Cryptocurrencies: challenges and caveats

Khaled Baqer
Cambridge University
Outline

• Background
  – Bitcoin consensus
  – The blockchain
• Challenges and caveats
  – Decentralisation
  – The block size
  – Energy consumption
  – Reputation and anonymity
• Bitcoin: machine Learning
• Summary
A new form of consensus

- Existing consensus mechanisms included voting, small groups, and $k$ out of $n$ signatures
- The blockchain mechanism is new as it scales without ‘apparently’ needing a central authority
- No pre-established trust is needed to maintain global consensus (the ledger of transactions)
The blockchain

• Signed transactions are sent to peers
• Transactions propagate in the network
• Transactions remain in limbo until a miner includes them in a block
• Miners compete to find a hash of the existing blockchain, plus the selected pending transactions, with a ‘special property’ which means they need about $2^{64}$ trials
• New: the miner is not pre-(s)elected
Is Bitcoin really decentralised?

- Mining pools: Satoshi didn’t see this coming
- 50% of miners (or less) can control what transactions are mined (censorship?)
- They can collectively decide which mining software and policies will be enforced
The block size debate

- At present, Bitcoin blocks are limited to 1MB
- That means 7 transactions per second, (average one block mined per 10 minutes)
- Some developers want to increase this
- Who controls what software will be used? What modifications to the protocol will be enforced?
Energy consumption

• In early days, miners found hashes using software on their PCs (or other people’s)
• Once bitcoins became valuable, firms started building custom hardware that turns electricity into hashes efficiently
• Major cost of mining a coin is energy
• In late 2016, the mining reward falls from 25 bitcoins to 12.5
Bitcoin: reputation and anonymity

• Silk Road: underground marketplace for drugs
• Idea: easy to create new identities (no central body to copy your passport and gas bill)
• But: the blockchain is completely public, so all transactions can be traced
• October 2013: Ross Ulbricht gets arrested
• Now: it’s the mainstay of ransomware
Bitcoin: machine learning

Khaled Baqer (Cambridge), Danny Huang (UCSD), Damon McCoy (NYU), Nicholas Weaver (ICSI, Berkeley)
Summary

• The accumulation of power is a problem
• The privacy mechanism – free pseudonyms – isn’t enough for businesses
• Fixing it so that its scales up properly is hard
• Problems: propagation delays, bandwidth, data storage, etc.
• Focus on resilience and censorship-resistance