Goal of this lecture note

- Bitcoin Networks
- Pre-cursors to Bitcoin
- Proof of Work-the Monopoly Problem
- Proof of X schemes
- Summary of Altcoins

1 Bitcoin Networks

- Test Bitcoin Network
- Main Bitcoin Network

1 Bitcoin Networks

- Experimental Test Bitcoin Network
  - Testnet runs the same code as the mainnet does, but can be run as an experiment.
  - One can change the protocol and runs one's own bitcoin with
    - New free coins
    - Faster block generations time
    - Different issuance schedule
    - Difficulty

1 Bitcoin Networks

- Joining and Maintaining the network
  - Every peer in the Bitcoin network aims to maintain a minimum of 8 connections and a maximum 125 connections.
  - Peers listen on port 8333 for inbound connections.

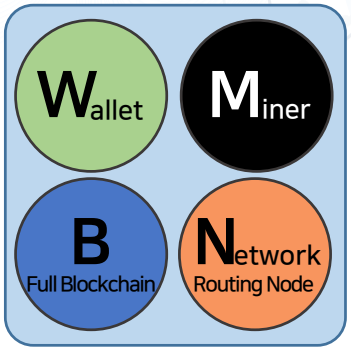
1 Bitcoin Networks

- Nodes Types and Roles
  - While nodes in the Bitcoin network are equal, they may take on different roles depending on the functionality they are supporting.
  - A bitcoin node is a collection of functions such as routing, blockchain database, mining, and wallet services.

Andreas M. Antonopoulos,『Mastering Bitcoin』, O'reilly, 2010

1 Bitcoin Networks

- Nodes Types and Roles
  - Each node has the routing function to participate in the network.
  - Full node has all four functions.
  - Wallet node has W and N.
  - Miner node has M, B, and N.
  - Full blockchain node has B and N.



Andreas M. Antonopoulos,『Mastering Bitcoin』, O'reilly, 2010

2 Pre-cursors to Bitcoin

- PoW is a gold, or a coin.
- Hashcash (02')
- RPOW (03') is a centralized currency.
- B-money (98') is a decentralized currency.
- Karma (03') is a distributed currency.
- BitGold (05') is a distributed currency.

2 Pre-cursors to Bitcoin

- Hashcash by Adam Back
  - Proof-of-work used to limit email spam. (97')
  - PoW with a num. of high zero bits is a token. (02')
- Reusable POW (03') by Hal Finny is a centralized currency.
  - A server issues a coin in return for a PoW.
  - Coins are reusable and transferrable.
  - The server checks the validity.
- B-money (98') by Wei Dai
  - Uses PoW money and a set of servers (decentralized) for validation, and assumes unjammable broadcast channel.

2 Pre-cursors to Bitcoin

- Karma by Vishnumurthy et al.(03') is a distributed currency.
  - A bank set keeps track of coins in file sharing.
  - Coin creation is adjusted considering inflation and deflation.
- BitGold by Nick Szabo (05')
  - Metalic gold vs Bitgold
  - Suggested to chain the proof-of-work. (uses the last entry to create new puzzle and adjust difficulty)
  - But relied on IP addresses and thus vulnerable to Sybil attack.

2 Pre-cursors to Bitcoin

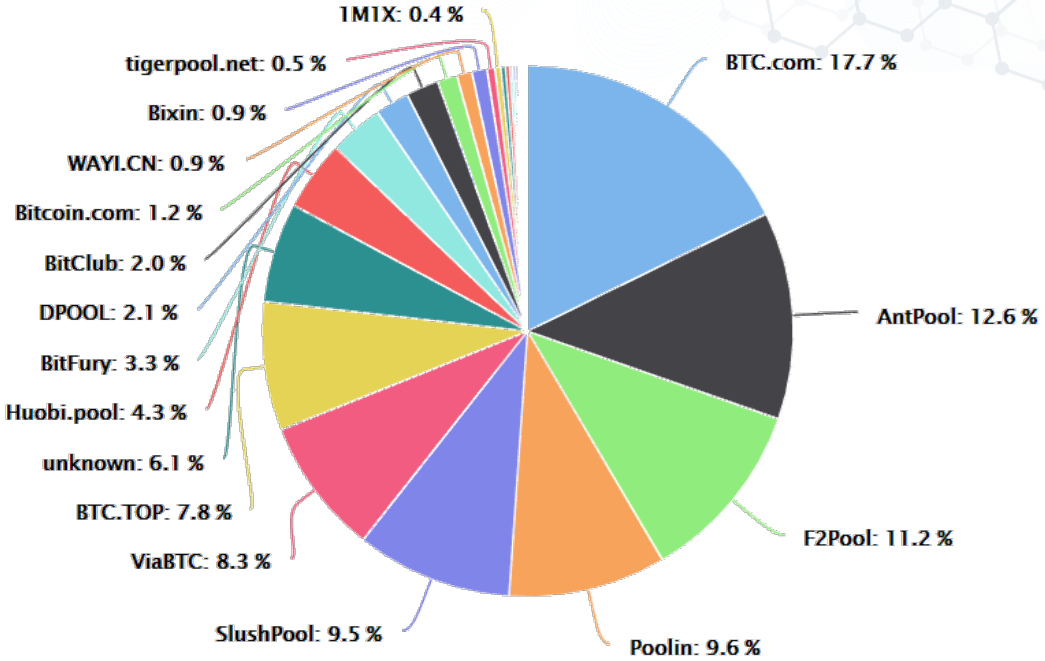
- Bitcoin
  - Inflation and deflation
  - Sybil attacks
  - Proof-of-work
  - One CPU one vote

3 Proof of Work-the Monopoly Problem

- Miners are rational profit seekers.
- They strive to make as much profit as possible.
- Mining operations are highly parallelizable, GPU mining quickly replaced CPU mining:
- FPGAs did GPUs.
- ASICs did FPGAs.

3 Proof of Work-the Monopoly Problem

- Proof of Work, any alternative?
  - PoW, monopolized today.
  - Handful of mining sites dominating.
  - The trust has been degraded.
  - No more one CPU one vote.
  - Rational profit seeking miners use ASICs now.



https://btc.com/ (기간: 2018. 09 ~ 2019. 09)

3 Proof of Work-the Monopoly Problem

- Items to consider for new PoW
  - One way is to diversify the puzzles and change them over time.
  - Considerations for new puzzles.
    - A puzzle should be difficult to solve but very easy to check.
    - The puzzle should be resistant to attacks.
    - Solution to the puzzle for a block should not be reusable.
    - Puzzle difficulty should be adjustable.
    - Anyone with a CPU who wishes to participate should be able to join.
    - Consensus must eventually be reached; there must be a common rule to resolve forks and to determine the main blockchain.

4 Proof of X Schemes

- Proof of Stake (PoS)/Delegated PoS
- Proof of Activity
- Proof of Publication

4 Proof of X Schemes

- Proof of Stake
  - Give higher PoW chance to a node with a higher stake (more coins).
  - Good: No high energy consumption
  - Bad: Rich gets richer problem
  - What if the node stays off line?
    - Delegated PoW

Reference: See page 2114, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 3, THIRD QUARTER 2016

4 Proof of X Schemes

- Proof of Stake based on Coin Age
  - *Coin age* is no. coins times the holding period.
    - Implemented in Peercoin (peercoin.net).
  - The difficulty of PoW is individually determined, inversely proportional to one's *coin age*.
  - If one finds a solution, one's *coin age* is reset.
  - Slowly increasing the chances of solving the puzzle next time.

Reference: See page 2114, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 3, THIRD QUARTER 2016

4 Proof of X Schemes

- Proof of Stake
  - In contrast to PoW, where the longest block chain survives, *coin age* PoS declares the block chain with the highest total sum of *destroyed coin age* as the main chain.
  - An attacker must hold a huge amount of coins.

4 Proof of X Schemes

- Proof of Stake
  - Good: Energy consumption is minimized.

[229] N. Houy, “It will cost you nothing to ‘kill’ a proof-of-stake cryptocurrency,”
Econ. Bull., vol. 34, no. 2, pp. 1038–1044, 2014.

4 Proof of X Schemes

- Proof of Stake
  - Bad
    - Coin age accumulates even when the node is not connected to the network.
    - Come online for reward go offline afterwards.
    - The lacking of sufficient number of online nodes, may facilitate attacks.

4 Proof of X Schemes

- Proof of Activity
  - In [234] the author notes higher activity produces a healthier economy.
  - Key Idea is to reward active peers.
  - Let a fresh coin accumulate age faster.
  - It is thus a combination of proof of work and proof of stake.

[234] L. Ren, “Proof of stake velocity: Building the social currency of the digital age,” Tech. Rep., Apr. 2014 [Online]. Available:http://www.reddcoin.com/papers/PoSV.pdf

4 Proof of X Schemes

- Proof of Activity
  - Hybrid of PoW and PoS.
  - Good: Saving in energy consumption
    - for p2p file sharing, e.g. BitTorrent.
  - Bad: Uses PoW. Thus still use a lot of energy. Uses PoS; coin hoarders still have higher chances of accumulating more rewards.

[234] L. Ren, “Proof of stake velocity: Building the social currency of the digital age,” Tech. Rep., Apr. 2014 [Online]. Available:http://www.reddcoin.com/papers/PoSV.pdf

4 Proof of X Schemes

- Proof of Publication
  - Documents and timestamps are hashed and secured by private key of the timestamping server.
  - But the server can easily backdate documents by hashing and signing a previous timestamp.
  - Linked chain of timestamps and use of a set of servers can prevent this problem.
  - But the approach comes with the premise of trusting the set of timestamping servers.
  - Thus, Sybil attacks shows up again.

4 Proof of X Schemes

- Proof of Publication
  - Recall the time-stamp server of the bitcoin white paper!
  - Bitcoin provides a secure distributed timestamping service, with an accuracy of about 10 min.

4 Proof of X Schemes

- Proof of Publication
  - Bitcoin can be used as a timestamping service.
  - Use cases include coin tosses [238], lotteries [239], or decentralized poker [240].
  - Multi Party Computing works without a central entity.

[238] A. Back and I. Bentov, "Note on fair coin toss via bitcoin," Computing Research Repository, Tech. Rep. abs/1402.3698, 2014.
[239] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Secure multiparty computations on bitcoin," in Proc. IEEE 35th Symp. Secur. Privacy (SP'14), May 2014, pp. 443–458.
[240] R. Kumaresan, T. Moran, and I. Bentov, "How to use bitcoin to play decentralized poker," in Proc. ACM 22nd Conf. Comput. Commun. Secur. (CCS'15:), Oct. 2015, pp. 195–206.

5 Summary of Altcoins

- Table IV – Summary of Altcoins and Extensions

	Approach	Distinct Feature (incl. References)	Sec.
Precursor	B-Money	Mining reward proportional to proof of work difficulty; requires a broadcast channel [7]	II-B, V-D, V-E
	Bit Gold	Chained proof of work [10]; Byzantine-resilient quorum [13]	III-B, V-D, V-E
	Karma	Distributed currency maintained by a bank set [8]	V-E
	RPOW	Centralized (reusable) proof of work exchange/ bank [9]	V-E
Altcoins	Bitshares (BTS)	Delegated proof of stake [231]	V-F
	Bytecoin (BCN)	Implements CryptoNote [190], which aims for unlinkable and untraceable transactions	V-C, V-E
	Counterparty (XCP)	Colored coin; used proof of burn	V-H, V-H
	Cryptonite (XCN)	Implements the mini block chain scheme [127]	IV-D
	Dash (DASH)	Formerly known as Darkcoin; implements native CoinJoin-like transactions [178]	V-C
	Dogecoin (DOGE)	Block payload holds TXIDs only; fast block generation	IV-D, V-E
	Litecoin (LTC)	Uses scrypt [214] to foster distributed power among miners	V-E
	Mastercoin (MSC)	Colored coin; exodus address	V-H
	Nextcoin (NXT)	Entirely proof of stake based	V-F
	Peercoin (PPC)	Identified coin age as alternative measure; proof of stake [227]	V-F
	Primecoin (XPM)	Proof of work with intrinsic value i. e. prime chains [218]	V-E
	Reddcoin (RDD)	Proof of stake velocity [234]	V-E
	RSCoin	Centrally controlled money supply with distributed verification [126]	IV-D
	Ripple (XRP)	Implements a novel Byzantine agreement protocol [200]	V-D
	Zerocash	Full-fledged altcoin, carrying on the ideas of Zerocoin [189]	V-C

5 Summary of Altcoins

- Table IV – Summary of Altcoins and Extensions

	Approach	Distinct Feature (incl. References)	Sec.
Altchains	Bitmessage	Secure messaging service [145]	IV-G
	Ethereum (Ether)	Turing complete smart contract processing [44], [45]	II-E
	Namecoin (NMC)	Key-value storage; realizes decentralized domain name coordination [143]	IV-G
	Permacoin	Decentralized file storage; proposes proof of retrievability [100]	V-E
Protocols / Extensions	CoinJoin	Uses multi-signature transactions to enhance privacy [160]	V-C
	CoinShuffle	Decentralized protocol to coordinate CoinJoin transactions [180]	V-C
	CoinSwap	Enables P2P-based trustless mixing [41]	V-C
	CommitCoin	Secure timestamping protocol [40]	V-H
	Mini block chain	Identifies individual block chain components [127]	IV-D
	Mixcoin	Mixing with accountability [174]	V-C
	Zerocoin	Unlinkable and untraceable transactions by employing zero knowledge proofs [187]	V-C