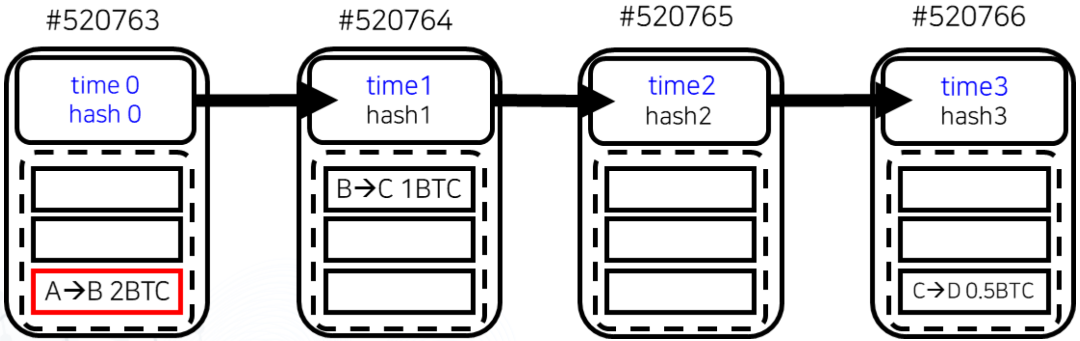
Goal of this lecture note

- Value Transfer over Internet
- Satoshi Nakamoto Cryptography Mailing List
- Brief History of Bitcoin

1 Bitcoin Enables Value Transfer over Internet!



1 Bitcoin Enables Value Transfer over Internet!

- Bitcoin is a P2P network of nodes
  - Attracts P2P nodes.
  - Has them talk to each other via Internet.
  - Has them maintain Blockchain.
  - Has each block time stamped and store transactions.
  - Has the blocks chained together with a hashing function.
  - Has a block include the hash or a summary of the past block.

1 Bitcoin Enables Value Transfer over Internet!

- Bitcoin is a P2P network of nodes
  - Puts PoW to make accidental or intentional block alteration very difficult.
  - Leaves the Blockchain open for public viewing.

1 Bitcoin Enables Value Transfer over Internet!

- Bitcoin has enabled P2P transactions over the Internet!
  - Bitcoin enables, communication of a digital message such as "A gives B a single coin" works like an in-person transfer of cash over the Internet.
  - Just by sending a digital message over the Internet, one can transfer a real value.
  - Namely, one can transfer a coin, a valuable digital asset, to anyone over the Internet without going through a trusted third party.

1 Bitcoin Enables Value Transfer over Internet!

- Bitcoin works just like an in person cash transfer. But how?
  - Each transaction is verified before being written into Blockchain.
  - Only have the verified transactions recorded in the ledger.
  - Once recorded, every block is sealed in an immutable way that the content cannot be altered.

1 Bitcoin Enables Value Transfer over Internet!

- For example, you want to buy a beer at a convenient store.

Could we do the similar thing with a counter party over the Internet?

1 Bitcoin Enables Value Transfer over Internet!

- A → B 2 BTC
  - Suppose a transaction of coin transfer from A to B
  - The difficulty is obvious in this case.
    - It is easy to make copies since it is a digital message.
    - Double spending attempt can be made
      A → C 2 BTC
  - Alteration of messages can occur
    - A′ instead of A, B′ instead of B, 3 BTC rather than 2 BTC
    - Causes include network errors and frauds

1 Bitcoin Enables Value Transfer over Internet!

- Transaction
  - Thus, there are three parts to a transaction via a message A→B 2BTC

    1. Verification of ownership
    2. Double spending free
    3. Verified transactions are scribed into the Blockchain

1 Bitcoin Enables Value Transfer over Internet!

- Explanation of Transaction

  Solution

  - As the ledger is openly published and shared in the P2P computers in the Internet, any transaction can be verified for the validity of ownership.
  - Being able to refer to Blockchain record anytime and anywhere, double spending can be checked against and deterred.

1 Bitcoin Enables Value Transfer over Internet!

- Explanation of Transaction

  Solution

  - Blockchain is a digital ledger whose content cannot be altered once recorded into it.

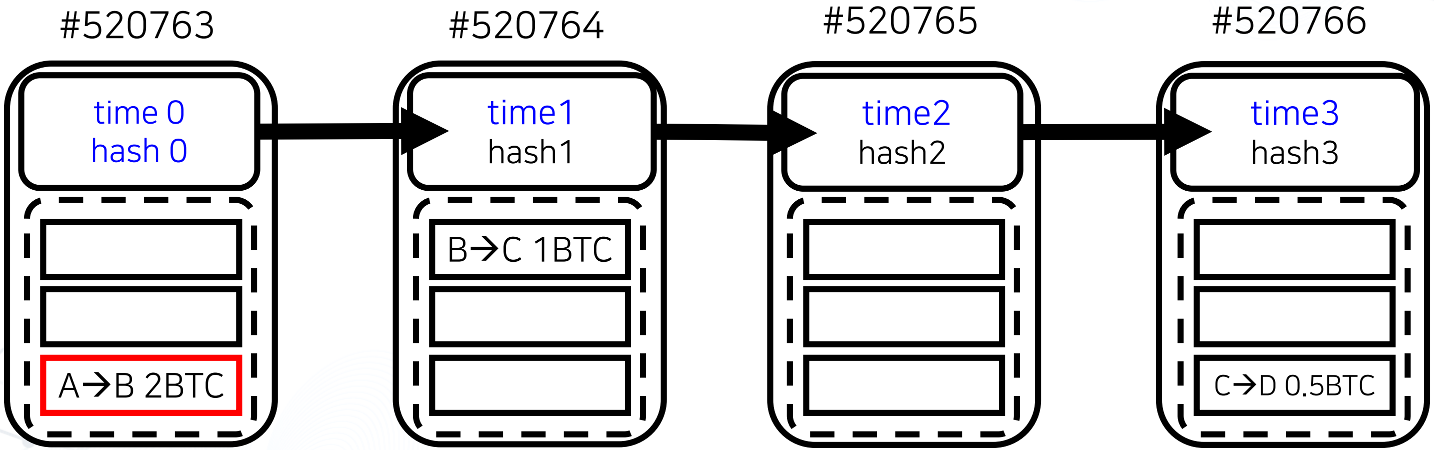
    - Blockchain means also a new cryptographic technology which is to resolve the issue how to keep the content of the digital file unaltered once recorded.

"Blockchain is believed to have many usages beyond currency"

1 Bitcoin Enables Value Transfer over Internet!

- A Blockchain is a digital book with a series of bound pages
  - Time 0: A (Sign of A) gives B two coins.
  - Time 1: B (Sign of B) gives C one coin.
  - Time 2: Empty
  - Time 3: C (Sign of C) gives D 0.5 coin.

1 Bitcoin Enables Value Transfer over Internet!



1 Bitcoin Enables Value Transfer over Internet!

- Blockchain is an open ledger in which transactions are recorded
  - What's written inside a block are the transactions and the timestamp of the block.
  - A series of such files connected in order of time is called Blockchain.

1 Bitcoin Enables Value Transfer over Internet!

- Blockchain is an open ledger in which transactions are recorded
  - Namely, Blockchain is a digital ledger with many bound pages.
    - As given above, coin transactions are recorded with time stamps.
    - Taking a look inside this ledger, one can always verify if a party owns enough coin to make a transaction or not.
    - From viewing the ledger, anybody can see how much coin belongs to a party.

1 Bitcoin Enables Value Transfer over Internet!

- Immutability
  - Proof-of-work (PoW) is defined to be a time consuming computational task.
  - A PoW is said to be heavy when the PoW task is very difficult to complete.
  - Bitcoin requires a heavy PoW to be used to make each chain connection.
  - This makes any accidental or intentional block alteration very difficult.

1 Bitcoin Enables Value Transfer over Internet!

- Immutability
  - To complete a PoW task, one computer may have to spend several years to complete a single chain connection task from a particular block to the next block.
  - How can one deceive others without alerting them for alteration?
  - One has to re-do all the PoWs in the chain starting from the very block to which an intentional alteration is made.

1 Bitcoin Enables Value Transfer over Internet!

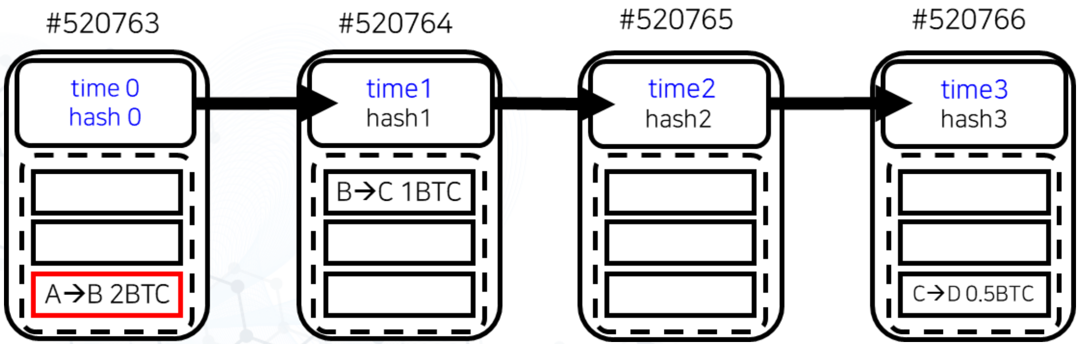
- Immutability
  - To deceive others, one needs to re-do all the PoW, all the computation already done to the chain very quickly.
  - To make an alteration is thus almost impossible difficult task to do.

1 Bitcoin Enables Value Transfer over Internet!

- Anonymity

  But please make no mistake

  - This ledger uses cryptographic hash values and gibberish looking addresses.
  - For example, A above, and B, C, D as well, represents the address of an individual.



1 Bitcoin Enables Value Transfer over Internet!

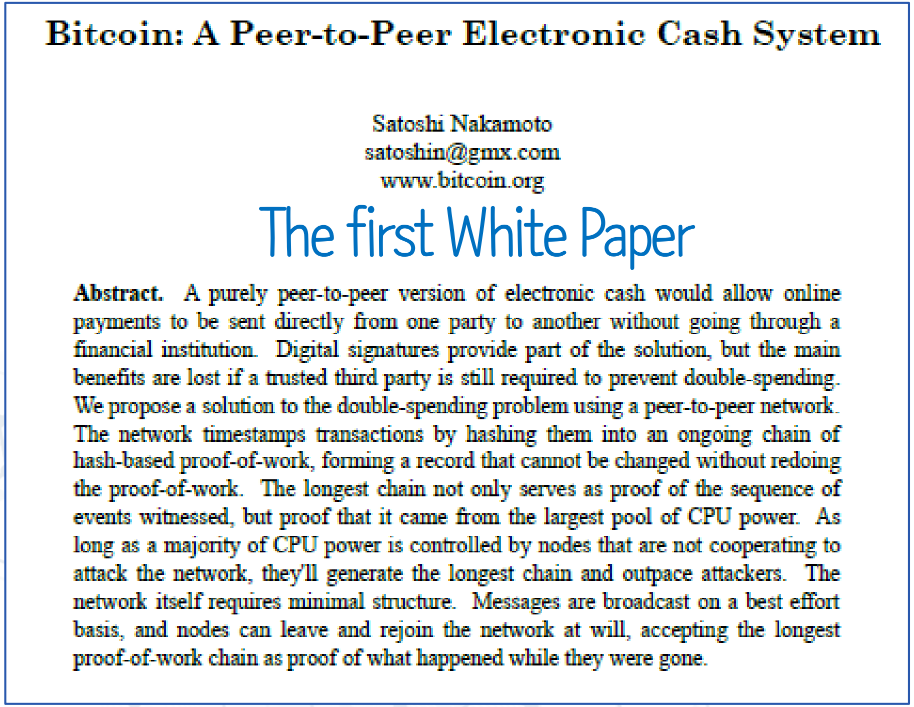
- Anonymity

  But please make no mistake
  - The coin ownerships are given to these cryptographically addresses.
  - Only can the right person who has the private key to the said address claim the ownership of the coin.

1 Bitcoin Enables Value Transfer over Internet!

- Bitcoin Blockchain Verticals
  - Decentralized
  - Public
  - Immutability
  - Trust
  - Minting coins
  - Anonymity
  - Security

2 Satoshi Nakamoto Cryptography Mailing List



Bitcoin: A Peer-to-Peer Electronic Cash System

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

The first White Paper

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.

2 Satoshi Nakamoto Cryptography Mailing List

- Bitcoin P2P e-cash paper

  NOVEMBER 1, 2008 SATOSHI NAKAMOTO CRYPTOGRAPHY MAILING LIST

  - I’ve been working on a new electronic cash system that’s fully peer-to-peer, with no trusted third party.
  - The paper is available at: http://www.Bitcoin.org/Bitcoin.pdf

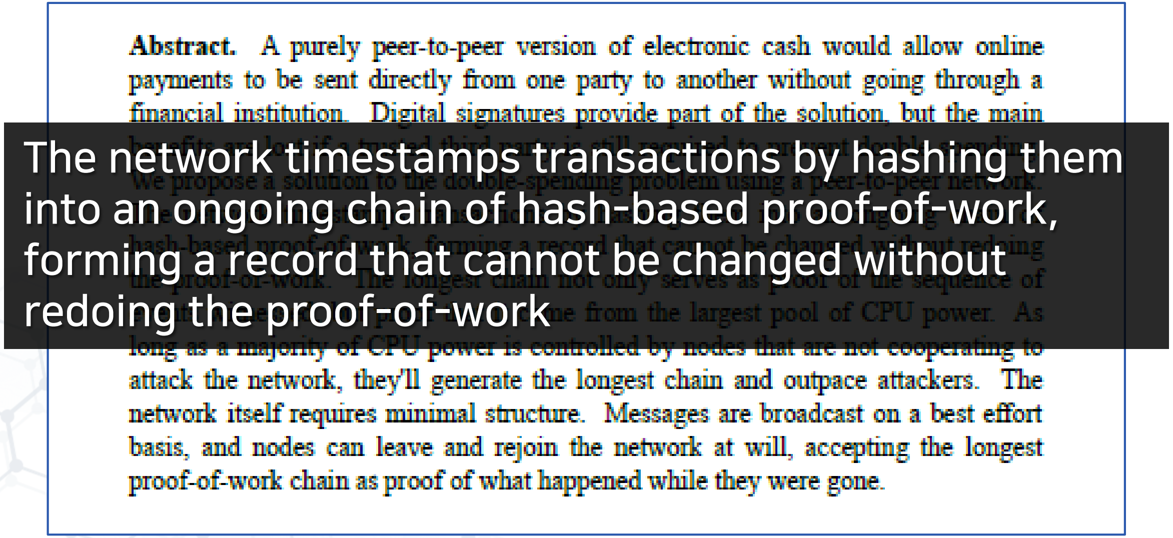
2 Satoshi Nakamoto Cryptography Mailing List

- Bitcoin P2P e-cash paper
  - The main properties are Double-spending is prevented with a peer-to-peer network.
  - No mint or other trusted parties.
  - Participants can be anonymous.
  - New coins are made from Hashcash style proof-of-work.
  - The proof-of-work for new coin generation also powers the network to prevent double-spending.

– Satoshi Nakamoto

2 Satoshi Nakamoto Cryptography Mailing List

- Bitcoin P2P e-cash paper
  - Bitcoin: A Peer-to-Peer Electronic Cash System



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

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.

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

2 Satoshi Nakamoto Cryptography Mailing List

- Re: Bitcoin P2P e-cash paper
  NOVEMBER 3, 2008 SATOSHI NAKAMOTO CRYPTOGRAPHY MAILING LIST
  - As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers.
  - But they don't. Bad guys routinely control zombie farms of 100,000 machines or more.

– Anonymous

2 Satoshi Nakamoto Cryptography Mailing List

- Re: Bitcoin P2P e-cash paper
  - People I know who run a blacklist of spam sending zombies tell me they often see a million new zombies a day.
  - This is the same reason that hashcash can't work on today's Internet - the good guys have vastly less computational firepower than the bad guys.

– Anonymous

2 Satoshi Nakamoto Cryptography Mailing List

- Re: Re: Bitcoin P2P e-cash paper
  NOVEMBER 3, 2008 SATOSHI NAKAMOTO CRYPTOGRAPHY MAILING LIST
  - Thanks for bringing up that point.
  - I didn't really make that statement as strong as I could have. The requirement is that the good guys collectively have more CPU power than any single attacker.

2 Satoshi Nakamoto Cryptography Mailing List

- Re: Re: Bitcoin P2P e-cash paper
  - There would be many smaller zombie farms that are not big enough to overpower the network, and they could still make money by generating Bitcoins. The smaller farms are then the “honest nodes”
    (I need a better term than “honest”).

2 Satoshi Nakamoto Cryptography Mailing List

- Re: Re: Bitcoin P2P e-cash paper
  - The more smaller farms resort to generating Bitcoins, the higher the bar gets to overpower the network, making larger farms also too small to overpower it so that they may as well generate Bitcoins too.
  - According to the “long tail” theory, the small, medium and merely large farms put together should add up to a lot more than the biggest zombie farm.

2 Satoshi Nakamoto Cryptography Mailing List

- Re: Re: Bitcoin P2P e-cash paper
  - Even if a bad guy does overpower the network, it's not like he's instantly rich. All he can accomplish is to take back money he himself spent, like bouncing a check.

2 Satoshi Nakamoto Cryptography Mailing List

- Re: Re: Bitcoin P2P e-cash paper
  - To exploit it, he would have to buy something from a merchant, wait till it ships, then overpower the network and try to take his money back.
  - I don't think he could make as much money trying to pull a carding scheme like that as he could by generating Bitcoins. With a zombie farm that big, he could generate more Bitcoins than everyone else combined.

2 Satoshi Nakamoto Cryptography Mailing List

- Re: Re: Bitcoin P2P e-cash paper
  - The Bitcoin network might actually reduce spam by diverting zombie farms to generating Bitcoins instead.

– Satoshi Nakamoto

2 Satoshi Nakamoto Cryptography Mailing List

- Re: Bitcoin P2P e-cash paper
  NOVEMBER 7, 2008 SATOSHI NAKAMOTO CRYPTOGRAPHY MAILING LIST
  - Lengthy exposition of vulnerability of a system to use-of-force monopolies elided.
  - You will not find a solution to political problems in cryptography.

2 Satoshi Nakamoto Cryptography Mailing List

- Re: Re: Bitcoin P2P e-cash paper
  NOVEMBER 7, 2008 SATOSHI NAKAMOTO CRYPTOGRAPHY MAILING LIST
  - Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years.
  - Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.

– Satoshi Nakamoto

3 Brief History

- Brief History of Bitcoin
  - Oct. 2009: $1 = 1,309 BTC
  - Feb. 2010: First Bitcoin market
  - May 2010: Pizza day (a pizza = 10,000 BTC)
  - Nov. 2010: Bitcoin $1 Million. $0.5/BTC
  - Feb. 2011: Bitcoin $ 206 Million
  - Mar. 2013: Bitcoin $1 Billion
  - Aug. 2013: Federal Judge Rules Bitcoin is Real Money

3 Brief History

- Brief History of Bitcoin
  - Dec. 2013: China CB, bars financial institutions from handling Bitcoin transactions.
  - Dec. 2014: Microsoft begins accepting Bitcoin payments.

3 Brief History

- ~2010: M. value created, Pizza Day
  - October 2009
    - Bitcoin receives an equivalent value in traditional currencies.
    - The New Liberty Standard established the value of a Bitcoin at $1 = 1,309 BTC.
    - The equation was derived so as to include the cost of electricity to run the computer that created the Bitcoins in the first place.

3 Brief History

- ~2010: M. value created, Pizza Day
  - February 2010
    - The world's first Bitcoin market is established by the now defunct dollar.

3 Brief History

- ~2010: M. value created, Pizza Day
  - May 2010
    - A programmer living in Florida named Laslo Hanyecz sends 10,000BTC to a volunteer in England, who spent about $25 to order Hanyecz a pizza from Papa John's.
    - Today that pizza is valued at £1,961,034 and stands as a major milestone in Bitcoin's history.

3 Brief History

- ~2010: M. value created, Pizza Day
  - November 2010
    - Bitcoin reaches $1 million. Based on the number of Bitcoins in circulation at the time, the valuation leads to a surge in Bitcoin value to $0.50/BTC.

3 Brief History

- 2013: Regulation started, “Bitcoin is money”

  - February 2011

    - Bitcoin reaches parity with the US dollar for the first time.
    - By June each Bitcoin is worth $31 giving the currency a market cap of $206 million.

3 Brief History

- 2013: Regulation started, “Bitcoin is money”
  - March 2013
    - The US Financial Crimes Enforcement Network (FINCEN) issues some of the world’s first Bitcoin regulation in the form of a guidance report for persons administering, exchanging or using virtual currency.
    - This marked the beginning of an ongoing debate on how best to regulate Bitcoin.

3 Brief History

- 2013: Regulation started, “Bitcoin is money”
  - March 2013
    - Bitcoin market capitalisation reaches $1b.

3 Brief History

- 2013: Regulation started, “Bitcoin is money”
  - August 2013
    - Federal Judge Mazzant claims: “It is clear that Bitcoin can be used as money” and “It can be used to purchase goods or services” in a case against Trendon Shavers, the so-called ‘Bernie Madoff of Bitcoin’ .
    - Bloomberg begins testing Bitcoin data on its terminal.
    - Although alternative tickers exist, endorsement from Bloomberg gives Bitcoin more institutional legitimacy.

3 Brief History

- 2013: Regulation started, “Bitcoin is money”
  - December 2013
    - China’s central bank bars financial institutions from handling Bitcoin transactions.
    - This ban was issued after the People’s Bank of China said Bitcoin is not a currency with “real meaning” and does not have the same legal status as fiat currency.
    - The ban reflects the risk Bitcoin poses to China’s capital controls and financial stability.
    - Today China remains the world’s biggest Bitcoin trader, with 80% of global Bitcoin transactions being processed in China.

3 Brief History

- 2015: Derivatives, Assets, Payments
  - December 2014
    - Tech giant Microsoft begins accepting Bitcoin payments.