Sensible Cryptocurrencies

Ghada Almashaqbeh
Columbia University

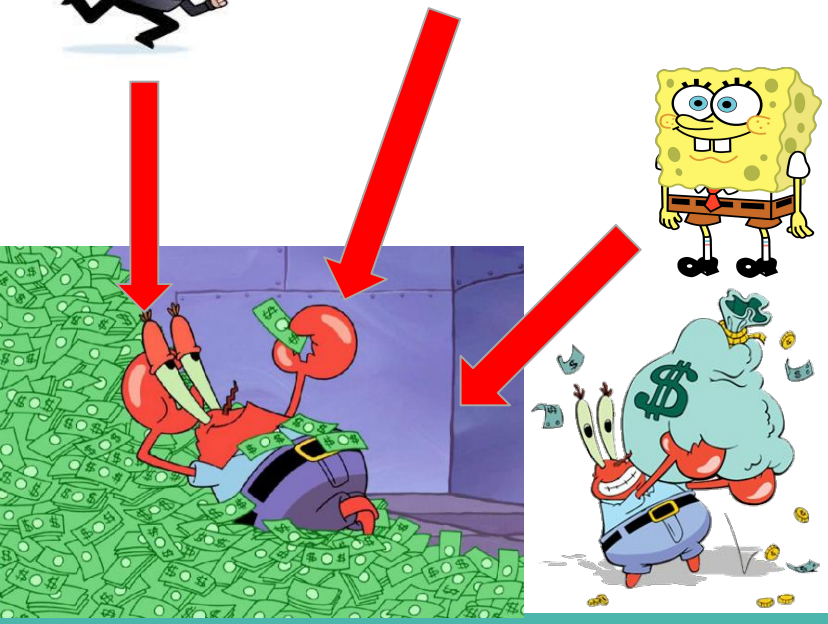
Ph.D Candidacy Exam
Nov. 2017

Outline

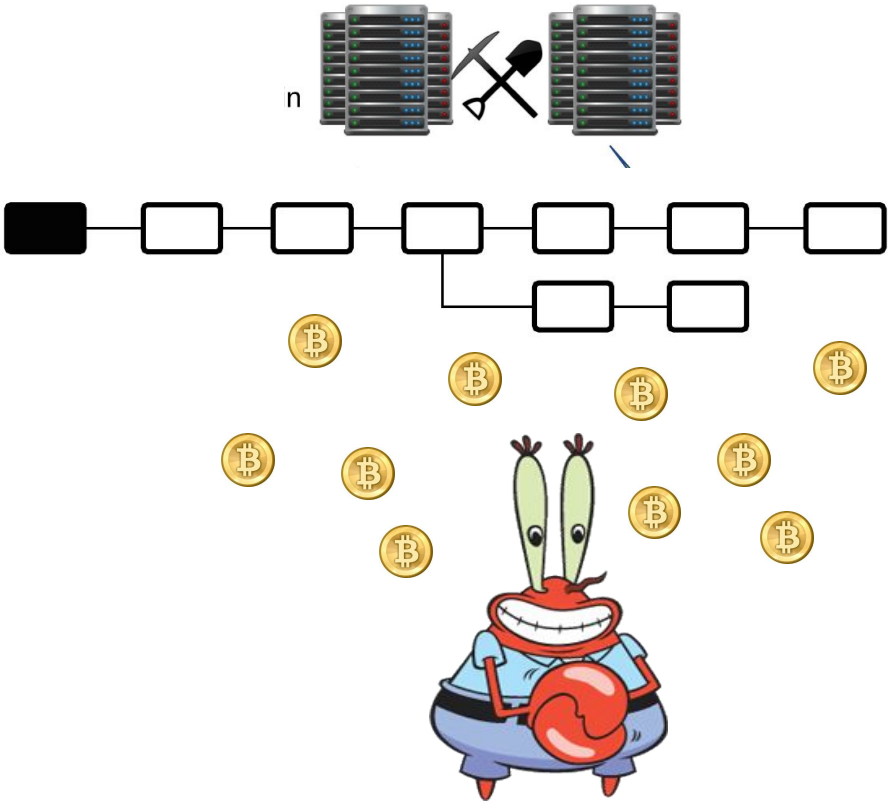
- Motivation.
- Main concepts.
  - Operation; transactions, mining, blockchain, consensus.
- Main problems and potential solutions:
  - Supported functionality,
  - mining and consensus,
  - anonymity,
  - micropayments.
- Security issues.
- The road ahead.
- References.

Once Upon A Time

Centralized Currency



Decentralized Currency



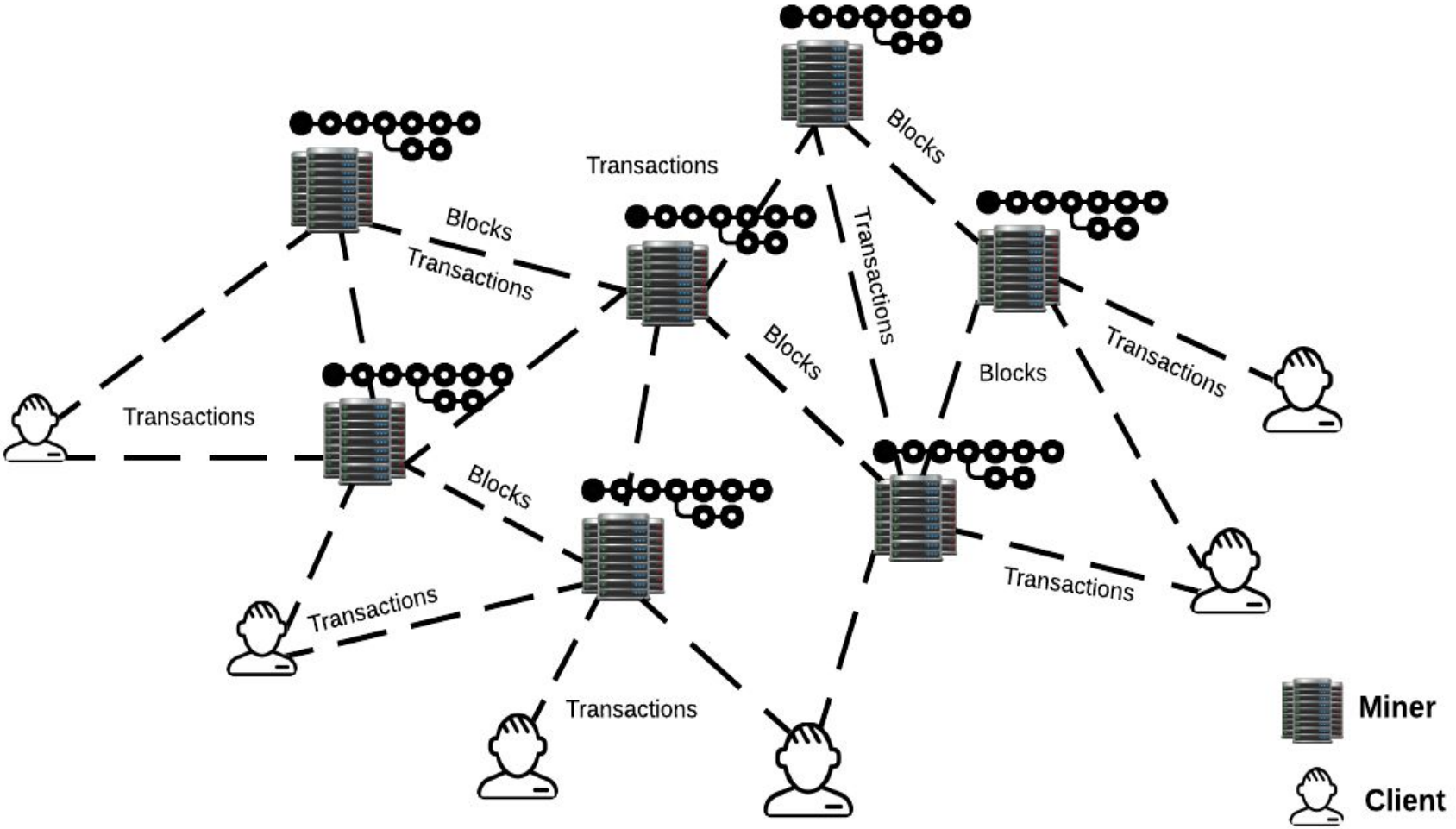
History

- A whitepaper posted online in 2008: “Bitcoin: A Peer-to-Peer Electronic Cash System”.
  - By Satoshi Nakamoto.
  - Described a distributed cryptocurrency system not regulated by any government.
- The system went live on January 2009.
- Now “Satoshi Nakamoto” is only associated with certain public keys on Bitcoin blockchain.
  - She/He/They was/were active on forums/emails/etc. till 2010.
- Currently there are ***1320 cryptocurrencies*** (https://coinmarketcap.com/).

Bitcoin in a Nutshell

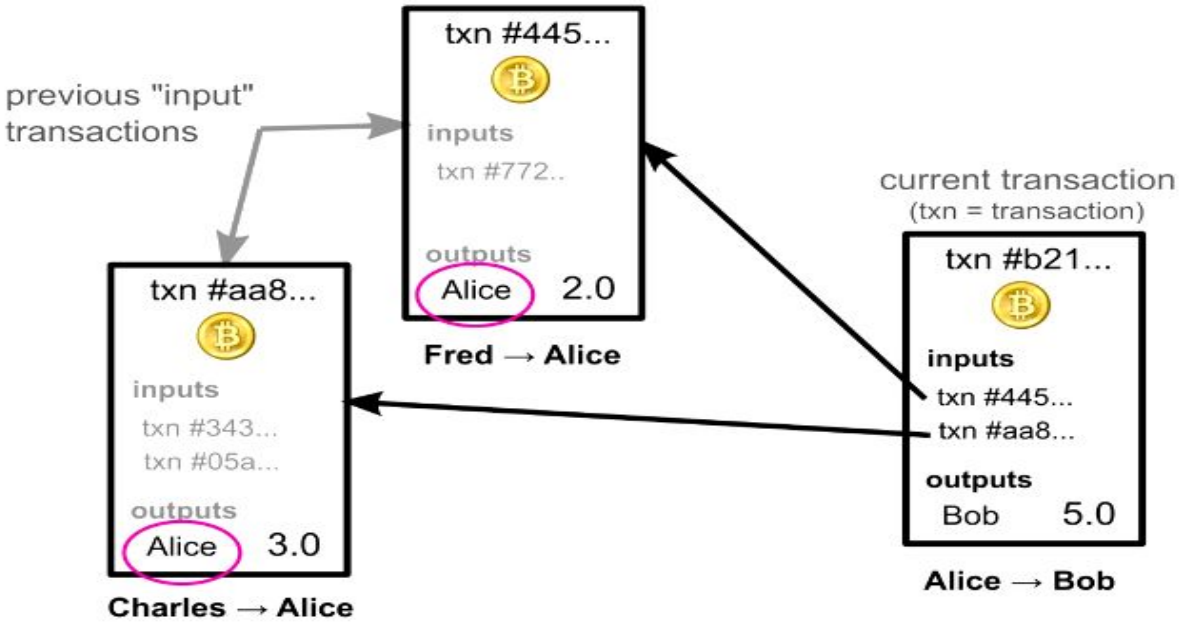
- A distributed currency exchange medium open to anyone to join.
- Utilize basic cryptographic primitives to control the money flow in the system.
- Main components:
  - **Players:** miners and clients.
  - **Transactions:** messages exchanged.
  - **Blockchain:** an append only log.
  - **Mining:** extending the blockchain.
  - **Consensus:** agreeing on the current state of the Blockchain.

Bitcoin Pictorially



Virtual Coins

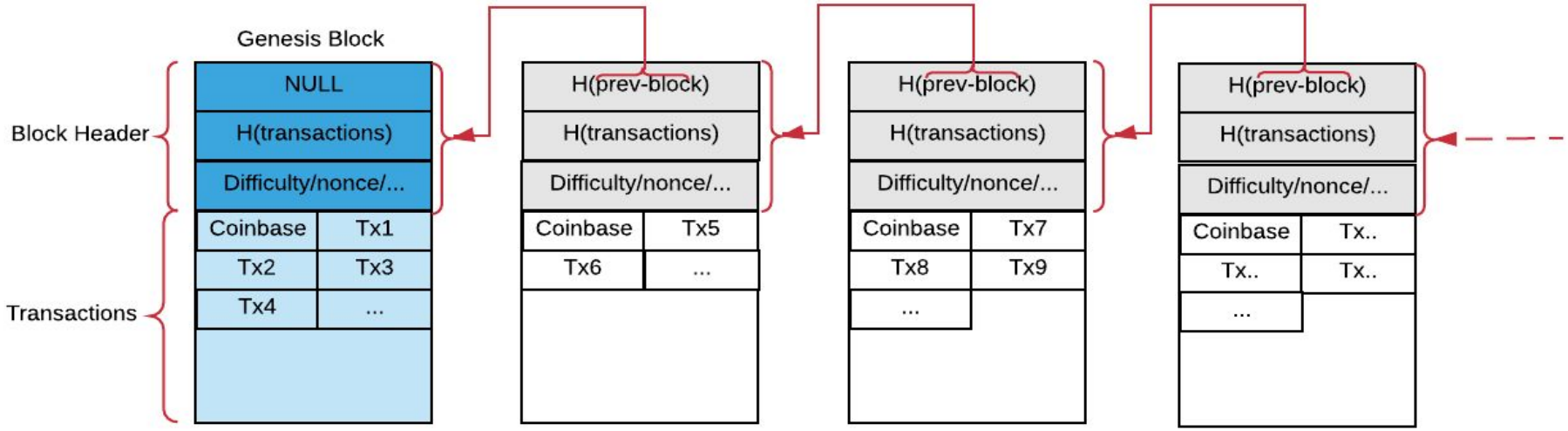
- Digital tokens, or transactions, that can be spent by providing signatures.
- No notion of accounts, track chains of transactions.
  - Wallets do that transparently for users.



Source: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Blockchain and Mining

- Append only log contains a full record of all transactions.
  - To handle double spending.
- Miners extend the blockchain by mining new blocks.
  - Solve a proof-of-work puzzle.
  - Collect monetary incentives.
- Clients track only their transactions.

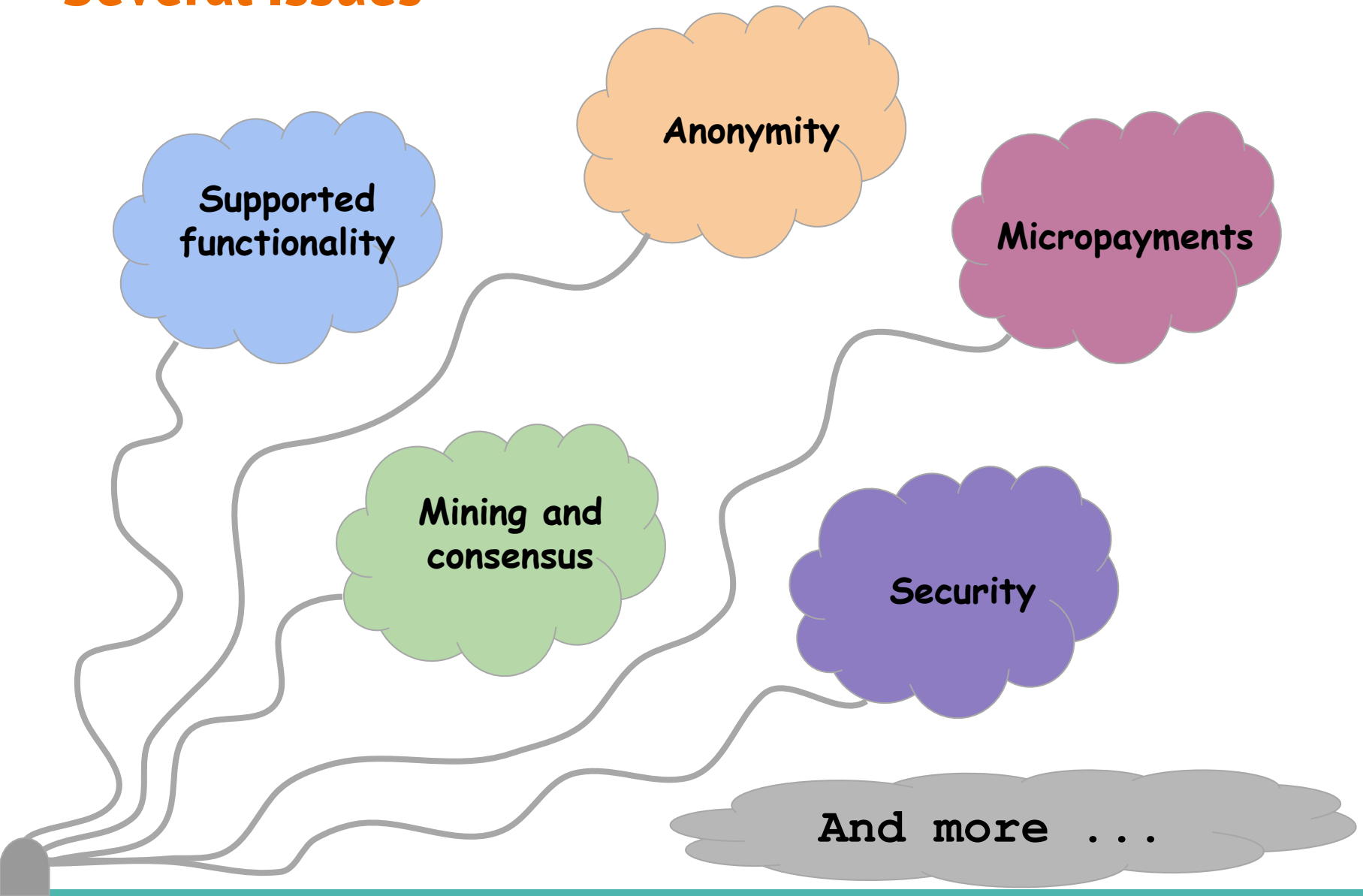


Consensus

- Miners hold , hopefully, consistent copies of the blockchain.
  - Only differ in the recent unconfirmed blocks.
- A miner votes for a block implicitly by building on top of it.
  - Mining power requirement handles Sybil attacks.
- Forking the blockchain means that miners work on different branches
  - Caused by network propagation delays, adversarial actions, etc.
  - Resolved by adopting the longest branch.

But …

Several Issues



Supported Functionality

Bitcoin

- **Vision:** distributed currency exchange medium with the virtue of simplicity.
  - Supports Turing-incomplete scripting language.
  - Tedious currency tracking model.

Ethereum

- **Vision:** a transaction-based state machine, or a virtual environment EVM, that runs distributed applications (Dapps).
  - Supports Turing-complete scripting language.
  - Global state, accounts, smart contracts, tokens, etc.

Ethereum

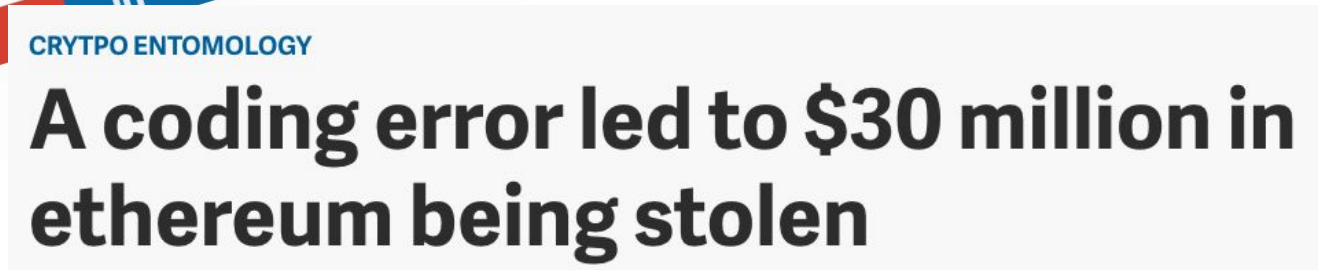
- Proposed by Vitalik Buterin in 2013 and went live in 2015.
- Users can issue two types of transactions: message calls and smart contracts deployment.
- Miners mine new blocks and implement smart contracts for clients.
  - Pay gas to prevent DoS against miners.
- The blockchain contains:
  - a full record of transactions,
  - smart contracts code,
  - and the global state of the network.
- Famously known to create new digital currencies on top of its platform called Ethereum Tokens.

Additional Features for Free?

- Security bugs in smart contracts.
- Gas cost (or transaction fees).
  - Limits the functionality scope of smart contracts.

Code was supposed to eliminate the need to trust humans. But humans, it turns out, are tough to take out of the equation.

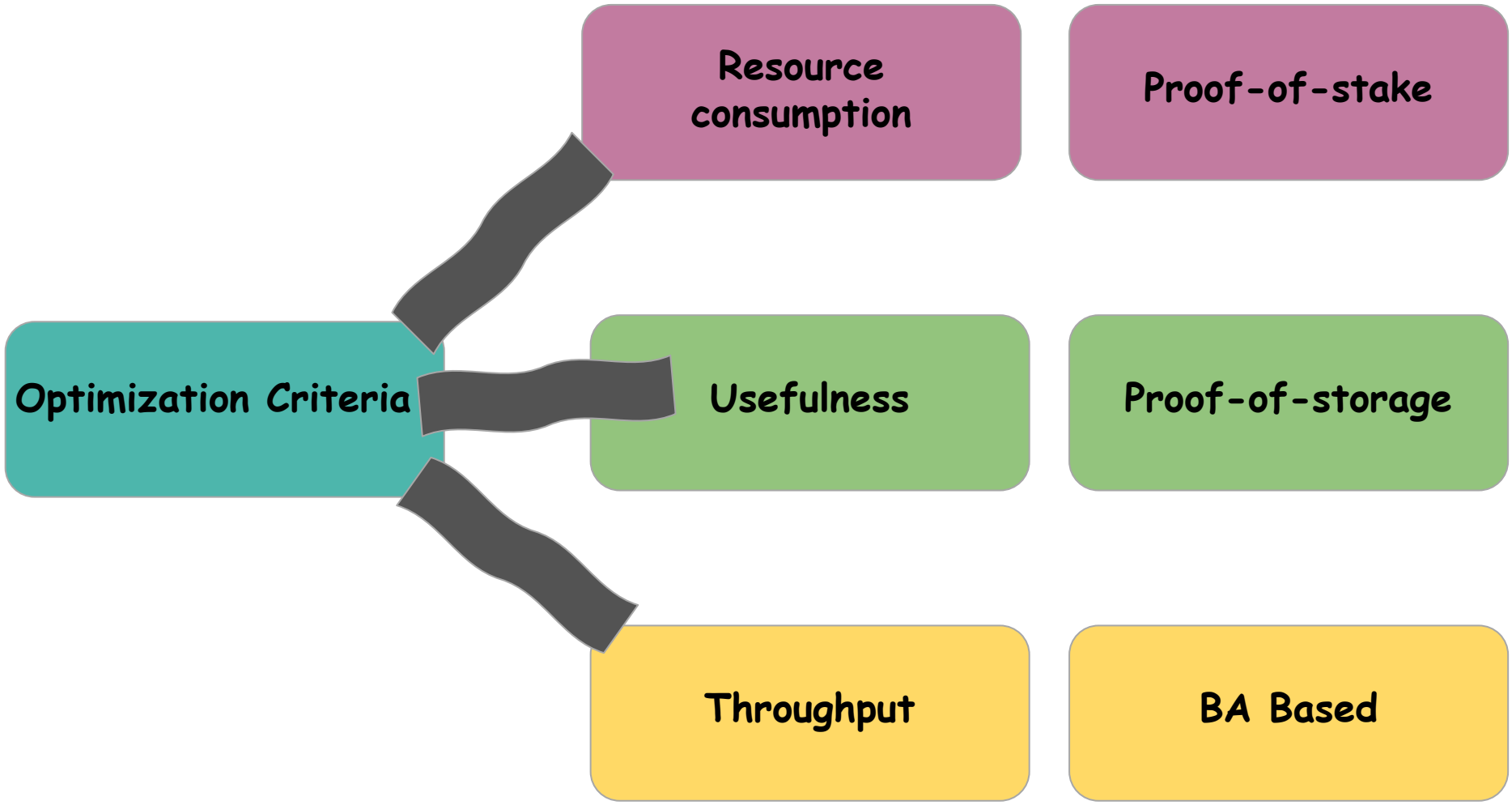
Source: https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/



Mining and Consensus

Bitcoin's PoW-Based Mining

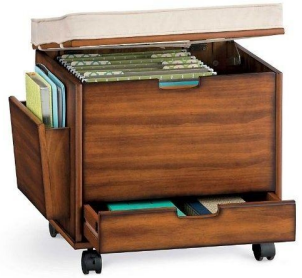
- Waste of resources.
  - In 2014 Bitcoin and Ireland's had comparable electricity consumption [O'Dwyer et al., 2014].
- Do the miners do useful computation?
- How about the transaction throughput?
- How long does it take to confirm a transaction?


Optimization Criteria
Resource consumption
Usefulness
Throughput
Proof-of-stake
Proof-of-storage
BA Based

Proof-of-Stake

- **Goal:** reduce energy consumption.
- Leader election is based on the amount of stake a miner holds.
  - Must be done in an unpredicted way.
- How to elect a leader? Examples,
  - Global verifiable random function, Algorand [Gilad et al., 2017].
  - MPC based coin flipping protocol, Ouroboros [Kiayias et al., 2017]
- Several issues:
  - Initial stake distribution.
    - Usually, mined using PoW then switch to pure PoS.
  - Nothing at stake attack.
    - Financial punishments, checkpoints.
  - Wealth distribution.

Proof-of-Storage



- **Different flavors:**
  - proof-of-space [Dziembowski et al., 2015],
  - proof-of-spacetime [Moran et al., 2016],
  - proof-of-retrievability [Miller et al., 2014].
- **Goal:**
  - Lower energy consumption, disk space vs. computation.
  - Useful mining algorithm.
- **Construction:**
  - Initialization phase, something like storage configuration.
  - Execution phase, present proofs-of-storage to the system.
- **Main concerns:**
  - Trade off between computation/storage [Moran et al., 2016].
  - Outsourcing, Permacoin [Miller et al., 2014].

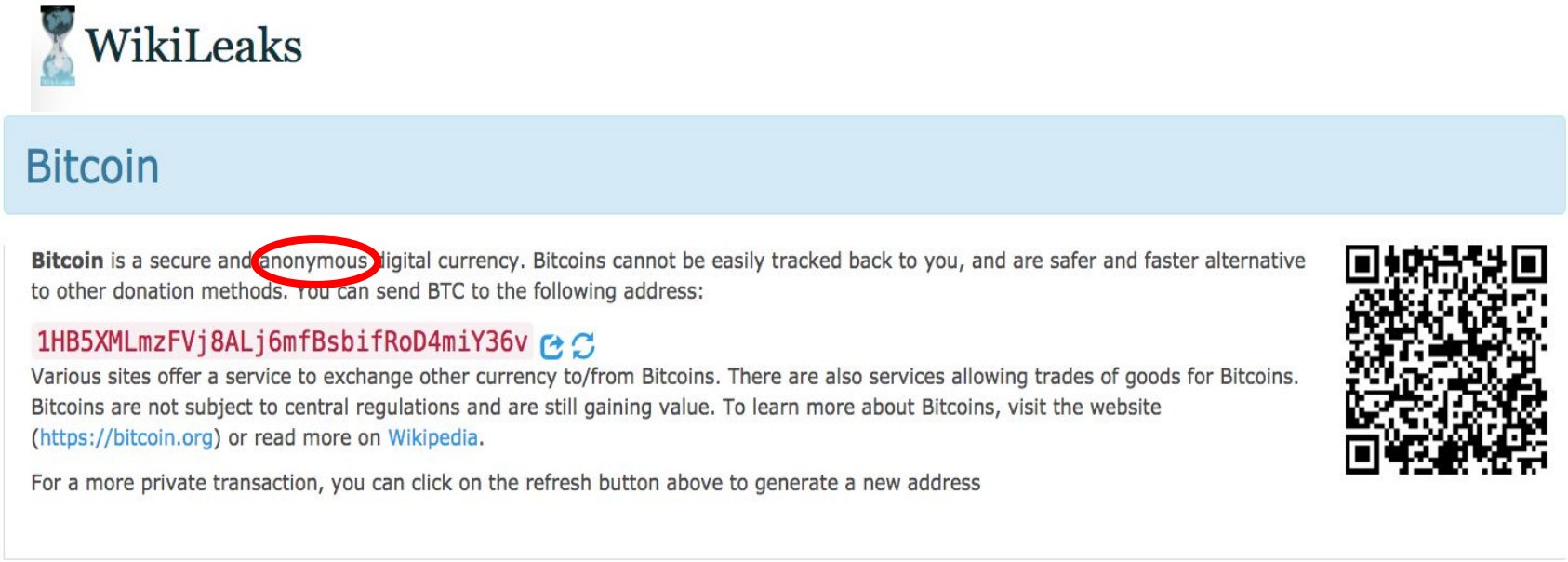
Byzantine Agreement Based

- Simply it is: “Agree faster.”
- **Goal:** speed up transactions confirmation and increase throughput.
- Elect a committee to perform a Byzantine agreement on the next block.
  - Based on PoW, Byzcoin [Kogias et al., 2016].
  - Based on PoS and VRFs, Algorand [Gilad et al., 2017].
  - In both transactions are confirmed in less than a minute.
- But:
  - Strong network connectivity assumption.
  - ⅓ of the mining power can be malicious.
  - Scalability (i.e. number of miners).

Anonymity

Is Bitcoin Anonymous?

- Believed to be, users are known by their public keys.
  - To protect privacy create new key pair for each new transaction.
  - Send the change to a new address each time.

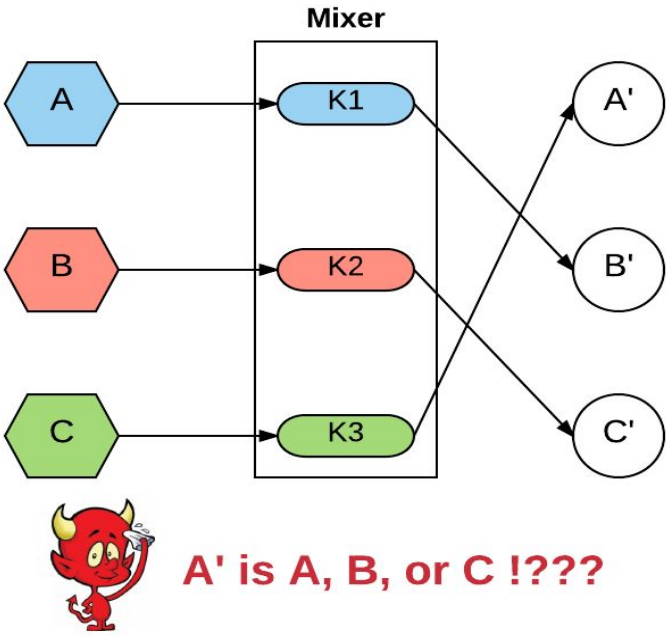


Source (accessed 11/23/2017): https://shop.wikileaks.org/donate

No, it is not ...

- Proved to be pseudo-anonymous:
  - The blockchain is public, track the flow of transactions.
  - Cluster Bitcoin addresses into entities, link them to identities and/or Bitcoin addresses posted by their owners on forums, etc., [Reid et al. 2014]
  - Link this flow to users' IPs [Koshy et al. 2014].

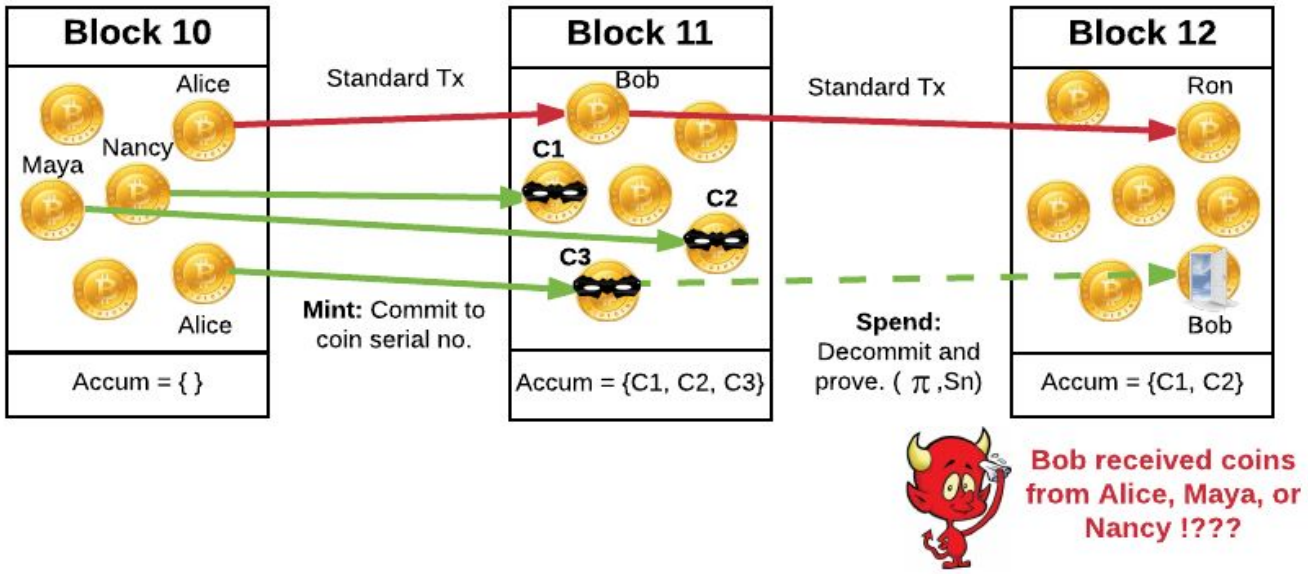
Mixing



- **Goal:** Break transactions linkability.
  - This creates an anonymity set of the output.
- Will the mixer return the money back? Will it forget the mapping?
- **Mixcoin** [Bonneau et al., 2014]
  - Mixers issue warranties to customers.
  - Use a series of mixers to reduce the probability of local records risk.
  - Still linkable in several cases, does not guarantee anonymity.

Decentralized Mixer

Zercoin [Miers et al., 2013], does not hide currency value or destination address, large overhead.



Anonymous Cryptocurrencies

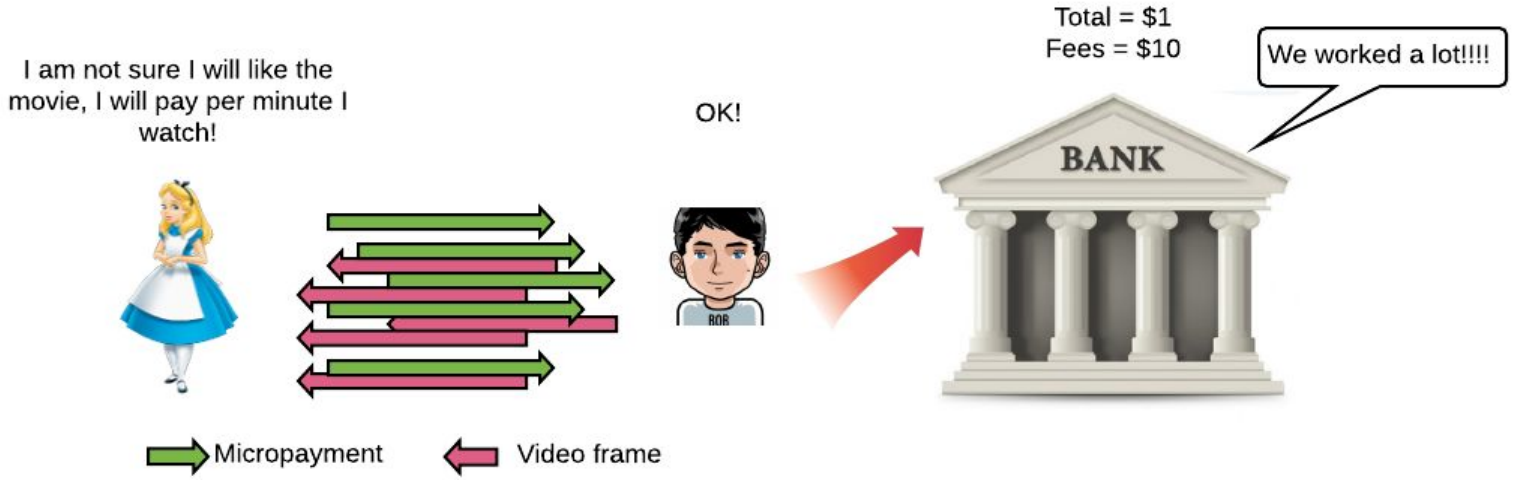
- Hide source, destination, and value.
- Zerocash [Ben Sasson et al., 2014].

Micropayments

Micropayments

"Micropayments are back, at least in theory, thanks to P2P." [*]

- A payment of micro value, i.e. pennies or fractions of pennies.
- Several applications, e.g. ad-free web, online gaming, etc.
- Suffer from high transactions fees and large payment log size.



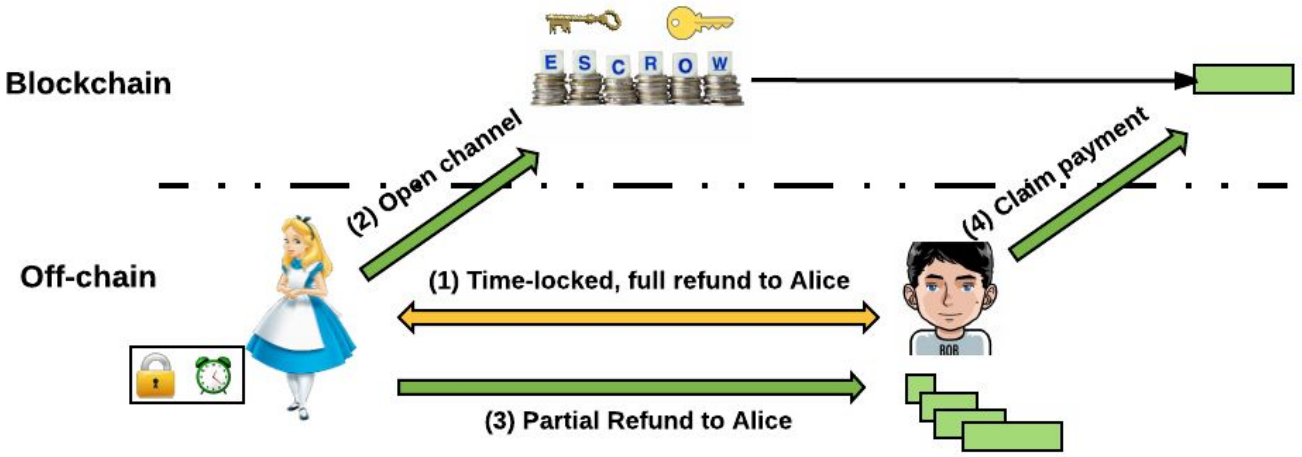
[*] Clay Shirky, The Case Against Micropayments, http://www.openp2p.com/pub/a/p2p/2000/12/19/micropayments.html

Translate to Cryptocurrency

- In Bitcoin [https://blockchain.info/stats],
  - The average transaction fee is around $5
  - Transaction throughput is around 10 tps.
- So,
  - Alice ⇒ pay too much,
  - Bob ⇒ wait too long,
  - Miners/blockchain ⇒ overwhelmed.
- But, cryptocurrency is a very attractive option to preserve decentralization in monetary-incentivized distributed systems.
- ***Solution,*** aggregate these tiny payments!

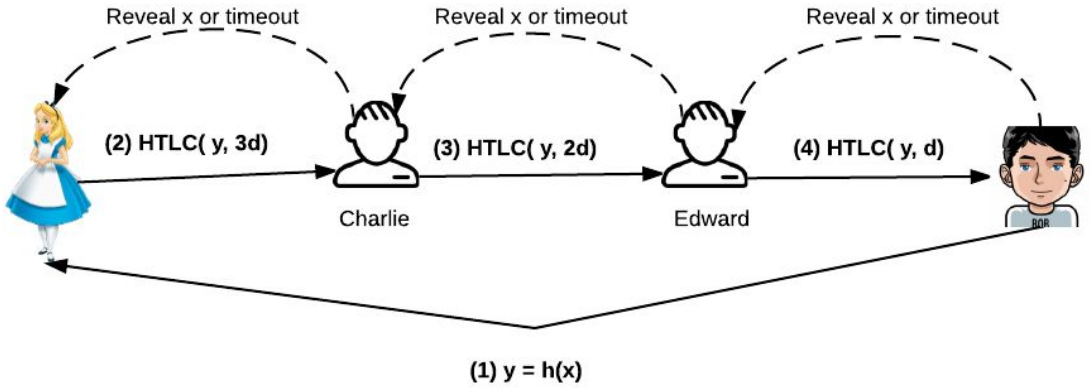
Micropayment Channels

- Simply a common locked fund between two parties with the currency ownership adjusted overtime.
- **Ingredients:**
  - Multi-signature escrow,
  - refund transaction,
  - and partial refund transactions.



Micropayment Networks

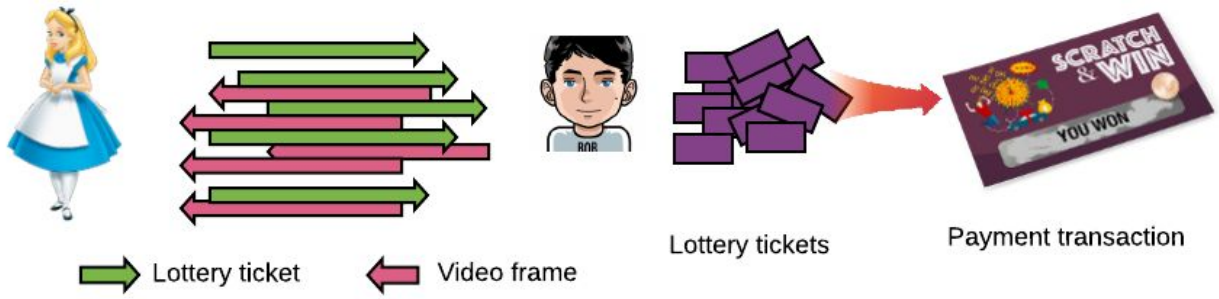
- How about paying several parties using the same escrow?
  - The lightning network [Poon et al., 2014]
  - ***A*** can pay ***B*** as long as there is a payment path between them.
  - Principal component: HTLC (Hash Time-Lock Contract).



- **Cons:** Possibility of centralization, large collateral cost, and ***fees are back?!***
- **Follow up:** Sprites reduces the collateral cost [Miller et al., 2016].

Probabilistic Micropayments

- Dated back to Rivest [Rivest, 1997] and Wheeler [Wheeler, 1996].



- Early implementations were centralized.
- Cryptocurrencies are utilized to achieve decentralization.

Decentralized Probabilistic Micropayments

- Ingredients:
  - Escrow creation.
  - Distributed lottery protocol.
  - Funds release.
- Main challenges:
  - Double spending (pay several parties the same lottery ticket).
  - Front running attacks.
- Two schemes: MICROPAY [Pass et al., 2015] and DAM [Chiesa et al., 2017]

Security

Security of Cryptocurrencies

- Sometimes referred to as stability.
- Relies on three components: transactions, blockchain, and the peer-to-peer network.
- Transactions.
  - Stability of transactions validation rules.
- A blockchain is secure if it achieves the following properties [Bonneau et al., 2015]:
  - Eventual consensus.
  - Exponential convergence.
  - Growth or liveness.
  - Correctness.
  - Fairness.
- Peer-to-peer network.
  - Its connectivity affects convergence, growth, and fairness in mining rewards.

Incentive Compatibility

- It is for the best of the miners to play by the rules.
  - Sometimes referred to as majority compliance.
- Not always true.
  - Selfish mining allows an attacker in control of less than 30% of the mining power to undermine fairness [Sompolinsky et al., 2015].
  - Goldfinger attack. CoiledCoin was destroyed by Eligius (a Bitcoin mining pool).
- Mining pools and centralization.

Last Stop

Conclusions

- Cryptocurrencies provide a disruptive work model.
  - But also exhibit complicated relations between, financially motivated, untrusted parties.
- Great potential and huge arena of applications.
  - However, deeper thinking is needed to assess when/where to apply.
- Are they just a hype that will fade away?!
  - Still provide an elegant proof of concept.

The Road Ahead

- Threat modeling for cryptocurrencies.
- Resource-backed cryptocurrencies.
- Probabilistic micropayments.
- Decentralized mining.

Utilize advanced virtual reality techniques to "Sleep on a bed of Bitcoins"

Questions?

aNd ThANk yOU :)

References

[Nakamoto, 2008] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.

[Wood, 2014] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum Project Yellow Paper 151 (2014).

[O'Dwyer et al., 2014] O'Dwyer, Karl J., and David Malone. "Bitcoin mining and its energy footprint." (2014): 280-285.

[Gilad et al., 2017] Gilad, Yossi, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. "Algorand: Scaling byzantine agreements for cryptocurrencies." In In Proceedings of the 26th ACM Symposium on Operating Systems Principles (SOSP). 2017.

[Kiayias et al., 2017] Kiayias, Aggelos, Alexander Russell, Bernardo David, and Roman Oliynykov. "Ouroboros: A provably secure proof-of-stake blockchain protocol." In Annual International Cryptology Conference, pp. 357-388. Springer, Cham, 2017.

[Dziembowski et al., 2015] Dziembowski, Stefan, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. "Proofs of space." In Annual Cryptology Conference, pp. 585-605. Springer, Berlin, Heidelberg, 2015.

Cont'd.

[Moran et al., 2016] Moran, Tal, and Ilan Orlov. "Proofs of Space-Time and Rational Proofs of Storage." IACR Cryptology ePrint Archive2016 (2016): 35.

[Miller et al., 2014] Miller, Andrew, Ari Juels, Elaine Shi, Bryan Parno, and Jonathan Katz. "Permacoin: Repurposing bitcoin work for data preservation." In Security and Privacy (SP), 2014 IEEE Symposium on, pp. 475-490. IEEE, 2014.

[Kogias et al., 2016] Kogias, Eleftherios Kokoris, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. "Enhancing bitcoin security and performance with strong consistency via collective signing." In 25th USENIX Security Symposium (USENIX Security 16), pp. 279-296. USENIX Association, 2016.

[Reid et al. 2014] Reid, Fergal, and Martin Harrigan. "An analysis of anonymity in the bitcoin system." In Security and privacy in social networks, pp. 197-223. Springer New York, 2013.

[Koshy et al. 2014] Koshy, Philip, Diana Koshy, and Patrick McDaniel. "An analysis of anonymity in bitcoin using p2p network traffic." In International Conference on Financial Cryptography and Data Security, pp. 469-485. Springer, Berlin, Heidelberg, 2014.

Cont'd.

[Bonneau et al., 2014] Bonneau, Joseph, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten. "Mixcoin: Anonymity for Bitcoin with accountable mixes." In International Conference on Financial Cryptography and Data Security, pp. 486-504. Springer, Berlin, Heidelberg, 2014.

[Miers et al., 2013] Miers, Ian, Christina Garman, Matthew Green, and Aviel D. Rubin. "Zerocoin: Anonymous distributed e-cash from bitcoin." In Security and Privacy (SP), 2013 IEEE Symposium on, pp. 397-411. IEEE, 2013.

[Ben Sasson et al., 2014] Sasson, Eli Ben, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. "Zerocash: Decentralized anonymous payments from bitcoin." In Security and Privacy (SP), 2014 IEEE Symposium on, pp. 459-474. IEEE, 2014.

[Poon et al., 2014] Poon, Joseph, and Thaddeus Dryja. "The bitcoin lightning network: Scalable off-chain instant payments." Technical Report (draft) (2015).

[Miller et al., 2016] Miller, Andrew, Iddo Bentov, Ranjit Kumaresan, and Patrick McCorry. "Sprites: Payment Channels that Go Faster than Lightning." arXiv preprint arXiv:1702.05812 (2017).

Cont'd.

[Rivest, 1997] Ronald Rivest.1997.Electronic lottery tickets as micropayments. In International Conference on Financial Cryptography. Springer, 307–314.

[Wheeler, 1996] David Wheeler. 1996. Transactions using bets. In International Workshop on Security Protocols. Springer, 89–92.

[Pass et al., 2015] Pass, Rafael. "Micropayments for decentralized currencies." In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 207-218. ACM, 2015.

[Chiesa et al., 2017] Chiesa, Alessandro, Matthew Green, Jingcheng Liu, Peihan Miao, Ian Miers, and Pratyush Mishra. "Decentralized Anonymous Micropayments." In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 609-642. Springer, Cham, 2017.

Example

- Ethereum has higher block generation rate than Bitcoin, around a block every 16 sec.
- Does the longest chain concept still work?
  - Ethereum adopts GHOST [Sompolinsky et al., 2015]