Financial Derivatives FINE 448

5. Cryptofinance

Daniel Andrei

McGill

Fall 2018

Outline

I What is a Bitcoin? What is a blockchain? 3

II Gambling with the Bitcoin 13

- Bitcoin and the S&P 500 14
- Bitcoin and the VIX 19
- Bitcoin and gold 20
- Bitcoin and “attention” 21
- Volatility and other risk measures 22
- Is Bitcoin a bubble? Crypto mania 23

III Mechanics of the Bitcoin 26

- Preliminaries 27
- Signing transactions 30
- Proof-of-work & Mining 37

IV Bitcoin Futures 50

V Getting Started with Bitcoin 57

VI Risks & Issues 59

Outline

I What is a Bitcoin? What is a blockchain? 3

II Gambling with the Bitcoin 13

- Bitcoin and the S&P 500 14
- Bitcoin and the VIX 19
- Bitcoin and gold 20
- Bitcoin and “attention” 21
- Volatility and other risk measures 22
- Is Bitcoin a bubble? Crypto mania 23

III Mechanics of the Bitcoin 26

- Preliminaries 27
- Signing transactions 30
- Proof-of-work & Mining 37

IV Bitcoin Futures 50

V Getting Started with Bitcoin 57

VI Risks & Issues 59

- Warning: you will get a lot of “recycled information” on the web

memecenter.com

- Try to find the source! (e.g. the paper *“A Peer-to-Peer Electronic Cash System,”* by Satoshi Nakamoto; the paper *“The Byzantine Generals Problem,”* by Lamport, Shostak and Pease)
- Try to understand and replicate some things by yourself!

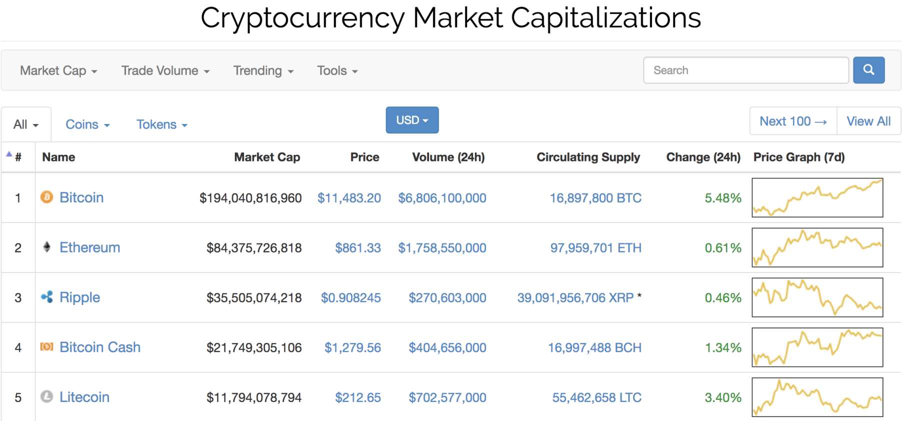
— What is a Bitcoin?

- *"Bitcoin is a type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds."* WHAT?
- *"Bitcoin is the first decentralized digital currency, as the system works without a central bank or single administrator."* WHAT??

What is a blockchain?

- *“Blockchains are immutable digital ledger systems implemented in a distributed fashion.”* WHAT???
- *“Blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography.”* WHAT????
- *“Blockchain is a digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly.”* WHAT?????
- *“Blockchain is a chain of blocks.”* WHAT??????

March 2018, — Coinmarketcap.com:



Cryptocurrency Market Capitalizations

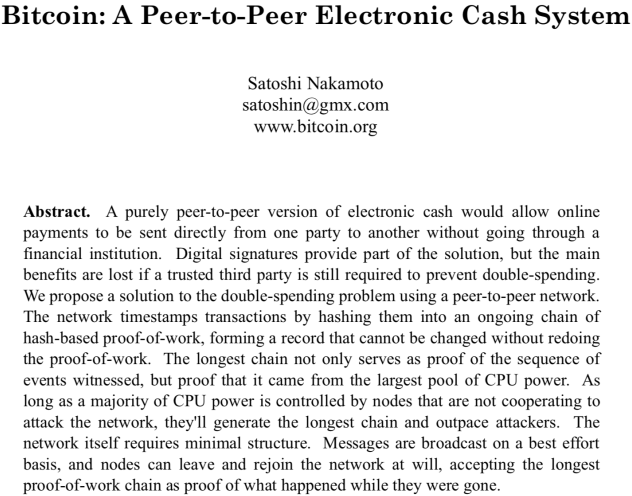
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$194,040,816,960	$11,483.20	$6,806,100,000	16,897,800 BTC	5.48%	
2	Ethereum	$84,375,726,818	$861.33	$1,758,550,000	97,959,701 ETH	0.61%	
3	Ripple	$35,505,074,218	$0.908245	$270,603,000	39,091,956,706 XRP *	0.46%	
4	Bitcoin Cash	$21,749,305,106	$1,279.56	$404,656,000	16,997,488 BCH	1.34%	
5	Litecoin	$11,794,078,794	$212.65	$702,577,000	55,462,658 LTC	3.40%	

- Market cap of Mastercard: ≈ $184 billion
- Transactions per second: Mastercard ∼2000, Bitcoin 7 (limit!)
- Currently, Coinmarketcap.com lists over 1,500 crypto-currencies. But most of them are highly illiquid.

Bitcoin units (March 2018)

Unit	Symbol	BTC	USD
bitcoin	BTC	1	\$11,339.47
milli-bitcoin (millibit, millie)	*m*BTC	$\frac{1}{1000}$	\$11.33947
micro-bitcoin (bit)	μBTC	$\frac{1}{1,000,000}$	\$0.01133947
satoshi	sat	$\frac{1}{100,000,000}$	\$0.0001133947

— Who is Satoshi Nakamoto?

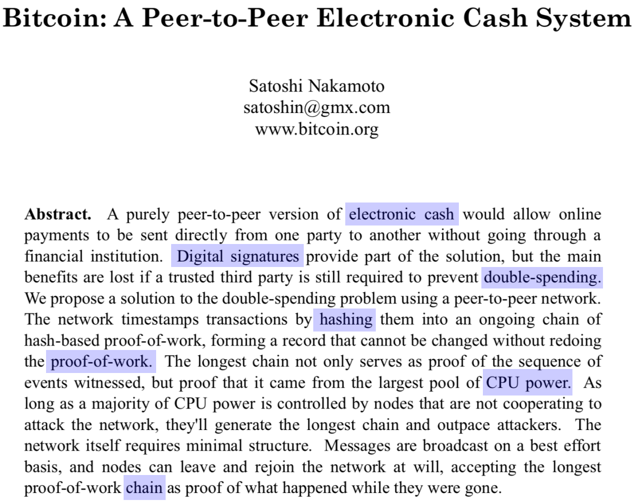


Bitcoin: A Peer-to-Peer Electronic Cash System

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.

— Who is Satoshi Nakamoto?



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 cash and the “double spend” problem

- Suppose you receive an email from me where I write *“I give you 1 unit of digital cash.”* There are three questions:
  1. Are you sure it is really coming from me?
  2. Are you sure I didn’t spent that unit before giving it to you?
  3. What is the value of 1 unit of digital cash?

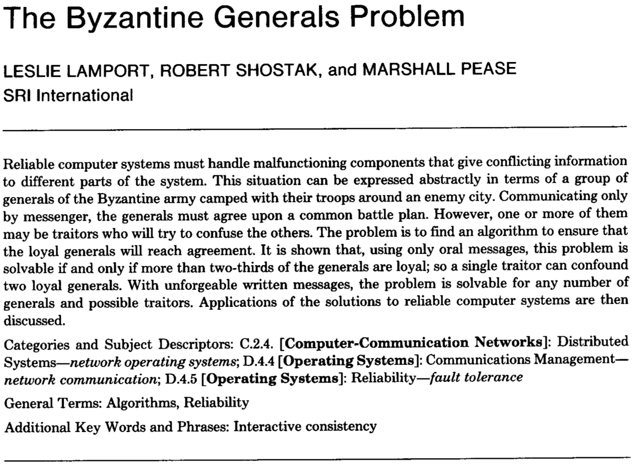
Electronic cash and the "double spend" problem

- Suppose you receive an email from me where I write *"I give you 1 unit of digital cash."* There are three questions:
    1. Are you sure it is really coming from me?
    2. Are you sure I didn't spent that unit before giving it to you?
    3. What is the value of 1 unit of digital cash?
- With Bitcoin, the answers are:
  (1) YES, (2) YES, (3) WE DON'T KNOW
    1. We can check if it is indeed me who "signed" the email
    2. We can build a **decentralized immutable ledger** that keeps track of all units of digital cash since the beginning of time. This includes the unit that I am sending to you. It is a proof that indeed I own that unit and that I haven't sent it to someone else before.
    3. Economics can help to answer the third question.

Electronic cash and the “double spend” problem

- Suppose you receive an email from me where I write *“I give you 1 unit of digital cash.”* There are three questions:
  1. Are you sure it is really coming from me?
  2. Are you sure I didn’t spent that unit before giving it to you?
  3. What is the value of 1 unit of digital cash?
- With Bitcoin, the answers are:
  (1) YES, (2) YES, (3) WE DON’T KNOW
  1. We can check if it is indeed me who “signed” the email
  2. We can build a **decentralized immutable ledger** that keeps track of all units of digital cash since the beginning of time. This includes the unit that I am sending to you. It is a proof that indeed I own that unit and that I haven’t sent it to someone else before.
  3. Economics can help to answer the third question.
- Crypto-currencies have been around since the 1980s (e.g., Digicash, Ecash). They failed because they did not provide a solution to the “double spend” problem
- **Bitcoin solves the double spend problem**

The double spend problem



The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International

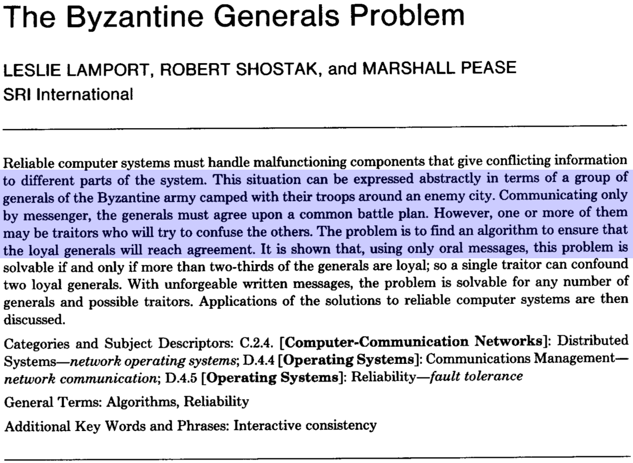
Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

Categories and Subject Descriptors: C.2.4. **[Computer-Communication Networks]**: Distributed Systems—*network operating systems*; D.4.4 **[Operating Systems]**: Communications Management—*network communication*; D.4.5 **[Operating Systems]**: Reliability—*fault tolerance*

General Terms: Algorithms, Reliability

Additional Key Words and Phrases: Interactive consistency

The double spend problem



The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International

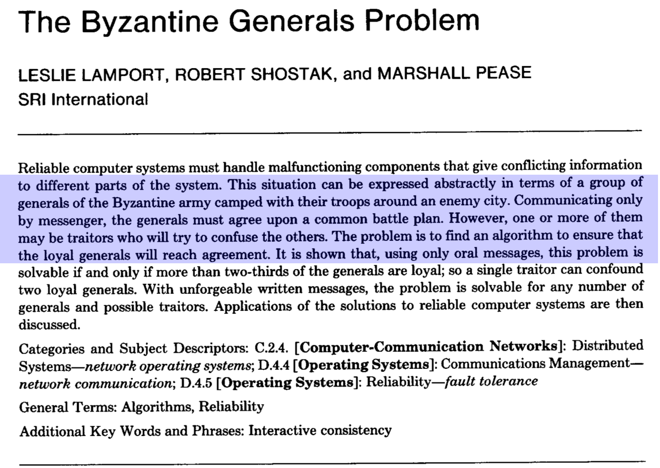
Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

Categories and Subject Descriptors: C.2.4. **[Computer-Communication Networks]**: Distributed Systems—*network operating systems*; D.4.4 **[Operating Systems]**: Communications Management—*network communication*; D.4.5 **[Operating Systems]**: Reliability—*fault tolerance*

General Terms: Algorithms, Reliability

Additional Key Words and Phrases: Interactive consistency

The double spend problem



The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International

Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

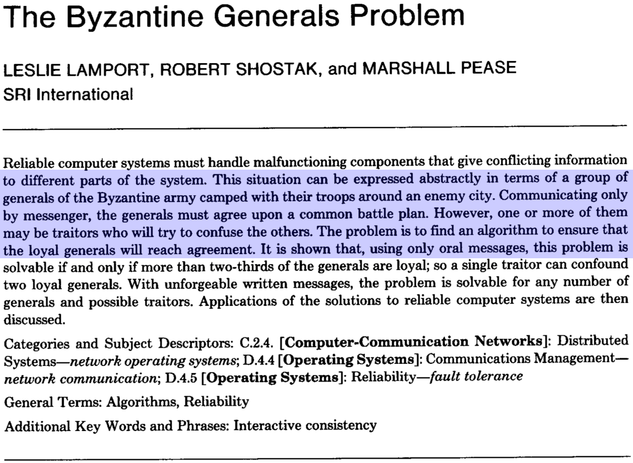
Categories and Subject Descriptors: C.2.4. [**Computer-Communication Networks**]: Distributed Systems—*network operating systems*; D.4.4 [**Operating Systems**]: Communications Management—*network communication*; D.4.5 [**Operating Systems**]: Reliability—*fault tolerance*

General Terms: Algorithms, Reliability

Additional Key Words and Phrases: Interactive consistency

- Mastercard/Visa/PayPal/etc... have a solution: central authority

The double spend problem



The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International

Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

Categories and Subject Descriptors: C.2.4. [**Computer-Communication Networks**]: Distributed Systems—*network operating systems*; D.4.4 [**Operating Systems**]: Communications Management—*network communication*; D.4.5 [**Operating Systems**]: Reliability—*fault tolerance*

General Terms: Algorithms, Reliability

Additional Key Words and Phrases: Interactive consistency

- Mastercard/Visa/PayPal/etc... have a solution: central authority
- Bitcoin provides an alternative solution **without** central authority

Blockchain technology

- Until blockchain technology, digital cash was infinitely copyable
- A trusted third party (bank, PayPal, etc.) had to keep a ledger to avoid the double spend problem
- The blockchain technology solves the double spend problem
- Trustless technology: a user does not need to trust the other party in the transaction—but does need to trust the system!

Blockchain technology

- Until blockchain technology, digital cash was infinitely copyable
- A trusted third party (bank, PayPal, etc.) had to keep a ledger to avoid the double spend problem
- The blockchain technology solves the double spend problem
- Trustless technology: a user does not need to trust the other party in the transaction—but does need to trust the system!

- Immutable history:
  - George Orwell, *1984*: "Ministry of Truth" was responsible for any necessary falsification of historical events
  - Blockchain would prevent that: the past cannot be modified!

Outline

I What is a Bitcoin? What is a blockchain? 3

II Gambling with the Bitcoin 13

- Bitcoin and the S&P 500 14
- Bitcoin and the VIX 19
- Bitcoin and gold 20
- Bitcoin and “attention” 21
- Volatility and other risk measures 22
- Is Bitcoin a bubble? Crypto mania 23

III Mechanics of the Bitcoin 26

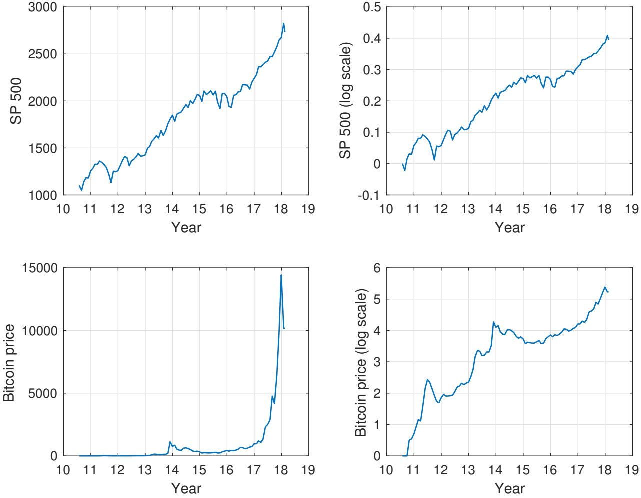
- Preliminaries 27
- Signing transactions 30
- Proof-of-work & Mining 37

IV Bitcoin Futures 50

V Getting Started with Bitcoin 57

VI Risks & Issues 59

Bitcoin and the S&P 500 (monthly data)



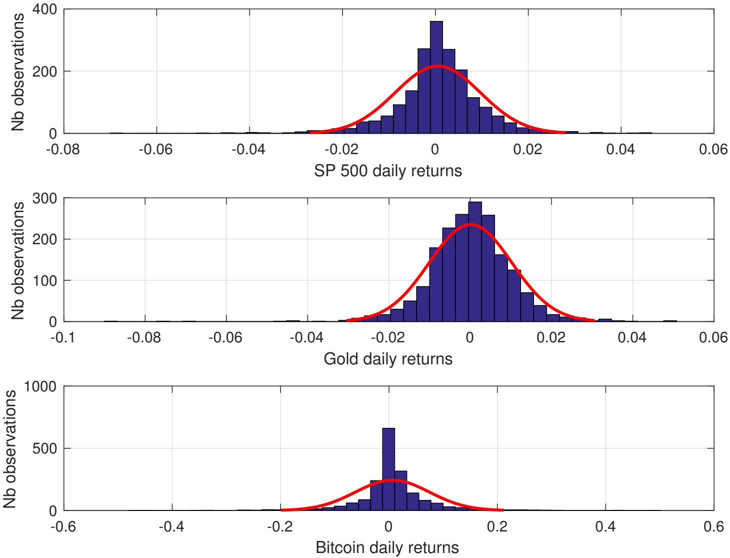
- S&P 500 had a great run since 2010.
- It's nothing when compared with the Bitcoin!

S&P 500, gold, and the Bitcoin

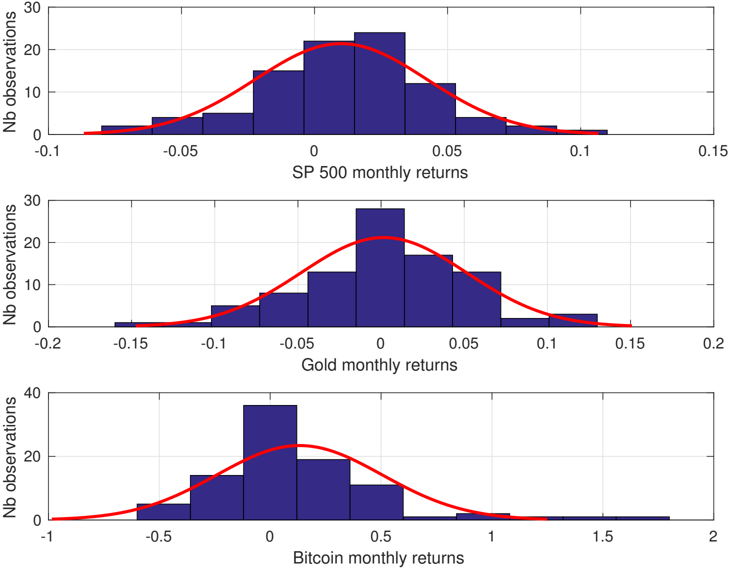
	Avg. ret	Volatility	Skewness	Kurtosis
S&P 500	0.1198	0.1116	-0.1001	3.5251
Gold	0.0199	0.1722	-0.2673	3.5301
Bitcoin	1.5879	1.2898	1.5767	7.1551

- There is a (weak) positive relationship between the monthly returns on S&P 500 and the monthly returns on Bitcoin. The coefficient of the returns on S&P500 is 2.29 (t-stat=1.91). The correlation between the two series is 0.2.

S&P 500, gold, and the Bitcoin



S&P 500, gold, and the Bitcoin



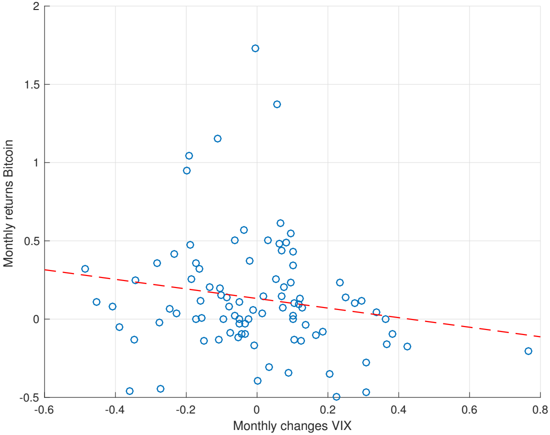
S&P 500, gold, and the Bitcoin

- Serial correlation with monthly returns:

$$r_{t+1} = a + br_t + \varepsilon$$

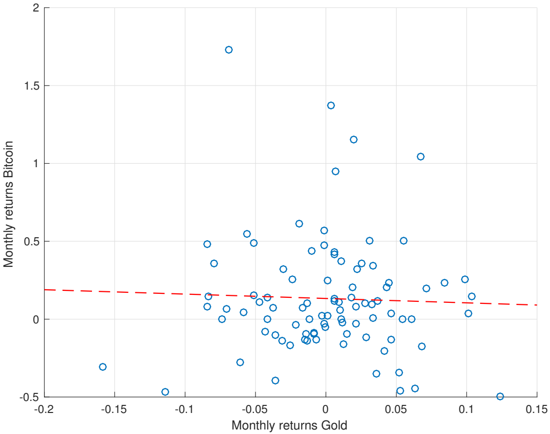
	b	t-stat	Adj. R^2
S&P 500	-0.15	-0.3542	0.0109
Gold	-0.10	-0.9114	-0.0019
Bitcoin	0.28	2.72	0.0668

Bitcoin and the VIX



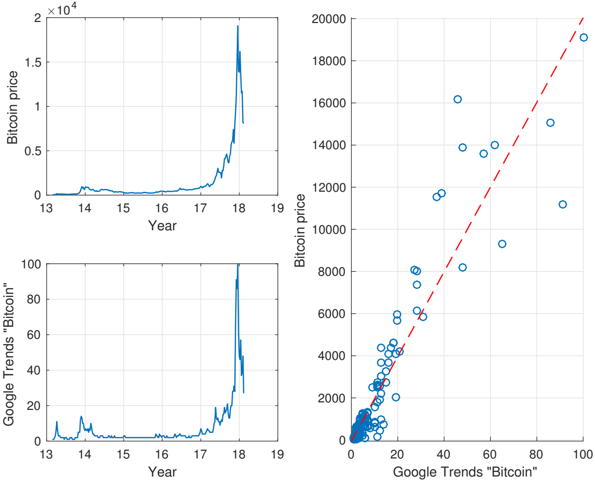
- There is a negiligible correlation between changes in Bitcoin prices and changes in the VIX (-17%). The relationship is not statistically significant, with an R^2 less than 2%
- The correlation between the S&P 500 and the VIX is -74%

Bitcoin and gold



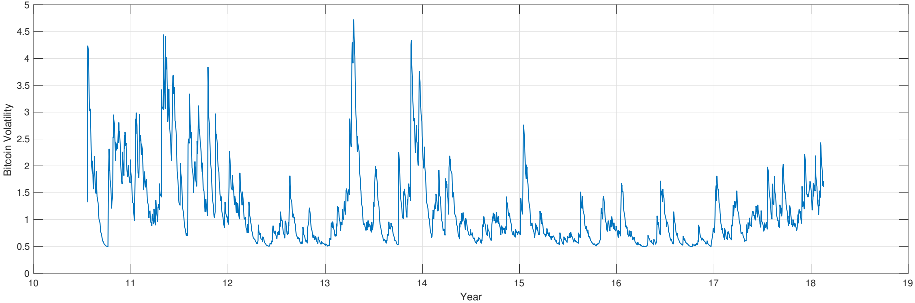
- Bitcoin = “Digital Gold”?!? I have not heard why
- Bitcoin would benefit from a flight to safety... It didn’t happen so far

Bitcoin and “attention”



- Regression: coeff=201 on attention, with t-stat 44, and $R^2 = 88\%$!
- See Andrei and Hasler, “Investor attention and stock market volatility.” (2014)

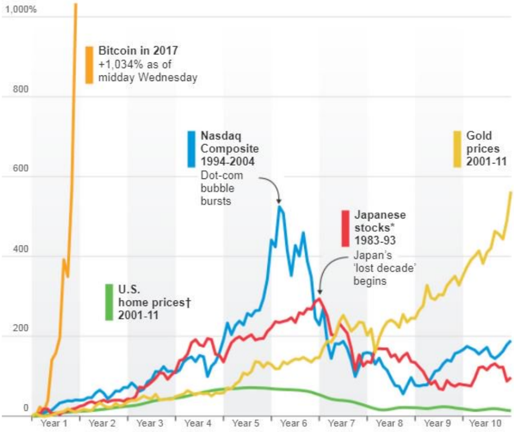
Volatility and other risk measures



Number of daily returns...	... less than...	S&P 500	Gold	Bitcoin
	-0.05	1	3	194
	-0.10	0	0	81
	-0.15	0	0	43
	-0.20	0	0	20
	-0.25	0	0	10
	-0.30	0	0	5

Is Bitcoin a bubble?

Bitcoin's 1,034% run-up this year compared to decade-long trends in other historically huge market moves



*Tokyo Stock Price Index †Case-Shiller Home Price Index

Sources: CoinDesk (bitcoin); FactSet (Nasdaq, Japanese stocks, gold); Thomson Reuters (home prices)

Is Bitcoin a bubble?

- Bitcoin does not pay any dividends
  $\Rightarrow$ price > 0 for two reasons:
  1. People see value in holding it (easy transfer of money, cheap transfer of money, avoid capital controls, laundering money, etc.). This is fundamental demand.
  2. Speculative demand. This usually comes together with (a) limited supply, (b) high volatility, and (c) high trading volume
- Clearly, both forces are at play for the Bitcoin.

Is Bitcoin a bubble?

- Bitcoin does not pay any dividends
  $\Rightarrow$ price > 0 for two reasons:
  1. People see value in holding it (easy transfer of money, cheap transfer of money, avoid capital controls, laundering money, etc.). This is fundamental demand.
  2. Speculative demand. This usually comes together with (a) limited supply, (b) high volatility, and (c) high trading volume
- Clearly, both forces are at play for the Bitcoin.
- The second force might be amplified by information diffusion: people hear from each other about the Bitcoin, then they observe the rise in the price, and decide to "follow the trend." The symptoms of this should be:
  - Momentum (see slide 18)
  - High demand for information (see slide 21)
  - High volatility (see slide 22)
  - High trading volume (just Google "Bitcoin trading volume")

Is Bitcoin a bubble?

- Bitcoin does not pay any dividends
  $\Rightarrow$ price > 0 for two reasons:
  1. People see value in holding it (easy transfer of money, cheap transfer of money, avoid capital controls, laundering money, etc.). This is fundamental demand.
  2. Speculative demand. This usually comes together with (a) limited supply, (b) high volatility, and (c) high trading volume
- Clearly, both forces are at play for the Bitcoin.
- The second force might be amplified by information diffusion: people hear from each other about the Bitcoin, then they observe the rise in the price, and decide to "follow the trend." The symptoms of this should be:
  - Momentum (see slide 18)
  - High demand for information (see slide 21)
  - High volatility (see slide 22)
  - High trading volume (just Google "Bitcoin trading volume")
- See Andrei and Cujean, "Information percolation, momentum and reversal." (2017)

— Crypto mania

- Reuters, Dec 21, 2017:

  Many tiny companies are pivoting operations or changing their names to cash-in on the cryptocurrency wave, in a trend reminiscent of the dotcom boom.

Name before	Name after	Market cap before	Market cap after
Bioptix Inc	Riot Blockchain Inc	\$68.6 mln	\$300.6 mln
SkyPeople Fruit Juice Inc	Future FinTech Group Inc	\$10.3 mln	\$22.5 mln

— Crypto mania

- Reuters, Dec 21, 2017:

  Many tiny companies are pivoting operations or changing their names to cash-in on the cryptocurrency wave, in a trend reminiscent of the dotcom boom.

Name before	Name after	Market cap before	Market cap after
Bioptix Inc	Riot Blockchain Inc	\$68.6 mln	\$300.6 mln
SkyPeople Fruit Juice Inc	Future FinTech Group Inc	\$10.3 mln	\$22.5 mln

- Wall Street Journal, Dec 18, 2017:

  [...] a software startup that doesn't plan to sell any software and describes what it is selling—something called a digital token—as having "no purpose."

  The company, block.one, has raised about \$700 million and counting. [...] Block.one's website doesn't say much about its key employees. [...] Its 14-page white paper posted on the site describes new software that promises to handle millions of transactions per second.

Outline

I What is a Bitcoin? What is a blockchain? 3

II Gambling with the Bitcoin 13

- Bitcoin and the S&P 500 14
- Bitcoin and the VIX 19
- Bitcoin and gold 20
- Bitcoin and “attention” 21
- Volatility and other risk measures 22
- Is Bitcoin a bubble? Crypto mania 23

III Mechanics of the Bitcoin 26

- Preliminaries 27
- Signing transactions 30
- Proof-of-work & Mining 37

IV Bitcoin Futures 50

V Getting Started with Bitcoin 57

VI Risks & Issues 59

Preliminaries I: Hexadecimal numbers (Base 16)

- Base 10 requires 10 digits (0 to 9)
- Base 16 requires 16 digits (0 to f):

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f

Preliminaries I: Hexadecimal numbers (Base 16)

- Base 10 requires 10 digits (0 to 9)
- Base 16 requires 16 digits (0 to f):

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f

- From decimal to hexadecimal:

$$125 = 7 \times 16 + 13 \quad \Rightarrow \quad 125 = 7d \tag{1}$$

- From hexadecimal to decimal:

$$7d = 7 \times 16 + 13 = 125 \tag{2}$$

Preliminaries I: Hexadecimal numbers (Base 16)

- Base 10 requires 10 digits (0 to 9)
- Base 16 requires 16 digits (0 to f):

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f

- From decimal to hexadecimal:

$$125 = 7 \times 16 + 13 \quad \Rightarrow \quad 125 = 7d \tag{1}$$

- From hexadecimal to decimal:

$$7d = 7 \times 16 + 13 = 125 \tag{2}$$

- **Question** Rank the following hexadecimal numbers:
  - `0fff`
  - `1000`
  - `abcd`
  - `abc9`

Preliminaries II: Large numbers

We will work with numbers between 0 and $2^{256} - 1$. That is, from 0 to...
115792089237316195423570985008687907853269984665640564039457584007913129639935

In hexadecimal base, this is the largest number with exactly 64 digits:
`ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff`

Preliminaries II: Large numbers

We will work with numbers between 0 and $2^{256} - 1$. That is, from 0 to...

```
115792089237316195423570985008687907853269984665640564039457584007913129639935
```

In hexadecimal base, this is the largest number with exactly 64 digits:

```
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
```

How large is this number?

- There are 10 trillion galaxies in the universe. Each galaxy has 100 billion stars. That makes 10^{24} stars. It's nothing:

  ```
  00000000000000000000000000000000000000000000d3c21bcecceda1000000
  ```

- ... 7×10^{27} atoms in the human body. It's nothing:

  ```
  0000000000000000000000000000000000000000169e43a85eb381aa58000000
  ```

- ... 10^{57} atoms of hydrogen in the sun. It's nothing:

  ```
  000000000000000028c87cb5c89a2571ebfdcb54864ada834a00000000000000
  ```

Preliminaries III: Hashing (SHA-256)

- “Secure Hash Algorithm” developed by the NSA
- Output is 64 numbers/characters (hexadecimal base!), no matter how long the input it receives
- SHA-256 (Option Markets 232D, Winter 2018):

  `493201a2d91ec374f12d8d3e51cf4e31b171ef0d2af0eec219def2334b546ce`
- SHA-256 (A purely peer-to-peer version [...] while they were gone.):

  `cda9b3812b878f66e6c5e7773fd7587419f644b67924766e13e78f544df943b3`
- Remove the period at the end:

  SHA-256 (A purely peer-to-peer version [...] while they were gone):

  `8202be4097fd4e6f48bad3c81a9bd2bd96ff3ad4d29255ad941074bf39da49c3`

Preliminaries III: Hashing (SHA-256)

- “Secure Hash Algorithm” developed by the NSA
- Output is 64 numbers/characters (hexadecimal base!), no matter how long the input it receives
- SHA-256 (Option Markets 232D, Winter 2018):

  `493201a2d91ec374f12d8d3e51cf4e31b171ef0d2af0eec219def2334b546ce`
- SHA-256 (A purely peer-to-peer version [...] while they were gone.):

  `cda9b3812b878f66e6c5e7773fd7587419f644b67924766e13e78f544df943b3`
- Remove the period at the end:

  SHA-256 (A purely peer-to-peer version [...] while they were gone):

  `8202be4097fd4e6f48bad3c81a9bd2bd96ff3ad4d29255ad941074bf39da49c3`
- It goes only one way.
- It is “collision resistant” (it is hard to find two inputs that hash to the same output)
- One can hash a hash
- On-line SHA-256 calculator:

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

Signing transactions I

- Let's generate a random **private key** for Warren Buffett:

  ```
  PRIVATEKEY =
  cffe4d67b53691c68b7c933b5b5234cbac02e8e072b150c942879b5b303de79c
  ```

  (This is a secret key. It is kept privately and used to sign messages)

Signing transactions I

- Let's generate a random **private key** for Warren Buffett:

  ```
  PRIVATEKEY =
  cffe4d67b53691c68b7c933b5b5234cbac02e8e072b150c942879b5b303de79c
  ```

  (This is a secret key. It is kept privately and used to sign messages)

- The **public key** associated with this private key is:

  ```
  PUBLICKEY =
  33082f3e63d61e68c8e71eb5cde621a06d06908f57d94b35bd42c0b06a95a67a
  158ac909e0efd59f51309297620850b47413987303572b1102b13f3fd9a2a588
  ```

  (This is a public verification key that Buffett gives to everybody)

Signing transactions I

- Let's generate a random **private key** for Warren Buffett:

  ```
  PRIVATEKEY =
  cffe4d67b53691c68b7c933b5b5234cbac02e8e072b150c942879b5b303de79c
  ```

  (This is a secret key. It is kept privately and used to sign messages)

- The **public key** associated with this private key is:

  ```
  PUBLICKEY =
  33082f3e63d61e68c8e71eb5cde621a06d06908f57d94b35bd42c0b06a95a67a
  158ac909e0efd59f51309297620850b47413987303572b1102b13f3fd9a2a588
  ```

  (This is a public verification key that Buffett gives to everybody)

- It is computationally unfeasible to forge signatures: An adversary who knows Buffett's public key and sees his signatures on some other messages can't forge his signature on some message for which he has not seen his signature. This is called the **unforgeability** property.

Signing transactions II

- Consider now the following **transaction**:

```
Warren Buffett pays 5 Bitcoins to Bill Gates.
```

Signing transactions II

- Consider now the following **transaction**:

  ```
  Warren Buffett pays 5 Bitcoins to Bill Gates.
  ```

- Hash the transaction:

  ```
  TXHASH = SHA-256(Warren Buffett pays 5 Bitcoins to Bill Gates.)  =
  38a76dcc83efb26e32c44acf13bb1ccb9476e6b9e338e23beb86e0fec013e08e
  ```

Signing transactions II

- Consider now the following **transaction**:

  ```
  Warren Buffett pays 5 Bitcoins to Bill Gates.
  ```

- Hash the transaction:

  ```
  TXHASH = SHA-256(Warren Buffett pays 5 Bitcoins to Bill Gates.)  =
  38a76dcc83efb26e32c44acf13bb1ccb9476e6b9e338e23beb86e0fec013e08e
  ```

- Warren Buffett **signs** the transaction using his private key:

  ```
  TXSIGNED = sign(TXHASH, PRIVATEKEY) =
  b94b2155c5ca18ebb5e9a1fb868434e9af7c739f1cf5a5c77af672b8a4da6224
  3852c9e0ef4a1462c6bc17ca090ff740d33b3670bc40810a3b22c7133626bc78
  ```

  (This is done privately! Only the result is public)

Signing transactions III

- At this moment, everyone can see:
    1. The transaction and its hash, `TXHASH`
    2. Warren Buffett's public key, `PUBLICKEY`
    3. The transaction signed, `TXSIGNED`

Signing transactions III

- At this moment, everyone can see:
  1. The transaction and its hash, `TXHASH`
  2. Warren Buffett's public key, `PUBLICKEY`
  3. The transaction signed, `TXSIGNED`
- No one, except Warren Buffett, can see the private key, `PRIVATEKEY`
- In fact, Warren Buffett or Bill Gates are not required to reveal their identity. The transaction can only incorporate public keys:

  ```
  PUBLICKEY pays 5 Bitcoins to OTHER_PUBLIC_KEY.
  ```
- The text of the transaction can be arbitrarily long. This doesn't matter, because it is hashed before being signed.

Signing transactions III

- At this moment, everyone can see:
  1. The transaction and its hash, `TXHASH`
  2. Warren Buffett's public key, `PUBLICKEY`
  3. The transaction signed, `TXSIGNED`
- No one, except Warren Buffett, can see the private key, `PRIVATEKEY`
- In fact, Warren Buffett or Bill Gates are not required to reveal their identity. The transaction can only incorporate public keys:

  ```
  PUBLICKEY pays 5 Bitcoins to OTHER_PUBLIC_KEY.
  ```
- The text of the transaction can be arbitrarily long. This doesn't matter, because it is hashed before being signed.
- Verifying the transaction is a deterministic and instantaneous operation:

  ```
  verify(TXHASH, PUBLICKEY, TXSIGNED) = true
  ```

Verifying transactions I

- Say that Bill Gates decides to change the transaction into:

  ```
  Warren Buffett pays 5,000 Bitcoins to Bill Gates.
  ```

- Hashing this transaction results into another output, `TXHASHFAKE`. Verifying this modified transaction yields:

  ```
  verify(TXHASHFAKE, PUBLICKEY, TXSIGNED) = false
  ```

Verifying transactions II

- Say that the transaction is not correctly registered for the public key `PUBLICKEY`, but for `WRONGPUBLICKEY`
- Verifying this transaction yields:

```
verify(TXHASH, WRONGPUBLICKEY, TXSIGNED) = false
```

Verifying transactions III

- Say someone else (Mark Zuckerberg) decides to sign this transaction.
- A different private key (Zuckerberg's key) would generate a different signed transaction, `TXSIGNEDZuckerberg`. Verifying this modified output yields:

  ```
  verify(TXHASH, PUBLICKEY, TXSIGNEDZuckerberg) = false
  ```

Digital Signatures Work!

- A great reference is Chapter 1 in:

  Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *“Bitcoin and cryptocurrency technologies.”* (2016). Princeton University Press

Proof-of-work & Mining

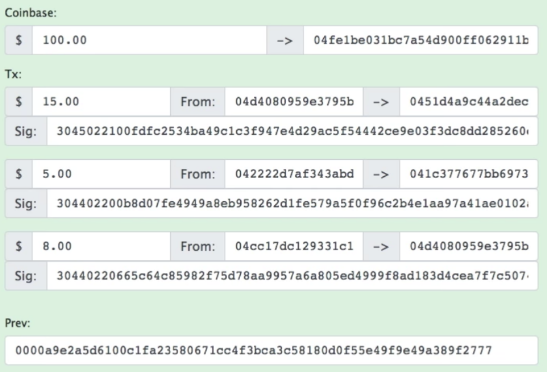
1. Miners build candidate **blocks** of transactions
2. Once a new candidate block is available, each miner will work to **"mine"** it. This is computationally (very) difficult.
3. Every $\sim$ 10 minutes, a new block is mined and added to the chain.

   (it takes 10 minutes because the **difficulty** is readjusted every 2,016 blocks)
4. The block is then **validated** by the whole network
5. The proces starts again from step 1 with a new candidate block.

We need to define: "block," "difficulty," "mining," "validation."

Proof-of-work I: A “block”

A block = a group of transactions with the following information:



Coinbase:

$ 100.00 -> 04fe1be031bc7a54d900ff062911b

Tx:

$ 15.00 From: 04d4080959e3795b -> 0451d4a9c44a2dec

Sig: 3045022100fdfc2534ba49c1c3f947e4d29ac5f54442ce9e03f3dc8dd285260

$ 5.00 From: 042222d7af343abd -> 041c377677bb6973

Sig: 304402200b8d07fe4949a8eb958262d1fe579a5f0f96c2b4e1aa97a41ae0102

$ 8.00 From: 04cc17dc129331c1 -> 04d4080959e3795b

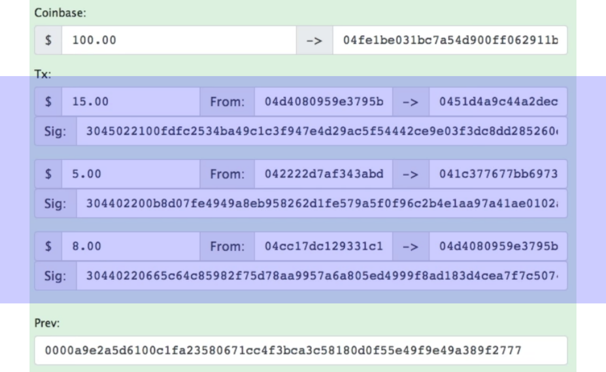
Sig: 30440220665c64c85982f75d78aa9957a6a805ed4999f8ad183d4cea7f7c507

Prev:

0000a9e2a5d6100c1fa23580671cc4f3bca3c58180d0f55e49f9e49a389f2777

Proof-of-work I: A “block”

A block = a group of transactions with the following information:



Coinbase:

$ 100.00 -> 04fe1be031bc7a54d900ff062911b

Tx:

$ 15.00 From: 04d4080959e3795b -> 0451d4a9c44a2dec

Sig: 3045022100fdfc2534ba49c1c3f947e4d29ac5f54442ce9e03f3dc8dd285260

$ 5.00 From: 042222d7af343abd -> 041c377677bb6973

Sig: 304402200b8d07fe4949a8eb958262d1fe579a5f0f96c2b4e1aa97a41ae0102

$ 8.00 From: 04cc17dc129331c1 -> 04d4080959e3795b

Sig: 30440220665c64c85982f75d78aa9957a6a805ed4999f8ad183d4cea7f7c507

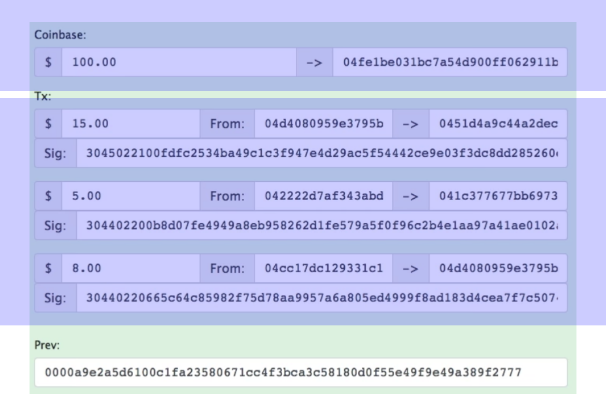
Prev:

0000a9e2a5d6100c1fa23580671cc4f3bca3c58180d0f55e49f9e49a389f2777

All the transactions in the block (verified!)

Proof-of-work I: A “block”

A block = a group of transactions with the following information:



Coinbase:

$ 100.00 -> 04fe1be031bc7a54d900ff062911b

Tx:

$ 15.00 From: 04d4080959e3795b -> 0451d4a9c44a2dec

Sig: 3045022100fdfc2534ba49c1c3f947e4d29ac5f54442ce9e03f3dc8dd285260

$ 5.00 From: 042222d7af343abd -> 041c377677bb6973

Sig: 304402200b8d07fe4949a8eb958262d1fe579a5f0f96c2b4e1aa97a41ae0102

$ 8.00 From: 04cc17dc129331c1 -> 04d4080959e3795b

Sig: 30440220665c64c85982f75d78aa9957a6a805ed4999f8ad183d4cea7f7c507

Prev:

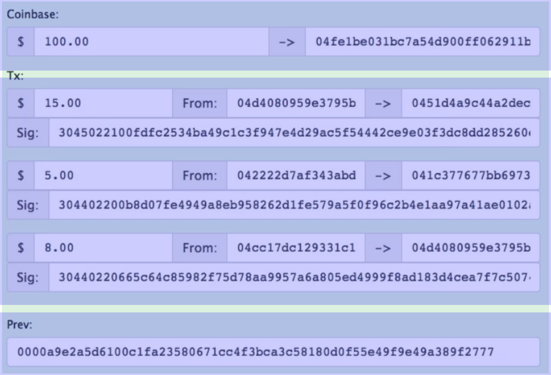
0000a9e2a5d6100c1fa23580671cc4f3bca3c58180d0f55e49f9e49a389f2777

Coinbase transaction (mining reward + transaction fee). Creates new coins!

All the transactions in the block (verified!)

Proof-of-work I: A “block”

A block = a group of transactions with the following information:



Coinbase:

$	100.00	->	04fe1be031bc7a54d900ff062911b

Tx:

$	15.00	From:	04d4080959e3795b	->	0451d4a9c44a2dec
Sig:	3045022100fdfc2534ba49c1c3f947e4d29ac5f54442ce9e03f3dc8dd285260				
$	5.00	From:	042222d7af343abd	->	041c377677bb6973
Sig:	304402200b8d07fe4949a8eb958262d1fe579a5f0f96c2b4e1aa97a41ae0102				
$	8.00	From:	04cc17dc129331c1	->	04d4080959e3795b
Sig:	30440220665c64c85982f75d78aa9957a6a805ed4999f8ad183d4cea7f7c507				

Prev:

0000a9e2a5d6100c1fa23580671cc4f3bca3c58180d0f55e49f9e49a389f2777

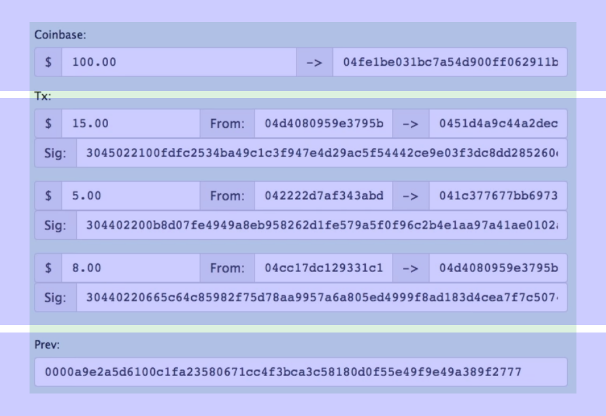
Coinbase transaction (mining reward + transaction fee). Creates new coins!

All the transactions in the block (verified!)

The hash of the previous block

Proof-of-work I: A “block”

A block = a group of transactions with the following information:



Coinbase:

$ 100.00 -> 04fe1be031bc7a54d900ff062911b

Tx:

$ 15.00 From: 04d4080959e3795b -> 0451d4a9c44a2dec

Sig: 3045022100fdfc2534ba49c1c3f947e4d29ac5f54442ce9e03f3dc8dd285260

$ 5.00 From: 042222d7af343abd -> 041c377677bb6973

Sig: 304402200b8d07fe4949a8eb958262d1fe579a5f0f96c2b4e1aa97a41ae0102

$ 8.00 From: 04cc17dc129331c1 -> 04d4080959e3795b

Sig: 30440220665c64c85982f75d78aa9957a6a805ed4999f8ad183d4cea7f7c507

Prev:

0000a9e2a5d6100c1fa23580671cc4f3bca3c58180d0f55e49f9e49a389f2777

Coinbase transaction (mining reward + transaction fee). Creates new coins!

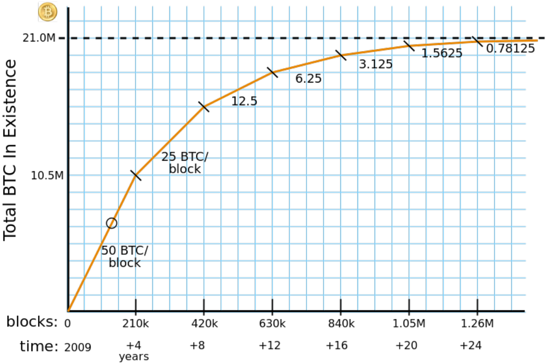
All the transactions in the block (verified!)

The hash of the previous block

There is a special block at the beginning of the list, called the **genesis block**, created by Satoshi Nakamoto. It contains, along with the normal data, the following text: *“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”*

Proof-of-work II: Coin creation

- Reward is 12.5 bitcoins today (— http://www.bitcoinblockhalf.com/) The reward halves every 210,000 blocks $\sim$ 4 years
- Maximum number of bitcoins in circulation will be 21,000,000 (in 2,140). Satoshi Nakamoto holds about 1,000,000.
- Over time, miners will make all their revenues from transaction fees.



Proof-of-work III: Difficulty=1

- Consider the following **target** with a “difficulty” of 1 (it has one zero in front of the 9):

  ```
  TARGET(1) =

  0900000000000000000000000000000000000000000000000000000000000000
  ```

Proof-of-work III: Difficulty=1

- Consider the following **target** with a “difficulty” of 1 (it has one zero in front of the 9):

```
TARGET(1) =

0900000000000000000000000000000000000000000000000000000000000000
```

- This number is lower than our maximum, $2^{256} - 1$. How much lower?
- On a scale from 0 to 100, this number would be 3.51563

Proof-of-work III: Difficulty=1

- Consider the following **target** with a “difficulty” of 1 (it has one zero in front of the 9):

  ```
  TARGET(1) =

  0900000000000000000000000000000000000000000000000000000000000000
  ```

- This number is lower than our maximum, $2^{256}-1$. How much lower?
- On a scale from 0 to 100, this number would be 3.51563
- If we randomly pick integers from 0 to $2^{256}-1$, we need on average 28 trials to get something smaller than `TARGET(1)`

Proof-of-work III: Difficulty=2

- Consider the following **target** with a “difficulty” of 2 (it has two zeros in front of the 9):

  ```
  TARGET(2) =

  0090000000000000000000000000000000000000000000000000000000000000
  ```

- This number is lower than our maximum, $2^{256}-1$. How much lower?
- On a scale from 0 to 100, this number would be 0.21973
- If we randomly pick integers from 0 to $2^{256}-1$, we need on average 455 trials to get something smaller than `TARGET(2)`

Proof-of-work III: Difficulty=n

- And so on...

Difficulty	Average # of trials
1	28
2	455
3	7,282
4	116,508
5	1,864,140
6	29,826,162
7	477,218,588
...	
18	8×10^{21}

- With Difficulty=7, the change of getting a number smaller than `TARGET(7)` ≈ the chance of winning the Powerball Lottery
- **The current difficulty (February 2018) is 18.**

Proof-of-work IV: Mining

- A “miner” plans to mine the following block:

  ```
  Previous block & The coinbase transaction & All other transactions
  ```

- The miner consecutively adds a **NONCE** at the end of the block until the hash of the transaction is smaller than `TARGET(n)`.

Proof-of-work IV: Mining

- A “miner” plans to mine the following block:

  `Previous block & The coinbase transaction & All other transactions`

- The miner consecutively adds a **NONCE** at the end of the block until the hash of the transaction is smaller than `TARGET(n)`.

- For Difficulty=1 (answer in 0.02 seconds):

```
TARGET(1)=0900000000000000000000000000000000000000000000000000000000000000

Previous block & The coinbase transaction & All other transactions19

HASH IS = 04498fc1d57867a44032334e6e8b54cefd4ad39244fa080df9e383c7e762115d
```

Proof-of-work IV: Mining

- A “miner” plans to mine the following block:

```
Previous block & The coinbase transaction & All other transactions
```

- The miner consecutively adds a **NONCE** at the end of the block until the hash of the transaction is smaller than `TARGET(n)`.
- For Difficulty=1 (answer in 0.02 seconds):

```
TARGET(1)=0900000000000000000000000000000000000000000000000000000000000000

Previous block & The coinbase transaction & All other transactions19

HASH IS = 04498fc1d57867a44032334e6e8b54cefd4ad39244fa080df9e383c7e762115d
```

- For Difficulty=2 (answer in 0.20 seconds):

```
TARGET(1)=0090000000000000000000000000000000000000000000000000000000000000

Previous block & The coinbase transaction & All other transactions513

HASH IS = 0043e0cf1c92e209fd867349192e3f07f3a0bc2e842fd88b453aa9375bf753d1
```

Proof-of-work IV: Mining

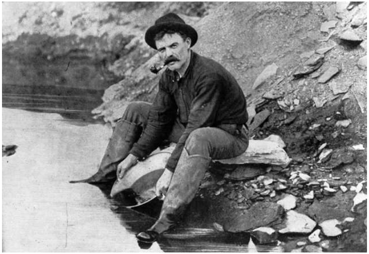
- And so on...
- Mining with my laptop:

Difficulty	Expected # of trials	NONCE	Time
1	28	19	0.02 sec
2	455	513	0.20 sec
3	7,282	12,953	3.93 sec
4	116,508	52,341	17.87 sec
5	1,864,140	1,829,359	570.00 sec
...			
18	8×10^{21}	???	$\sim$ 3.5 billion years!!!

- The number of trials increases exponentially. Forget about mining bitcoins with a laptop!

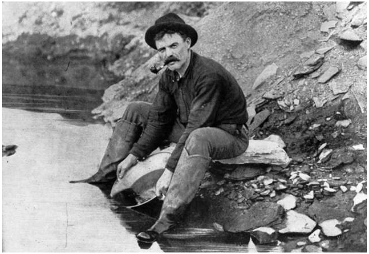
Modern mining

Proof-of-work = a miner found the right combination



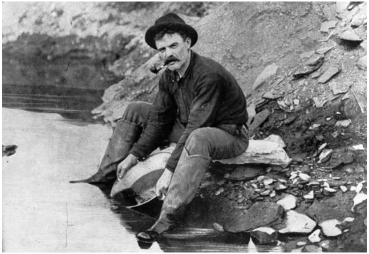
- Say miner node “Forty-Niner” finds the right combination and transmits the block to all its peers.

Proof-of-work = a miner found the right combination



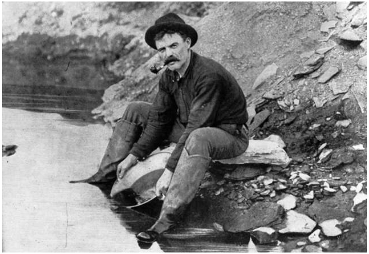
- Say miner node “Forty-Niner” finds the right combination and transmits the block to all its peers.
- Everyone can verify instantaneously if the combination is right
- On top of this, everyone can quickly verify if all transactions are valid **and not already spent**; and also if the Coinbase transaction is valid.

Proof-of-work = a miner found the right combination



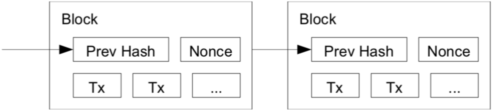
- Say miner node “Forty-Niner” finds the right combination and transmits the block to all its peers.
- Everyone can verify instantaneously if the combination is right
- On top of this, everyone can quickly verify if all transactions are valid **and not already spent**; and also if the Coinbase transaction is valid.
- This verification is a “proof-of-work”

Proof-of-work = a miner found the right combination



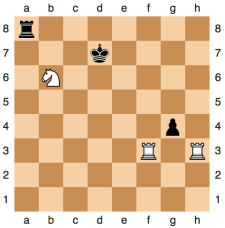
- Say miner node “Forty-Niner” finds the right combination and transmits the block to all its peers.
- Everyone can verify instantaneously if the combination is right
- On top of this, everyone can quickly verify if all transactions are valid **and not already spent**; and also if the Coinbase transaction is valid.
- This verification is a “proof-of-work”
- There is no incentive for “Forty-Niner” to spend energy to mine fake transactions. That would be a waste of money.
- The incentive (Coinbase transaction) is the secret sauce! (more on the risks generated by this later)

The immutable chain:

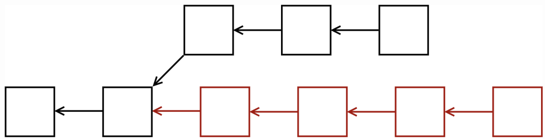


- It is thus possible to build a global list of valid transactions.
- The size of the Bitcoin blockchain reached approximately 149 gigabytes in December 2017.
- Because history is immutable, the double-spend problem is solved.
- George Orwell would love this. It works!

... until it doesn't. The “Forking Attack”:



- Consider a miner named “Ministry of Truth” (MoT)
- MoT has the majority of hash power (> 0.5)
- With this huge computing power, MoT can go back in time and double-spend some money:



Readings

- Chapter 5 in:

  Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *“Bitcoin and cryptocurrency technologies.”* (2016). Princeton University Press
- Chapter 10 in:

  Antonopoulos, Andreas M., *“Mastering Bitcoin,”* (2017)

Outline

I What is a Bitcoin? What is a blockchain? 3

II Gambling with the Bitcoin 13

- Bitcoin and the S&P 500 14
- Bitcoin and the VIX 19
- Bitcoin and gold 20
- Bitcoin and "attention" 21
- Volatility and other risk measures 22
- Is Bitcoin a bubble? Crypto mania 23

III Mechanics of the Bitcoin 26

- Preliminaries 27
- Signing transactions 30
- Proof-of-work & Mining 37

IV Bitcoin Futures 50

V Getting Started with Bitcoin 57

VI Risks & Issues 59

Bitcoin Futures

- Introduced in December 2017 by Chicago Mercantile Exchange (CME) and Chicago Board Options Exchange (CBOE)
- Benefits:
  - Increased transparency
  - Efficient price discovery
  - Centralized clearing
  - Improved liquidity
  - Better risk management
  - Easier to speculate
- No need for a digital wallet, because Bitcoin futures are financially-settled and therefore do not involve the exchange of Bitcoin.
- Bitcoin is in limited supply and it is hard to short $\Rightarrow$ need a market for lending (e.g., Genesis Global Trading)

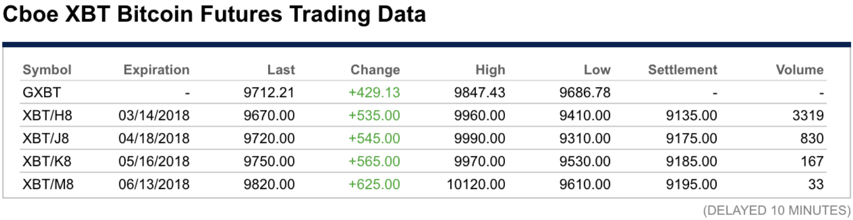
CBOE XBT Bitcoin Futures

- **Listing Date:** December 10, 2017
- **Description:** Cash-settled futures contracts that are based on the Gemini Exchange auction (“Gemini Exchange Auction”) price for bitcoin in U.S. dollars
- **Contract Multiplier:** 1 bitcoin
- **Ticker Symbols:** XBT
- **Contract Expirations:** The Exchange may list for trading up to four near-term expiration weeks (“weekly” contracts), three near-term serial months (“serial” contracts), and three months on the March quarterly cycle (“quarterly” contracts). Initially the exchange will list three near-term serial months.
- **Margin Requirements:** Maintenance = 40%

  Initial margin = 1.10 × Maintenance

  (brokerage firms may impose higher margin requirements)

CBOE XBT Bitcoin Futures (March 2018)



Cboe XBT Bitcoin Futures Trading Data

Symbol	Expiration	Last	Change	High	Low	Settlement	Volume
GXBT	-	9712.21	+429.13	9847.43	9686.78	-	-
XBT/H8	03/14/2018	9670.00	+535.00	9960.00	9410.00	9135.00	3319
XBT/J8	04/18/2018	9720.00	+545.00	9990.00	9310.00	9175.00	830
XBT/K8	05/16/2018	9750.00	+565.00	9970.00	9530.00	9185.00	167
XBT/M8	06/13/2018	9820.00	+625.00	10120.00	9610.00	9195.00	33

(DELAYED 10 MINUTES)

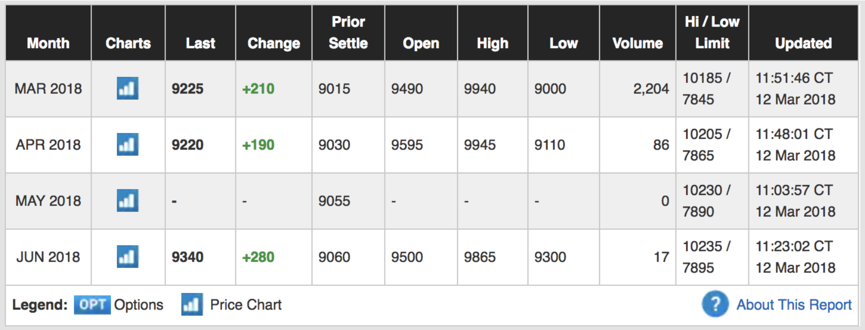
- Various brokers offer trading in XBT futures:
  TD Ameritrade, E*TRADE, InteractiveBrokers, Silexx, etc.

CME BTC Bitcoin Futures

- **Listing Date:** December 17, 2017
- **Ticker Symbol:** BTC
- **Contract Unit:** 5 bitcoin, as defined by the CME CF Bitcoin Reference Rate (BRR), which aggregates bitcoin trading activity across major bitcoin spot exchanges between 3:00 p.m. and 4:00 p.m. London time.
- **Settlement** Cash settled by reference to Final Settlement Price, equal to the CME CF Bitcoin Reference Rate (BRR) on Last Day of Trading.
- **Listed Contracts:** Monthly contracts listed for the nearest 2 months in the March quarterly cycle (Mar, Jun, Sep, Dec) plus the nearest 2 serial months not in the March quarterly cycle.
- **Margin Requirements:** Maintenance margin $=$ 43%

  Initial margin $= 1.1 \times$ Maintenance

CME BTC Bitcoin Futures (March 2018)



Month	Charts	Last	Change	Prior Settle	Open	High	Low	Volume	Hi / Low Limit	Updated
MAR 2018	📊	**9225**	+210	9015	9490	9940	9000	2,204	10185 / 7845	11:51:46 CT 12 Mar 2018
APR 2018	📊	**9220**	+190	9030	9595	9945	9110	86	10205 / 7865	11:48:01 CT 12 Mar 2018
MAY 2018	📊	**-**	-	9055	-	-	-	0	10230 / 7890	11:03:57 CT 12 Mar 2018
JUN 2018	📊	**9340**	+280	9060	9500	9865	9300	17	10235 / 7895	11:23:02 CT 12 Mar 2018

Legend: OPT Options 📊 Price Chart ? About This Report

More information

- CBOE:

  http://cfe.cboe.com/cfe-products/xbt-cboe-bitcoin-futures
- CME:

  http://www.cmegroup.com/trading/equity-index/us-index/bitcoin.html

Outline

I What is a Bitcoin? What is a blockchain? 3

II Gambling with the Bitcoin 13

- Bitcoin and the S&P 500 14
- Bitcoin and the VIX 19
- Bitcoin and gold 20
- Bitcoin and “attention” 21
- Volatility and other risk measures 22
- Is Bitcoin a bubble? Crypto mania 23

III Mechanics of the Bitcoin 26

- Preliminaries 27
- Signing transactions 30
- Proof-of-work & Mining 37

IV Bitcoin Futures 50

V Getting Started with Bitcoin 57

VI Risks & Issues 59

Getting Started with Bitcoin

- The logic behind the Bitcoin is that it is a fast, cheap and easy way to send and receive money.

Getting Started with Bitcoin

- The logic behind the Bitcoin is that it is a fast, cheap and easy way to send and receive money.
- Not yet. Let's say I want to start with \$100 worth of Bitcoin...
  1. Went to Coinbase.com, connected my bank account, and bought \$100 worth of Bitcoin. I got \$96.16 ⇒ fees are about 4%.
  2. Then I needed a "wallet." Went to Blockchain.com and downloaded a wallet. Transferred all my Bitcoins from Coinbase.com to my wallet. I got \$93.61 in my wallet ⇒ "network fees" of about 3%.
- It's not cheap to get started. What if I decide to sell all Bitcoins and get dollars back? I will probably end up with \$85!

Getting Started with Bitcoin

- The logic behind the Bitcoin is that it is a fast, cheap and easy way to send and receive money.
- Not yet. Let's say I want to start with \$100 worth of Bitcoin...
  1. Went to Coinbase.com, connected my bank account, and bought \$100 worth of Bitcoin. I got \$96.16 ⇒ fees are about 4%.
  2. Then I needed a "wallet." Went to Blockchain.com and downloaded a wallet. Transferred all my Bitcoins from Coinbase.com to my wallet. I got \$93.61 in my wallet ⇒ "network fees" of about 3%.
- It's not cheap to get started. What if I decide to sell all Bitcoins and get dollars back? I will probably end up with \$85!
- It was not easy. On top of this, I have this feeling that I sent \$100 into a void (more about risks in a few slides).
- I'm not sure how fast it is: — *Jan 10, 2018: Miami Bitcoin Conference Stops Accepting Bitcoin Due to Fees and Congestion*
- Is it that easy to pay with Bitcoins at the grocery store?

Outline

I What is a Bitcoin? What is a blockchain? 3

II Gambling with the Bitcoin 13

- Bitcoin and the S&P 500 14
- Bitcoin and the VIX 19
- Bitcoin and gold 20
- Bitcoin and “attention” 21
- Volatility and other risk measures 22
- Is Bitcoin a bubble? Crypto mania 23

III Mechanics of the Bitcoin 26

- Preliminaries 27
- Signing transactions 30
- Proof-of-work & Mining 37

IV Bitcoin Futures 50

V Getting Started with Bitcoin 57

VI Risks & Issues 59

Risks & Issues

- Volatility (see slide 22)
- Forks (see slide 48). The blockchain can also split because various groups cannot agree about a modification, e.g., Bitcoin Cash:
  - The block size limit is 1 MB.
  - A group of people decided to increase Bitcoin transaction capacity eight times. The change, called a hard fork, took effect on August 1, 2017
- Free entry: everyone can create a substitute, in unlimited supply (although there are network effects, so it might be tough to replace the Bitcoin). Maybe we will see a future with multiple big cryptocurrencies that "compete" among each other?
- How "decentralized" it really is? Two pools control near half the mining in March 2018 (BTC.com and AntPool)

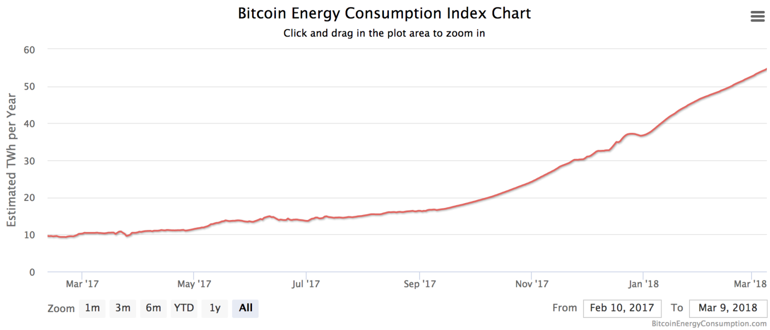
Bitcoins can “disappear”

- Mt. Gox was a bitcoin exchange based in Japan
- In 2014 it was handling over 70% of all Bitcoin transactions worldwide
- In February 2014, Mt. Gox suspended trading, closed its website, and filed for bankruptcy
- Approximately 850,000 bitcoins belonging to customers and the company were missing and likely stolen

Bitcoins can "disappear"

- Mt. Gox was a bitcoin exchange based in Japan
- In 2014 it was handling over 70% of all Bitcoin transactions worldwide
- In February 2014, Mt. Gox suspended trading, closed its website, and filed for bankruptcy
- Approximately 850,000 bitcoins belonging to customers and the company were missing and likely stolen
- **If a user loses a private key, then any asset associated with that key is lost**
- **"Bitcoins were stolen..." = "Private keys were found"**
- **Transactions cannot be reversed in case of error or fraud**

Energy consumption (wastage?)



From Feb 10, 2017 To Mar 9, 2018

- A theoretical outcome: "arms race" in which miners end up over-investing (Biais et al., *"The blockchain folk theorem,"* 2018)
- Can't miners solve a real problem? (e.g., simulations for weather forecasting, data crunching for Amazon)
- This would power half of households in California. Iceland expected to use more energy mining bitcoins than it will to power its homes (2018)

“It’s Magic!”

- The danger of “techno-solutionism”: the idea that all the problems in health, education, finance and so on can be solved with the blockchain seems a bit naive.
- Too much hype. A lot of “wishful thinking.”
- It’s techy, complicated. Some who get it become part of the cult
- Arthur C. Clarke:

  “Any sufficiently advanced technology is indistinguishable from magic.”
- It’s not magic! It will not solve all our problems!
- But, it’s a new technology. It might be revolutionary. It merits our attention and scrutiny. Economists should further study its structure.

Disagreement

- Nouriel Roubini (NYU economist):
  "The biggest bubble in history comes down crashing." Feb 2018
- Augustin Carstens (head of the Bank of International Settlements):
  "Bitcoin has become a combination of a bubble, a Ponzi scheme and an environmental disaster."
- Paul Krugman (Nobel Prize in Economics, 2008):
  "Bitcoin is Evil."
- Bhagwan Chowdhry (Professor of Finance, UCLA):
  "I (Shall Happily) Accept the 2016 Nobel Prize in Economics on Behalf of Satoshi Nakamoto"
- Kenneth Rogoff (Harvard economist):
  "A decade from now, bitcoin is more likely to be $100 than $100,000."

References

Andrei, D. and J. Cujean (2017).
Information percolation, momentum and reversal.
Journal of Financial Economics 123(3), 617–645.

Andrei, D. and M. Hasler (2014).
Investor attention and stock market volatility.
The review of financial studies 28(1), 33–72.

Antonopoulos, A. M. (2017).
Mastering Bitcoin: Programming the Open Blockchain.
" O'Reilly Media, Inc.".

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta (2018).
The blockchain folk theorem.

Huberman, G., J. D. Leshno, and C. C. Moallemi (2017).
Monopoly without a monopolist: An economic analysis of the bitcoin payment system.

References (cont'd)

- Lamport, L., R. Shostak, and M. Pease (1982).
  The byzantine generals problem.
  ACM Transactions on Programming Languages and Systems (TOPLAS) 4(3), 382–401.

- Nakamoto, S. (2008).
  Bitcoin: A peer-to-peer electronic cash system.

- Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder (2016).
  Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.
  Princeton University Press.

- Orwell, G. (2009).
  Nineteen eighty-four.
  Everyman's Library.