CS1699: Blockchain Technology and Cryptocurrency

19. Altcoins

Bill Laboon

What is an Altcoin?

- Any cryptocurrency launched since Bitcoin
- Bitcoin was a sea change in how currencies can work - just like we can really divide computing into pre- and post-Turing eras
- But Bitcoin makes certain tradeoffs, ones that not everyone thinks are optimal

Bitcoin Strengths

- Ludicrously secure
- Technologically conservative, battle-tested
- Inflation-proof: only 21 million bitcoin will ever be mined
- Mind share: when people think "cryptocurrency," they think "Bitcoin"

Bitcoin Drawbacks/Trade-offs

- Relatively slow confirmation times
- Pseudonymous, not anonymous
- Simple scripting language
- Energy-inefficient
- Centralized mining (ASICs)
- Extremely large rewards to early adopters

Launching An Altcoin

- Write the code (or fork from Bitcoin or other cryptocurrency)
- Modify parameters:
  - Consensus mechanism
  - Puzzle algorithm
  - Scripting language
  - Block size/time (or a non-blockchain system)
  - Coin generation mechanism
  - etc.

Bootstrapping

- Apologies to Tom Petty, "the beginning is the hardest part"
- No market value, since no use for the coin
- No security, since no miners
- No incentive to develop on it
- No knowledge of coin amongst potential users

Altcoin Infanticide

- If you are using a similar POW algorithm (or one which can be calculated with a CPU or other easily-accessible system), someone else can come with >50% hashpower and execute 51% attacks
- *Why?* Reduce competition, kill scams, show that it is technically possible, for the lolz
- Possible solution: stay "under the radar" until you have enough hashpower (or equivalent) to resist attacks

Altcoins Need A Community

- This can be something specific (e.g. the dental industry for Dentacoin) or something broader (people who don't like the distribution of bitcoin or its energy inefficiency)
- Keeping it "in-community" before making it universal allows hashpower to build up
- People part of a community less likely to attack / sabotage

Allocating Altcoins

- Selling for bitcoin or other currency (e.g. Ethereum, ICOs)
- Burning bitcoin or other currency (e.g. Counterparty)
- Performing non-automatable work (e.g. Nano)
- Pre-mining or pre-allocation (controversial!)

Pump and Dump

- Altcoins are absolutely rife with scammers
- For low-volume altcoins, can add "pretend volume" and make price increase ("pump")
- Others see price increase and buy more, causing more of a price increase
- Original buyers sell their holdings ("dump")
- New buyers are left "holding bags"

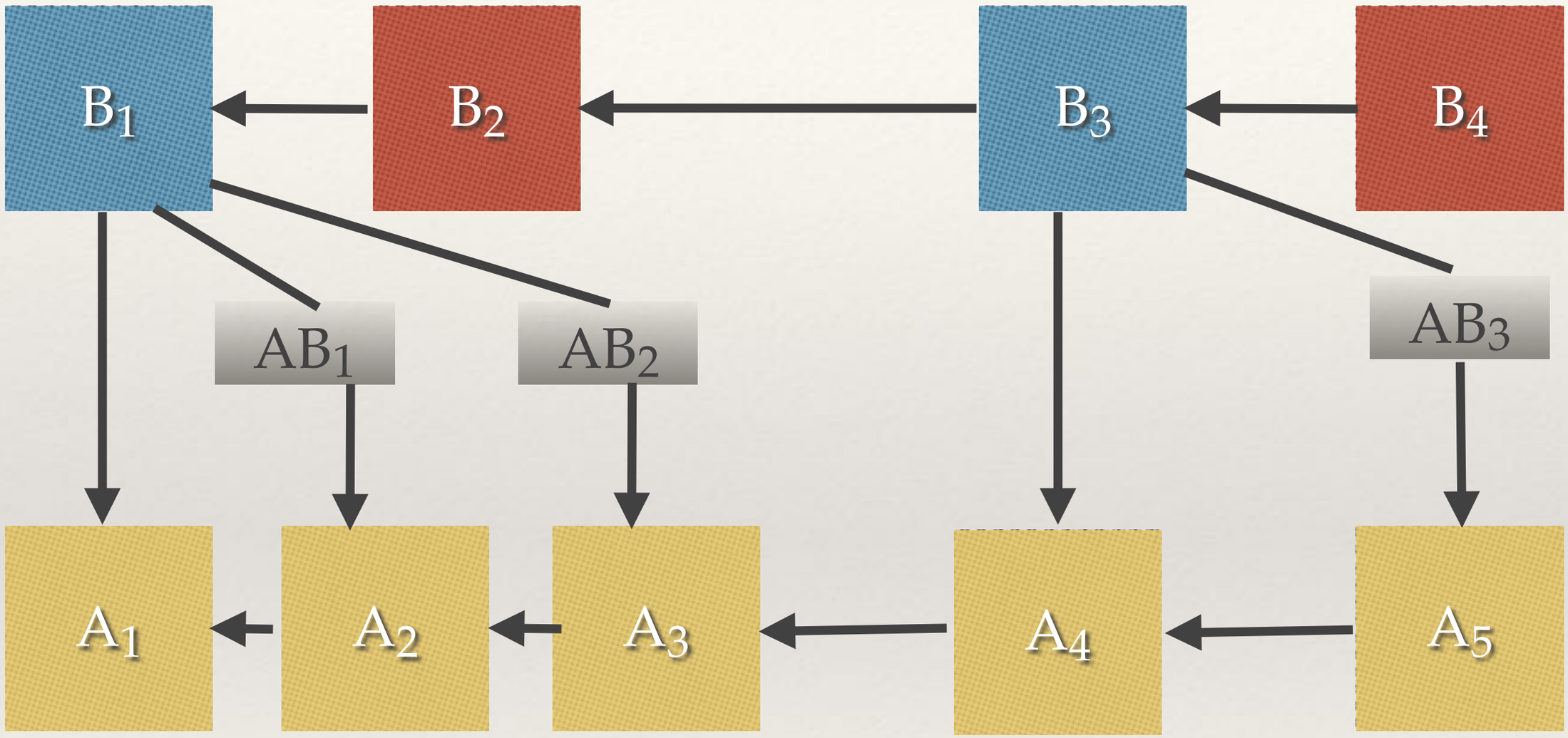
Merge Mining

- Mine on parent chain, but child chain blocks rely on parent chain hashing
- Need to use same hash algorithm
- Additional data in coinbase scriptSig field or other location for arbitrary data (for non-Bitcoin parent chain)

Merge Mining

- Blocks are now "double-dipping"
  - To Bitcoin network (parent chain), merge miners' blocks look just like regular blocks, albeit perhaps with strange coinbase data
  - To altcoin network (child chain), can understand coinbase data stored in Bitcoin (parent chain) blocks
- Can use different target to also get attempted blocks from Bitcoin network (parent chain) and use them for altcoin network (child chain)

Merge Mining Diagram (Bitcoin/Altcoin)



B1 Bitcoin block, altcoin miner

B2 Bitcoin block, non-altcoin miner

A1 Altcoin block

AB1 Attempted Bitcoin block

Benefits of Merge Mining

- No additional computing power necessary (can use "empty" space in coinbase)
- Parent chain (e.g. Bitcoin) mostly unaffected (very, very minor bloat)
- Increased effective hashpower for altcoin

Drawbacks of Merge Mining

- Complex to set up, possible unknown security issues
- For small coins who need merge mining, very minimal benefit to miners on parent chain
- Time-consuming to set up for miners
- Many Bitcoin miners are *Bitcoin maximalists*