BCNET

Shared IT Services for Higher Education & Research

Conference 2017

Blockchain and Potential Applications in Higher Ed

Hugh Burley, TRU

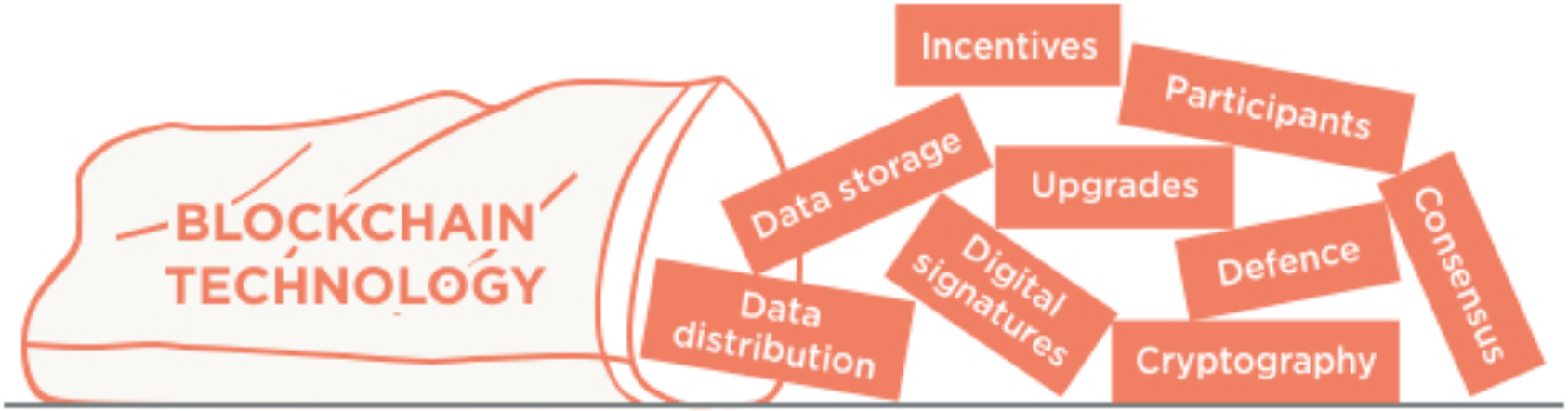
Garry Sagert, UVic

Goals of Presentation

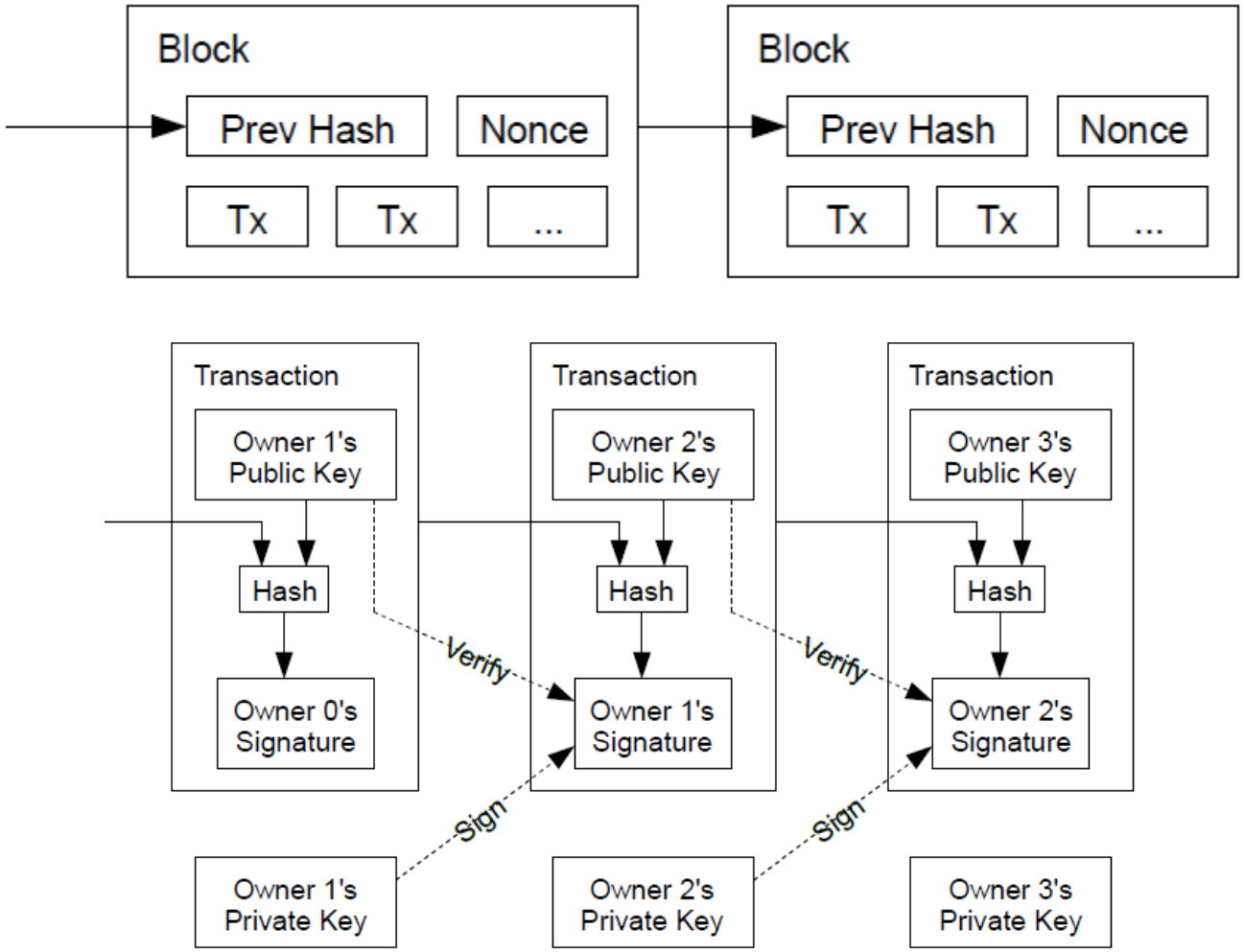
- Concepts underlying blockchain illustrated using two examples: Bitcoin & Ethereum
- Describe the potential for global disruption
- Consider potential applications for higher ed

Blockchain

A collection of technologies that can be used for public permissionless or private networks to create a ***trusted*** distributed/shared ledger.



Digital Signatures & Cryptography



Two Visions

BitCoin	Ethereum
A purely peer-to-peer version of electronic cash [which] would allow online payments to be sent directly from one party to another without going through a financial institution.	To create an unstoppable censorship-resistant self-sustaining decentralised world computer.

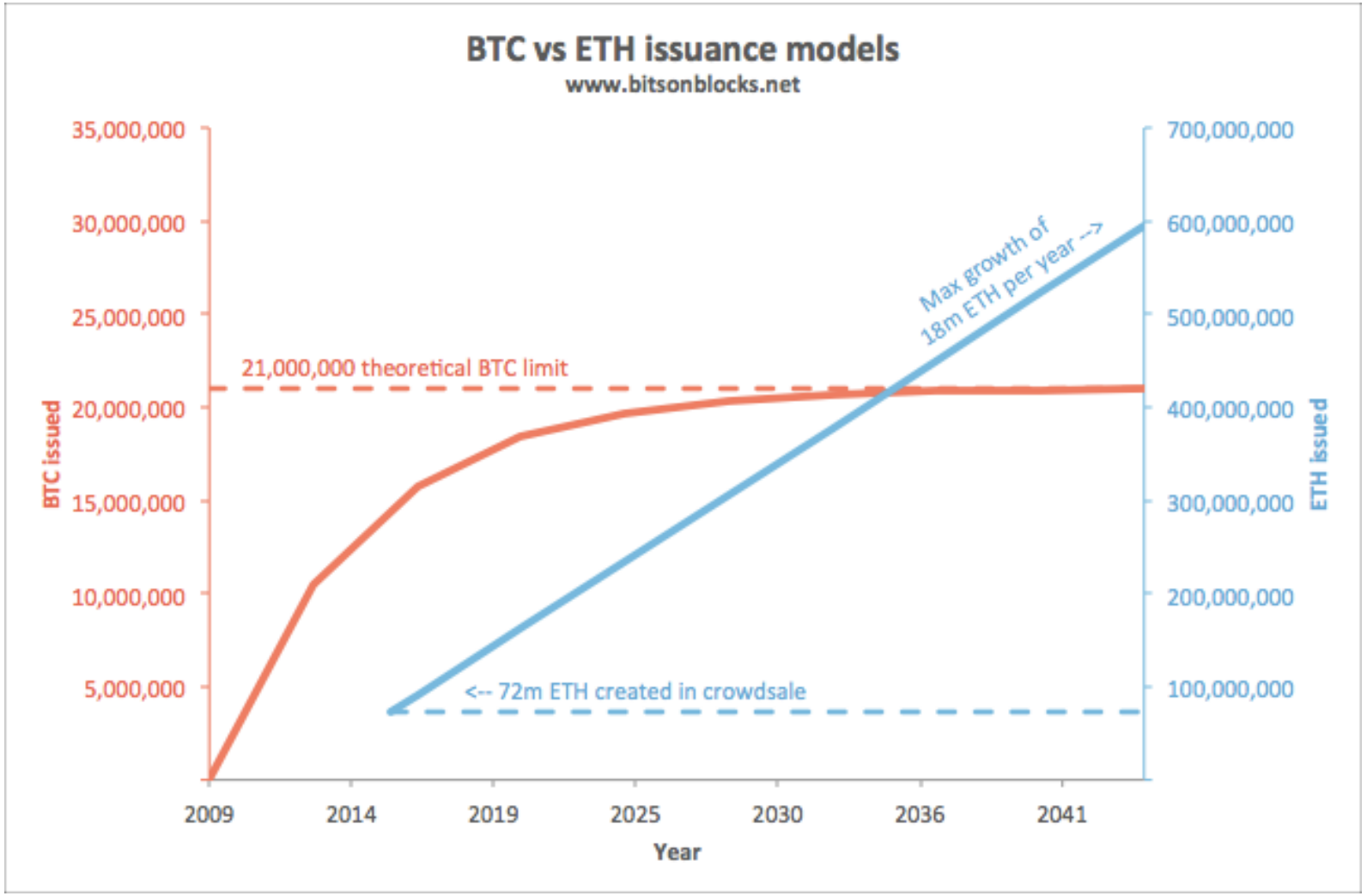
Data Distribution & Participants

BitCoin	Ethereum
Both are Peer to Peer – pseudonymous	
New blockchain created ~ 10 min	New blockchain created ~ 14 sec

https://geth.ethereum.org/downloads/
https://bitcoin.org/en/download

Incentives for Mining

BitCoin	Ethereum
12.5 new BTC/block mined up to 21 billion + transaction fee	5 ETH block reward (0r 4.375 new ETH for an uncle), plus a small new reward for referencing up to 2 recent uncles (1/32 of a block reward ie 1/32 x 5 ETH = 0.15625 new ETH per uncle), plus gas from contracts that were run during the block


BTC vs ETH issuance models
www.bitsonblocks.net
35,000,000
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
BTC issued
700,000,000
600,000,000
500,000,000
400,000,000
300,000,000
200,000,000
100,000,000
ETH issued
21,000,000 theoretical BTC limit
Max growth of
18m ETH per year -->
<-- 72m ETH created in crowdsale
2009
2014
2019
2025
2030
2036
2041
Year

A dishonest miner can:

1. Refuse to relay valid transactions to other nodes
2. Attempt to create blocks that include or exclude specific transactions of their choosing
3. Attempt to create a ‘longer chain’ of blocks that make previously accepted blocks become ‘orphans’ and not part of the main chain

They can’t:

1. Create bitcoins out of thin air
2. Steal bitcoins from your account
3. Make payments on your behalf or pretend to be you

https://geth.ethereum.org/downloads/
https://bitcoin.org/en/download

Defence

BitCoin	Ethereum
A compute intensive Proof of Work and peer-to-peer auditing.	A memory hardened Proof of Work - Ethhash and peer-to-peer auditing.

Consensus

BitCoin	Ethereum
Proof of Work + Longest Chain Rule	Currently PoW based on memory hardened compute + longest chain, but moving to a Proof-of-Stake protocol called Casper. Allows orphaned blocks/Uncles, to be referenced.

Upgrades

BitCoin	Ethereum
BIPs	Ethereum Foundation

Data Storage

BitCoin	Ethereum
BTC Transactions Coloured coins	ETH Transactions + Turing Complete Smart Contracts

Why is this so disruptive?

- It was previously assumed that secure transaction ledgers require a trusted third party
- Trusted third parties (e.g. banks) still exert influence over transactions
- Removing this influence enables innovation, especially across jurisdictions
- For example, an American could lend money to somebody in Africa without a trusted third party

Why is this so disruptive?

- The payload can be anything!!!
  - Electronic currencies
  - Real-estate transactions
  - Vehicle ownership
  - Smart contracts
  - Blueprints for 3D printing
- De-centralized nature mitigates data loss risks

What about higher ed?

- Exchanging and verifying student credentials is a complex, costly, and subject to fraud
- Student credentials could be in a blockchain
- All institutions would have a copy
- Students provide access to their records by providing institutions with their public keys
- Institutions append credentials earned to the student's blockchain record

What are the barriers?

- Concepts can be complex to communicate
- Blockchain technology is evolving rapidly
- Scalability and transaction speed are limited
- Consensus model needs to be determined

Questions?

- Hugh Burley (hburley@tru.ca)
- Garry Sagert (gsagert@uvic.ca)