer to Bob
Bob's address and key for that transfer
FROM
TO
Amount
Carol's address

Graphics from King, Williams and Yanofsky (2013)

The Mechanics

Examples

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



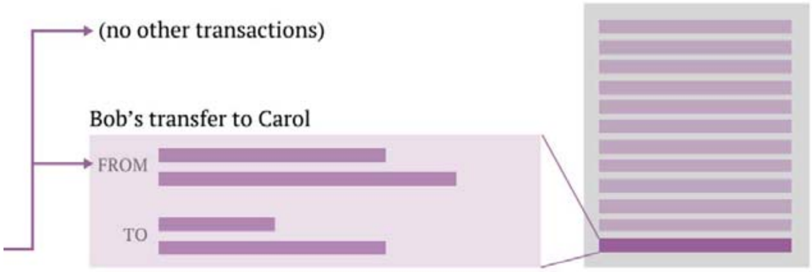
Other transactions that have occurred since Alice's original transfer to Bob

Graphics from King, Williams and Yanofsky (2013)

The Mechanics

Examples

- If transaction validated, then added to the ledger

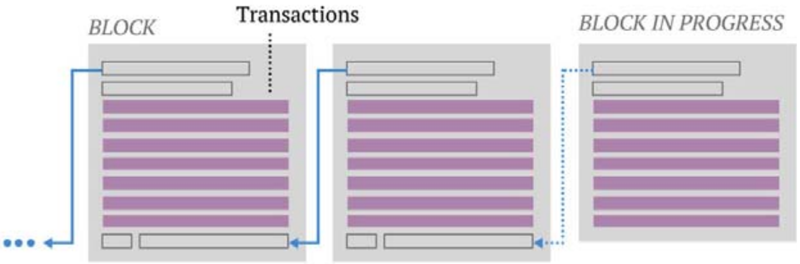


Graphics from King, Williams and Yanofsky (2013)

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 a "blockchain"

Graphics from King, Williams and Yanofsky (2013)

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
- Current size of blockchain is 90gb
- Updates are provided by the system of miners

https://blockchain.info/charts/blocks-size

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

- 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 the board worth?

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

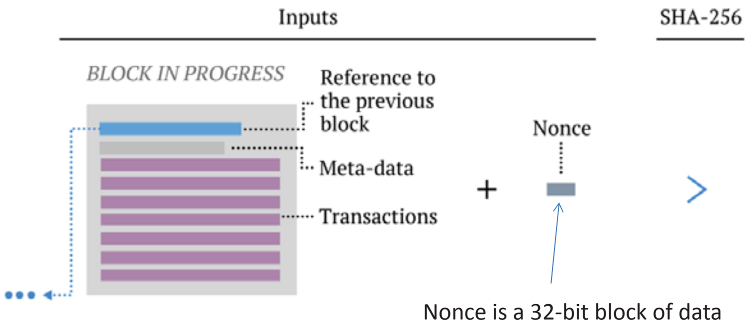
Hash

- 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) 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”



Nonce is a 32-bit block of data

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.

00000eb9c313a3c87d4b1fadb69a9d1395cdbc802b10707fa7e620ad722c0f63

- More leading zeroes means fewer solutions – and more time to solve the problem – it determines the “difficulty” (currently 18 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 16, 2017, 3:47PM)

000000000000000000028e88115c254439a0ae070a75bbf38795c197a1d40e6c4

Nonce = **3063458477**

See http://blockexplorer.com

The Mechanics

Probability of a single hash being the solution:

0.000000000000000000000211758237

Probability of winning 6/49 lottery twice in a row

0.000000000000000000000000019029

See http://blockexplorer.com

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 18 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:

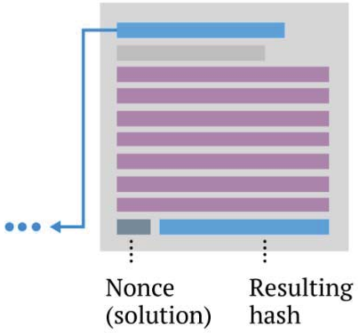
```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

We get four 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

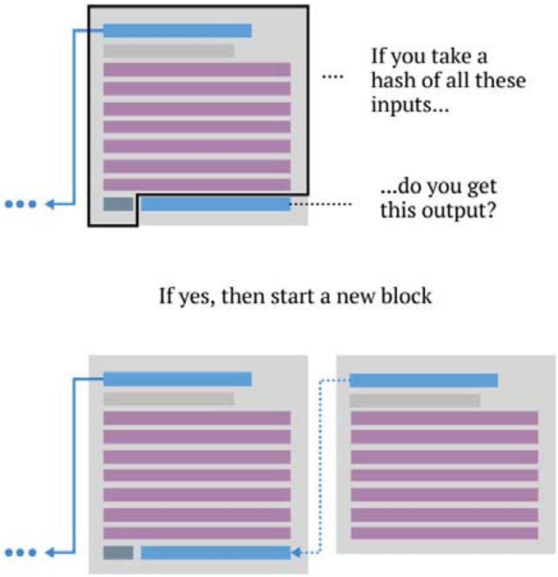


Graphics from King, Williams and Yanofsky (2013)

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 you take a hash of all these inputs...
...do you get this output?
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**

*Each component in hex. The hex is expressed in little-endian format, i.e. 12345678 in little-endian is 78563412. The string is hashed twice with SHA-256 and final hash is presented in little-endian format.

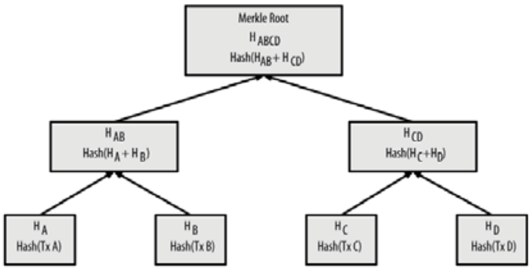
The Mechanics

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

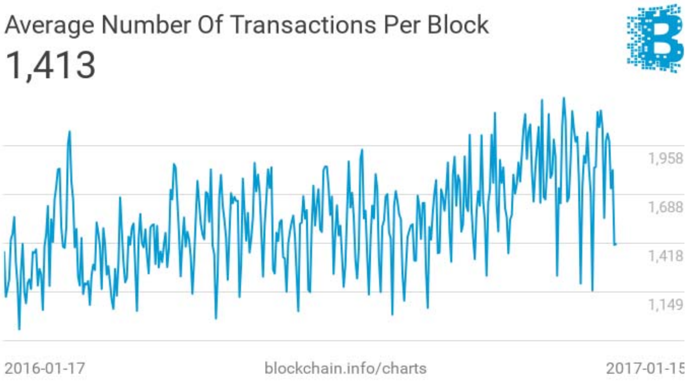
The Mechanics

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



Each data block is a transaction

http://chimera.labs.oreilly.com/books/1234000001802/ch07.html#merkle_trees

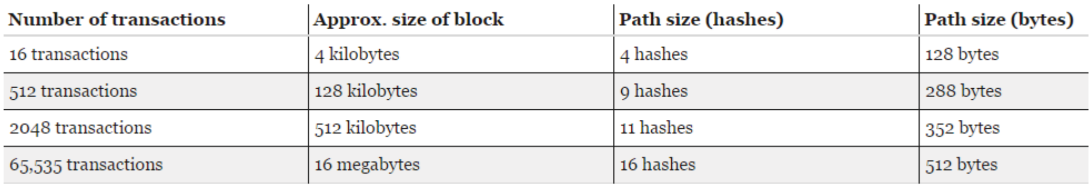


Block averages 1,500 transactions

https://blockchain.info/charts

The Mechanics

Merkle trees very efficient

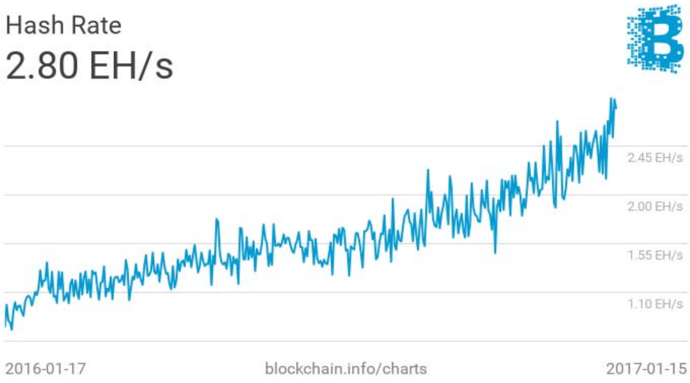


Number of transactions	Approx. size of block	Path size (hashes)	Path size (bytes)
16 transactions	4 kilobytes	4 hashes	128 bytes
512 transactions	128 kilobytes	9 hashes	288 bytes
2048 transactions	512 kilobytes	11 hashes	352 bytes
65,535 transactions	16 megabytes	16 hashes	512 bytes

http://chimera.labs.oreilly.com/books/1234000001802/ch07.html#merkle_trees

The Mechanics

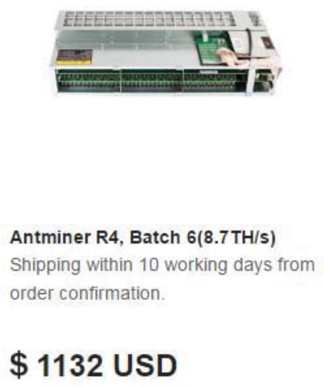
Lots of hashes! 2.8 billion gigahashes per second!



https://blockchain.info/charts

The Mechanics

Lots of hashes! 2.8 billion gigahashes per second!



Antminer R4, Batch 6(8.7TH/s)
Shipping within 10 working days from order confirmation.

$ 1132 USD

2.8 million TH/s divided by 8.7 = 321,839 machines

Cost of matching current network power= $364 million

Realistically, you would have buy much more because by the time you get delivery, you will have less than half the hashing power

The Mechanics

Miners' role:

- Mining code is open source
- Miners are competitive
- Miners pool resources and can be strategic

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., transactions validated and blocks cryptographically linked) so that no trust is needed

The Mechanics

Vulnerability

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

The Mechanics

Vulnerability

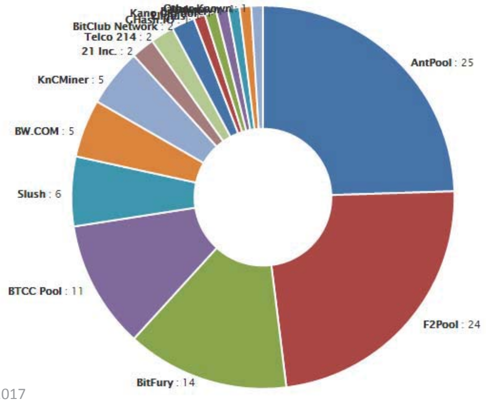
- January 9, 2014 Ghash.io had 45% of all mining
- Had to appeal to people to exit the pool

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

The Mechanics

Vulnerability

- January 2016: Two pools controlling almost 50%

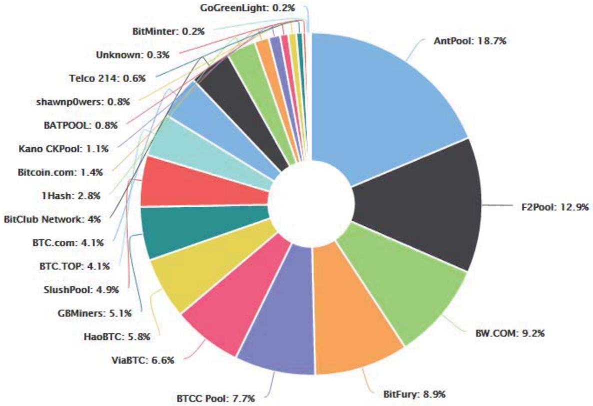


See https://blockchain.info/pools

The Mechanics

Vulnerability

- January 2017

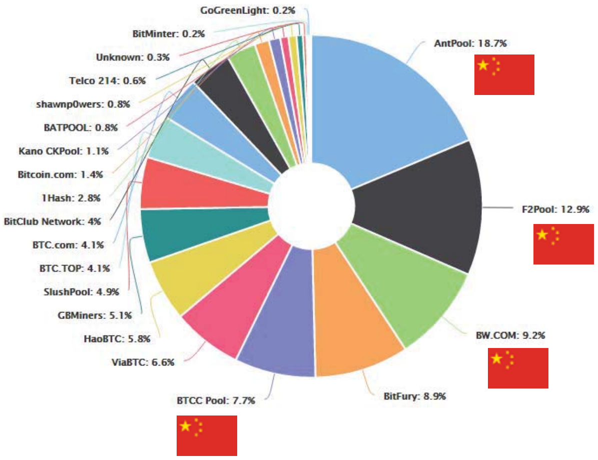


See https://blockchain.info/pools

The Mechanics

Vulnerability

- January 2017

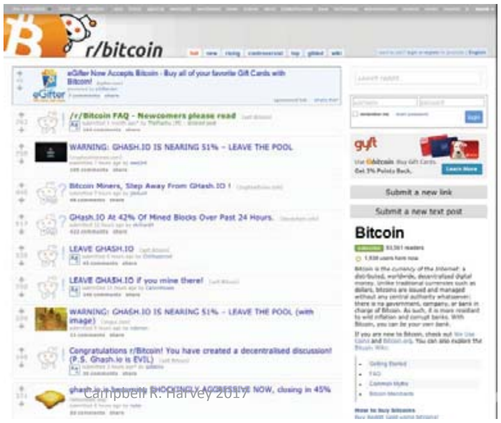


See https://blockchain.info/pools and https://bitcoinchain.com/pools

The Mechanics

Vulnerability

- Not clear what the incentive is to "take over"
- If it ever happened, the value of the Bitcoin might disappear



eGifter Now Accepts Bitcoin - Buy all of your favorite Gift Cards with Bitcoin!

/r/Bitcoin FAQ - Newcomers please read

WARNING: GHASH.IO IS NEARING 51% - LEAVE THE POOL

Bitcoin Miners, Step Away From GHash.IO !

GHash.IO At 42% Of Mined Blocks Over Past 24 Hours.

LEAVE GHASH.IO

LEAVE GHASH.IO if you mine there!

WARNING: GHASH.IO IS NEARING 51% - LEAVE THE POOL (with image)

Congratulations r/Bitcoin! You have created a decentralised discussion! (P.S. Ghash.io is EVIL)

ghash.io is becoming SHOCKINGLY AGGRESSIVE NOW, closing in 45%

Bitcoin

Bitcoin is the currency of the Internet: a distributed, worldwide, decentralized digital money. Unlike traditional currencies such as dollars, bitcoins are issued and managed without any central authority whatsoever: there is no government, company, or bank in charge of Bitcoin. As such, it is more resistant to wild inflation and corrupt banks. With Bitcoin, you can be your own bank.

If you are new to Bitcoin, check out We Use Coins and Bitcoin.org. You can also explore the Bitcoin Wiki:

- Getting Started
- FAQ
- Common Myths
- Bitcoin Merchants

How to buy bitcoins

The Mechanics

Private Key/Public Key:

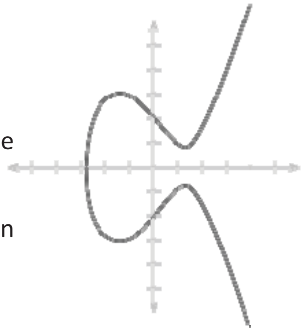
- Bitcoin based on strong cryptography
- Usually we think of using a key to encrypt and decrypt
- It is possible to use two keys: private (secret) and public (give to anyone)
- You can sign a message using a private key such that the signature is unforgeably tied to the public key
- Two keys are know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

The Mechanics

Signing:

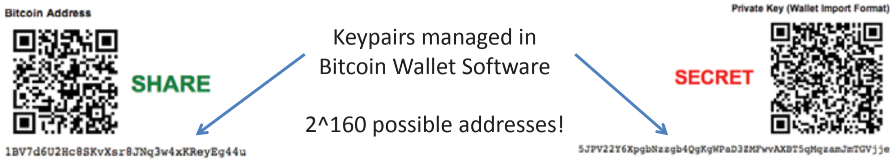
- Signing involves your private key and a nonce
- Anyone can use the nonce and public key to verify that the message was created with the private key
- Creation of a transaction address is very secure, involves
  - Cryptographic “Elliptic Curve DSA” on curve secp256k1
  - Double application of SHA-256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



Bitcoin Address
SHARE
1BV7d6U2Hc8SKvXsr8JNq3w4xKReyEg44u
Private Key (Wallet Import Format)
SECRET
5JPV22Y6XpgbNzzgb4QgKgWPaD3ZMFwvAXBT5qMqzamJmTGVjje

Keypairs managed in Bitcoin Wallet Software

2^160 possible addresses!

“Bank Account Number”

Cheap, expendable, easy to produce

“Signing Key”

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

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

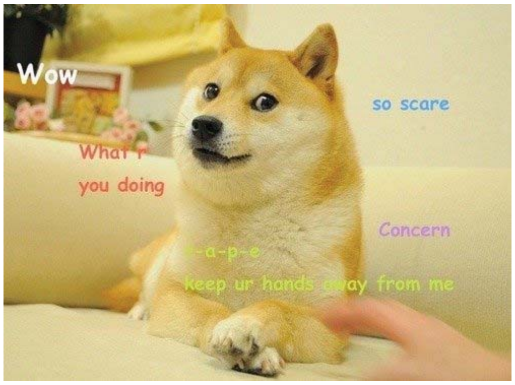
Case study

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

Dogecoin

Case study

- Turns into meme in 2012



Dogecoin

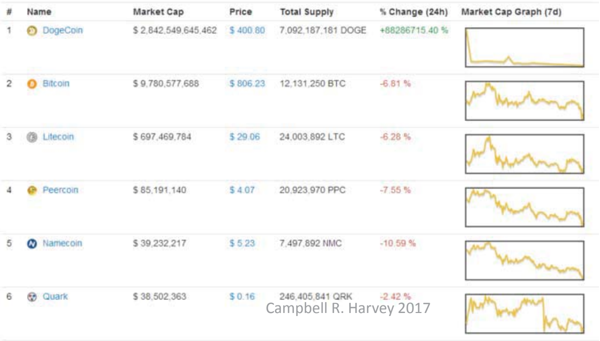
Case study

- 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

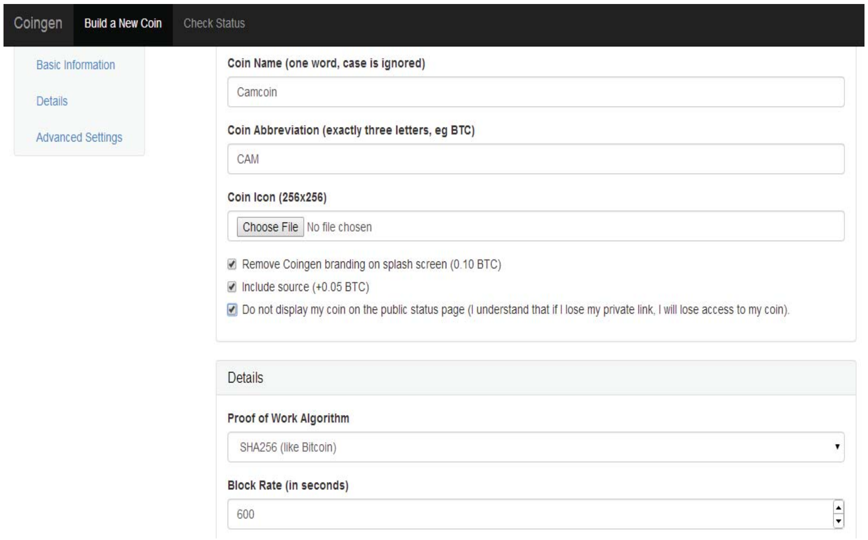
Dogecoin

Case study

- December 14, 2013 value was $400.80 per dogecoin
- December 15, 2013 value was $0.0002 per dogecoin
- January 16, 2017 value was $0.000207 per dogecoin (#15 on coinmarketcap.com)

Camcoin

What your own altcoin?



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

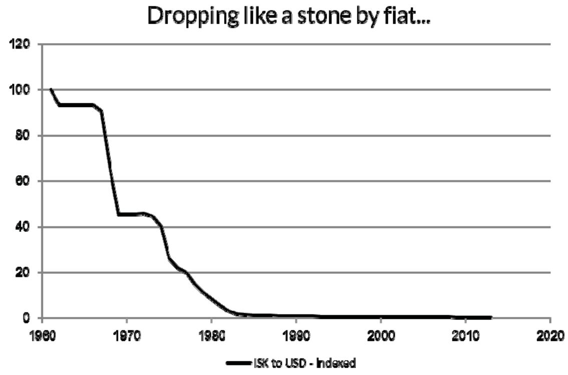
Camcoin

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 $3.00.

Appendix: 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.

Appendix: 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 hyrvnia. 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.

Appendix: 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.

Appendix: 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.

Appendix: Reverse Engineering a Block Header: Step by Step

```
# Analysis of block (Python v.3)
print ("Analysis of https://blockchain.info/rawblock/0000000000000000be983a81043933c38008010b849fd6a35d5dd2d57f929bd");
import hashlib
import codecs
# hash: 0000000000000000be983a81043933c38008010b849fd6a35d5dd2d57f929bd (this is what we are trying to recreate)
# ver: 3
# prev_block: 000000000000000051f5de334085b92ce27c03888c726c9b2bb78069e55aeb6
# mrkl_root: f4db18d3ecab87eeb23a56490d5b0b514848d510d409b43f6bbf2b82f55da8db
# time: 1442663985
# bits: 403867578 (this is the difficulty)
# nonce: 3548193207
# -----------------
# version = 3, encoded as '03000000' (4-byte little endian);
# previous_hash = 'b6ae559e0678bbb2c926c78838c027ce925b0834e35d1f050000000000000000'; (already hex, little endian)
# merkle_root = 'dba85df5822bbf6b3fb409d410d54848510b5b0d49563ab2ee87abecd318dbf4'; (already hex, little endian)
# time = 1442663985, encoded as '314efd55' (4-byte little-endian hex);
# bits = '181287ba', stored as 'ba871218'(4-byte little-endian hex);
# nonce = 3548193207, encoded as 'b7217dd3' (4-byte little-endian hex).
header_hex =
'03000000b6ae559e0678bbb2c926c78838c027ce925b0834e35d1f050000000000000000dba85df5822bbf6b3fb409d410d54848510b5b0d49563ab2ee87abecd318dbf4314efd55ba871218b7217dd3'
#                        -version|---previous hash-------------------------------------------------------------------------|---merkle root--------------------------------------------------------------------------|time---|-bits-----|nonce
header_bin = codecs.decode(header_hex, 'hex')
hash1 = hashlib.sha256(header_bin).digest()
hash2 = hashlib.sha256(hashlib.sha256(header_bin).digest()).digest()
# Note [::-1] is the little endian operation
print (codecs.encode((hash2[::-1]), 'hex_codec'))
```