CSBC2000

Week 1 | Class 1

Motivation and Basics of Blockchain Infrastructure

Course Information: Info

- **Instructor:** Govind Mohan
- **Email:** gov@yorku.ca
- **Program:** Certificate in Blockchain Development
- **Schedule:**
  - Week 1: Feb 8-11
  - Week 2: Feb 16-18, 22
  - Week 3: Feb 23-25, Mar 1

Course Information: Assignments

Assessment Item	Due Date	% of Final Grade
Participation and Discussion Forum Contribution	Daily	10%
Assignment #1 - Coding Assignment	Feb 16@11:59PM	25%
Assignment #2 - Coding Assignment	Feb 22@11:59PM	25%
Assignment #3 - Blockchain Use Case Presentation	Mar 1@11:59PM	40%
TOTAL		100%

Course Information: Week Breakdown

- **Week 1:** Basics of blockchain infrastructure and decentralized computer network
- **Week 2:** Intro to cybersecurity in the context of DLT and distributed systems
- **Week 3:** Architecting DLTs from a business requirements perspective

Introduction + Survey

- Let's get to know each other!
- Name
- Brief professional/academic background
- Learning goals for this program
- What you know about blockchain

A history of Blockchain

- Haber, Stornetta (1991): "electronic digital documents are so easy to tamper with, and the change need not leave any telltale sign on the physical medium. What is needed is a method of time-stamping digital documents with the following two properties. First, we must find a way to time-stamp the data itself, without any reliance on the characteristics of the medium on which the data appears, so that it is impossible to change even one bit of the document without the change being apparent. Second, it should be impossible to stamp a document with a time and data different from the actual one"

A history of Blockchain

- Satoshi Nakamoto wrote the monumental "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2009
- Notable additions: Incentive layer and Proof-of-work consensus
- Ethereum: created by Vitalik Buterin in 2013, extending Bitcoin with a state machine model

What really is money?

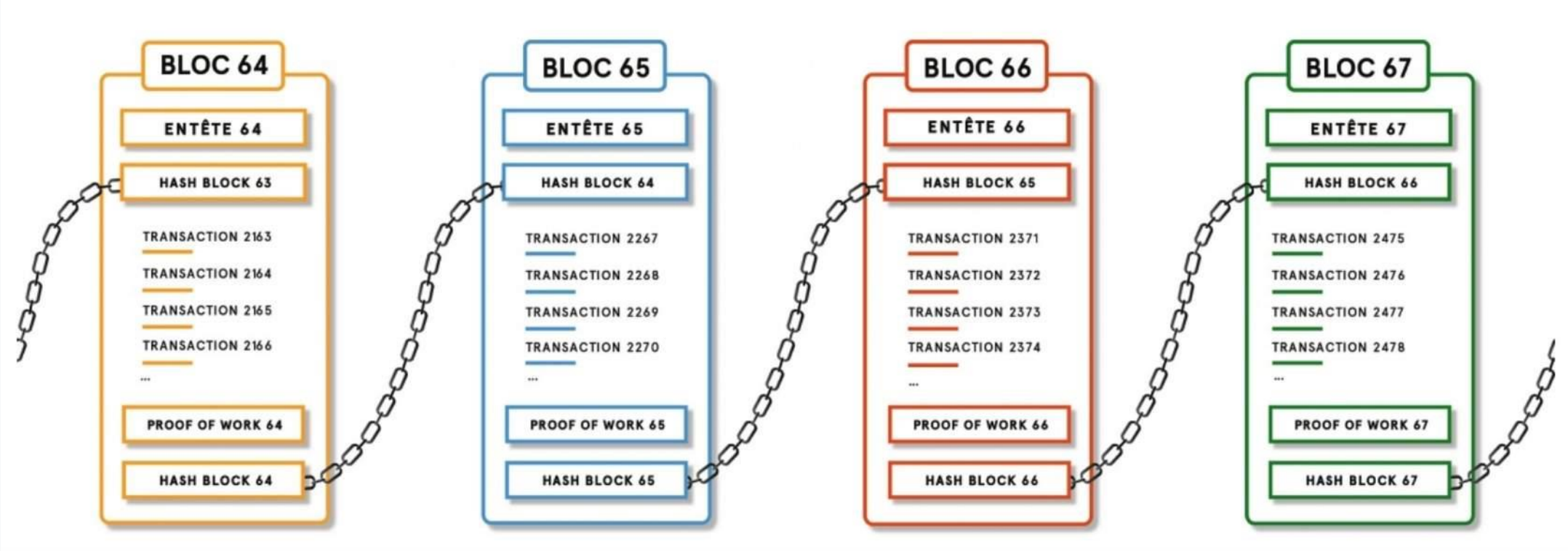
- Bartering
- Agreed upon unit of value
- Econ definitions of Currency backing in 1900-1999:
  - Gold Standard (~1945)
  - Bretton-Woods (~1975)
  - ??? (2020)

Rai Stone

What really is a Bitcoin?

- Currency = History of transactions!
- It takes "work" to update and maintain the ledger
- Miners are incentivized to put in the "work" with rewards
  - Up to a certain point! There is a limit of 21mn Bitcoins that can exist
  - Halving: works as a synthetic central bank

The Blockchain



Block Contents: Transactions

- PKI
- Bitcoin Address
- Sender, Amount, Receiver
- UTXO: Unspent Transaction Output

Block Header: Hash

- Unique fingerprint of this block
- Combines various other parts of the block to ensure uniqueness
- Each block stores the previous block's hash, and uses it to compute its own hash
- Transactions can be hashed sequentially but there's a better way
  - Merkle Trees next week

Block Header: Proof-of-Work

- A quick primer on SHA and hashing:
  - Serves as a fingerprint
  - Pseudorandom bit generator
  - $2^{128} \approx 3.6 \times 10^{13}$ years. In comparison, our universe is only about 13.7×10^{9} years old
- Setting expectations on SHA is the basis of PoW
  - As we saw, very difficult to compute
  - However, very easy to verify!

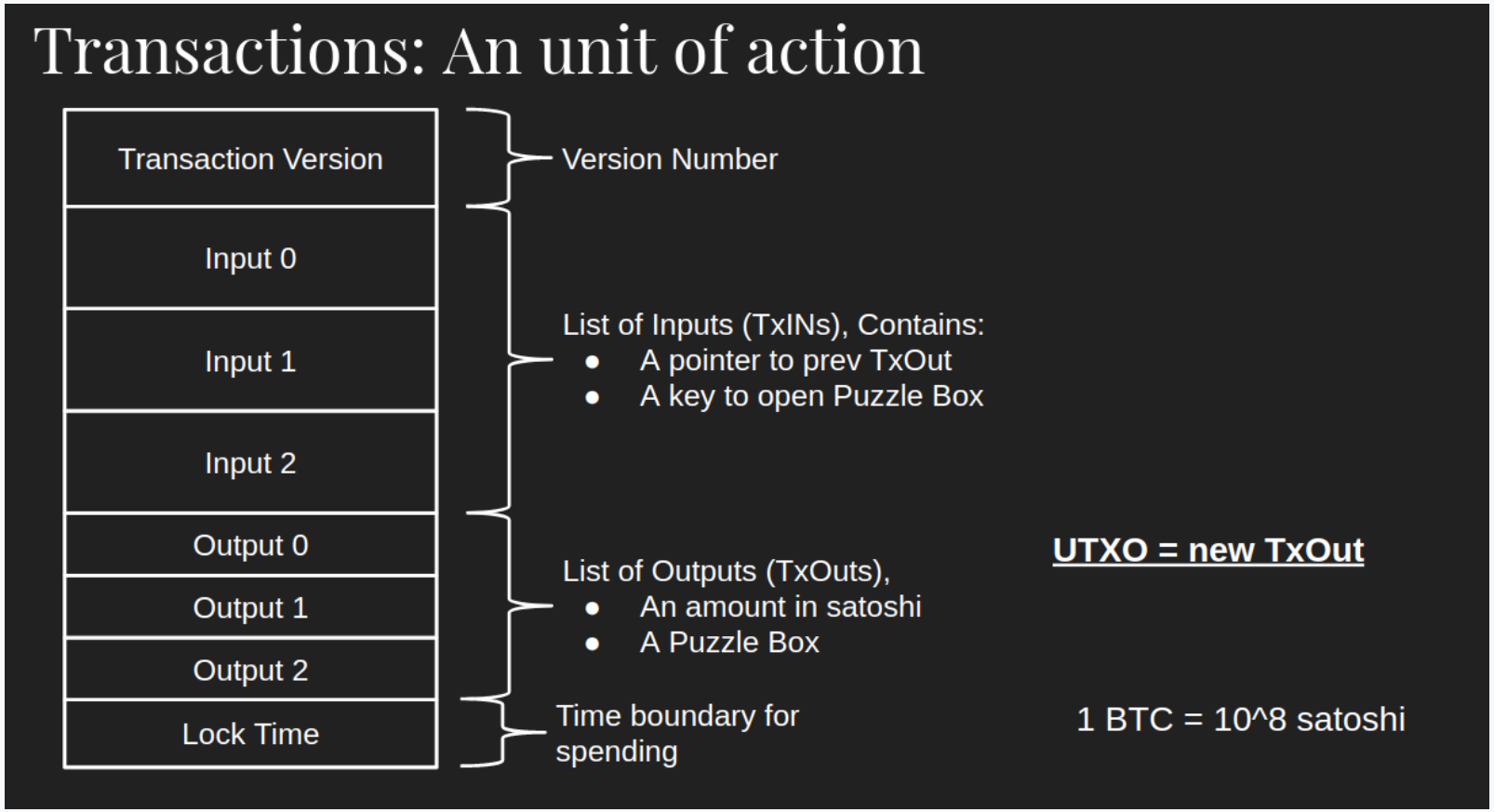
Block Header: Other stuff

- Timestamp; this is what Haber and Stornetta wanted to solve
- Block height, which is the index of the block

Block Contents: UTXO

- How did Bitcoin start from the first block?
  - Satoshi gave people BTC
  - Miners received block rewards
- What happens after
  - Value moves around in txs
  - Only unspent outputs are tracked

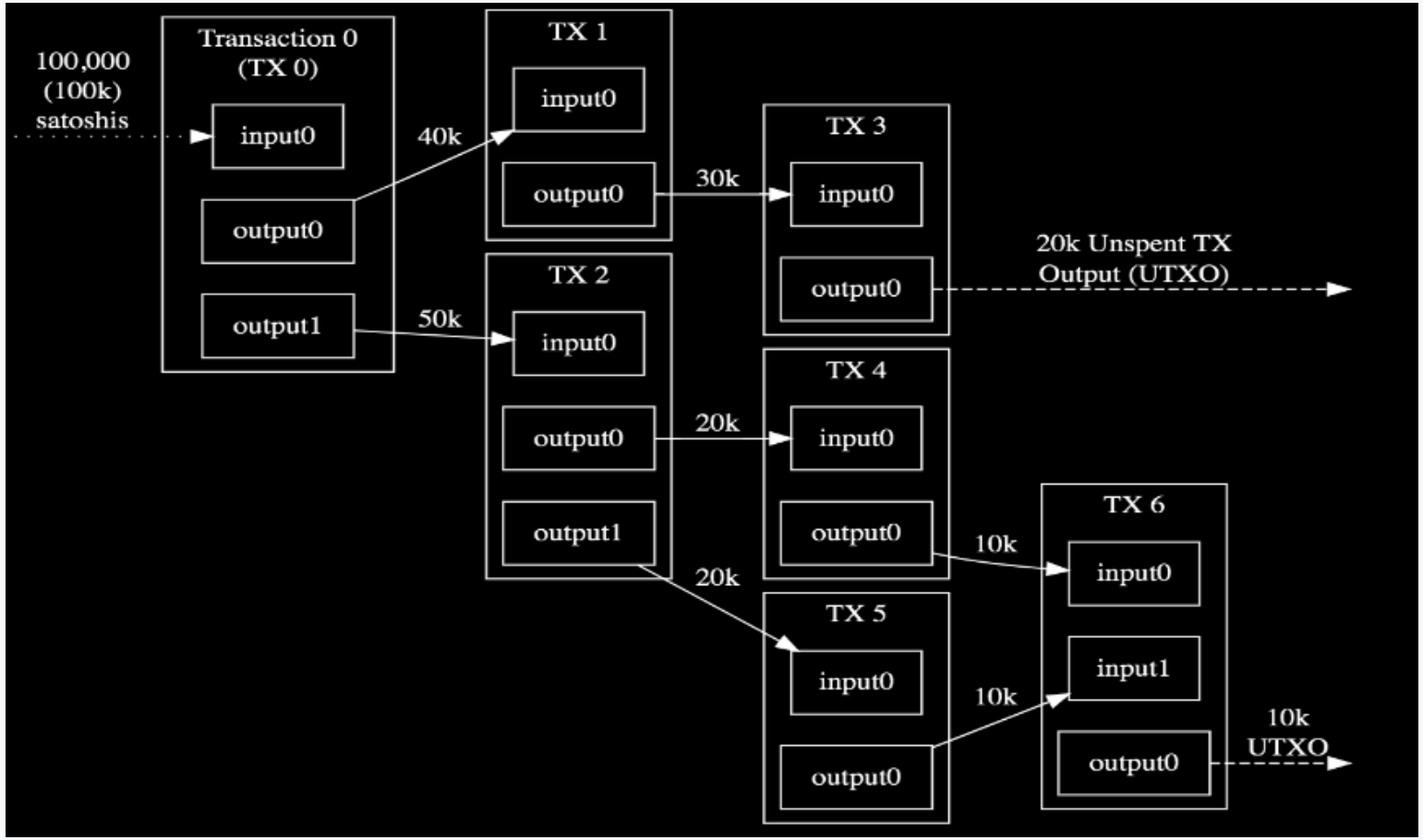
Block Contents: UTXO



Block Contents: UTXO

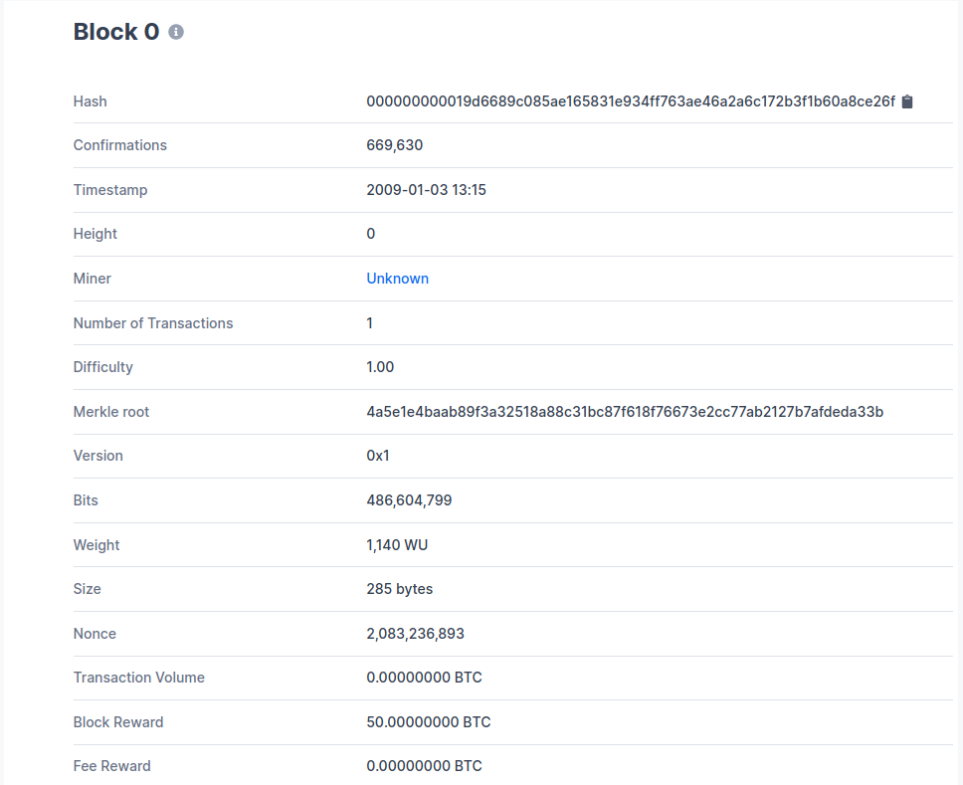
- A transaction Output consists of a cryptographic lock and a value. For now, you can imagine that the outputs are somehow locked and the input provides a key to unlock them. The value is simply the amount in satoshis (1 sat = 10^-8 BTC) that is locked inside the output.
- Every Transaction input consists of a pointer and an unlocking key. The pointer points back to a previous transaction output. And the key is used to unlock the previous output it points to. Every time an output is successfully unlocked by an input, it is marked inside the blockchain database as “spent”.

Block Contents: UTXO



Genesis Block

- The first block in the chain is termed as the genesis block
- It contains all the initialization parameters for the rest of the chain



Block 0

Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Confirmations	669,630
Timestamp	2009-01-03 13:15
Height	0
Miner	Unknown
Number of Transactions	1
Difficulty	1.00
Merkle root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Version	0x1
Bits	486,604,799
Weight	1,140 WU
Size	285 bytes
Nonce	2,083,236,893
Transaction Volume	0.00000000 BTC
Block Reward	50.00000000 BTC
Fee Reward	0.00000000 BTC

Addresses and Keys

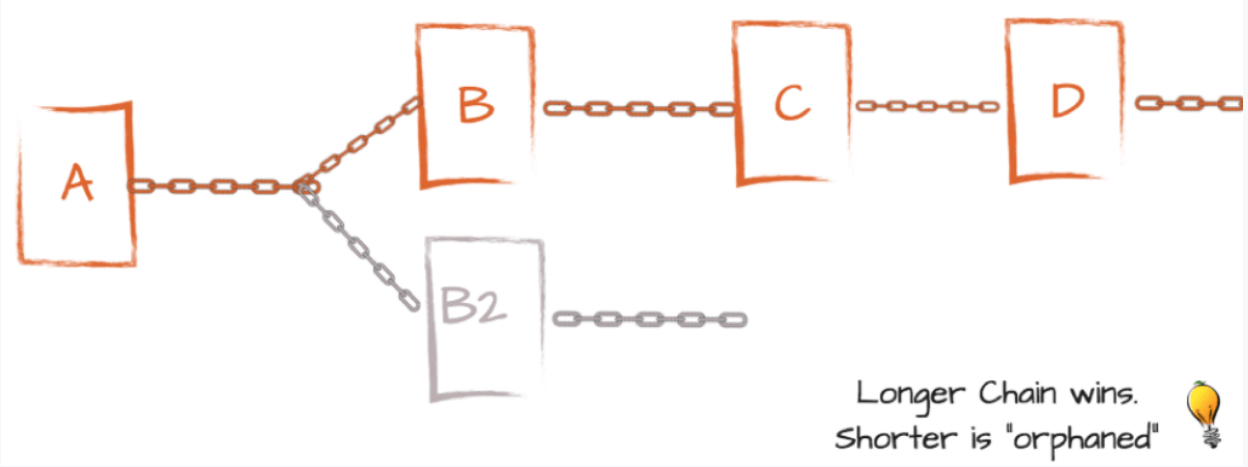
- If you own some Bitcoin, you will possess the following:
  - A public key: Used to verify your transactions on the blockchain; used to generate the bitcoin address
  - A private key: Required for you to execute transfer of funds from your account
  - A bitcoin address: Represents your Bitcoins; others can send/receive funds via your address
- A Bitcoin wallet generally is just a manager for your keys
  - This is why you need to control your keys!!
- More on this next week

Conflicts

- What if there are multiple miners that solve a PoW problem simultaneously?
- - Unlikely but not impossible
- - This leads to a fork. Multiple blocks could be added to all the subchains in the fork
- We need a mechanism to decide between forks

The Longest Chain Rule

- The chain with "the most work" is always favored by the network
- That is to say, if there are multiple chains in a fork, the one with the most subsequent work will win



51% Attack

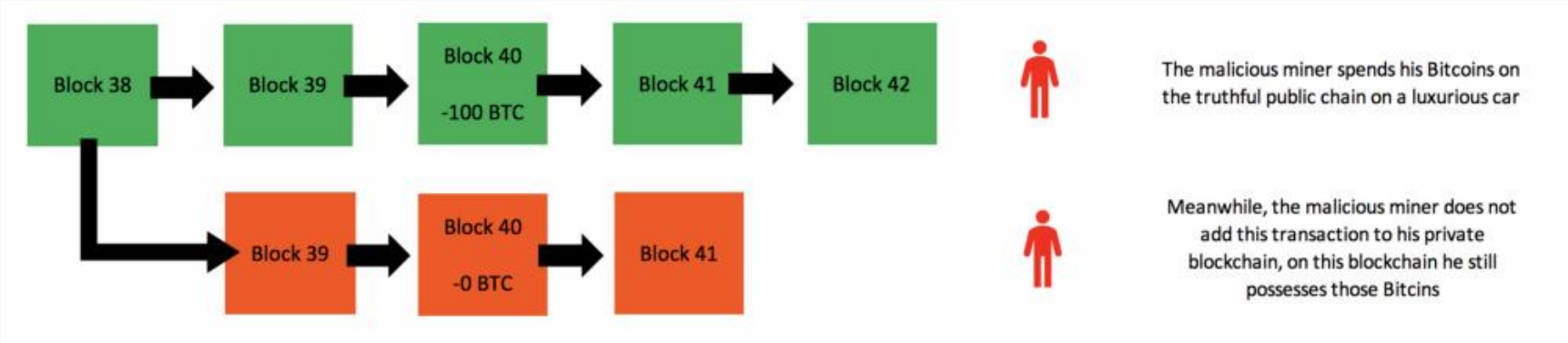
- How can an attacker control the Bitcoin blockchain? The rewards are surely lucrative...
- Bitcoin consensus is based on the largest amount of work in a chain
- Why not just get a ton of computers and just make a chain that must be accepted?
- This is very hard as they'd need to put in work to change this history as well as change the current chain WHILE non-malicious peers are still mining

Double Spend

- What happens if a user tries to cheat the system?
- They can send Bitcoin to another person and then make a simultaneous transaction for the same amount to an address they control
- Transactions sit in the mempool while they are waiting to be mined into a block
- If they don't have enough hashing power, either transaction gets accepted and they have no choice but to accept

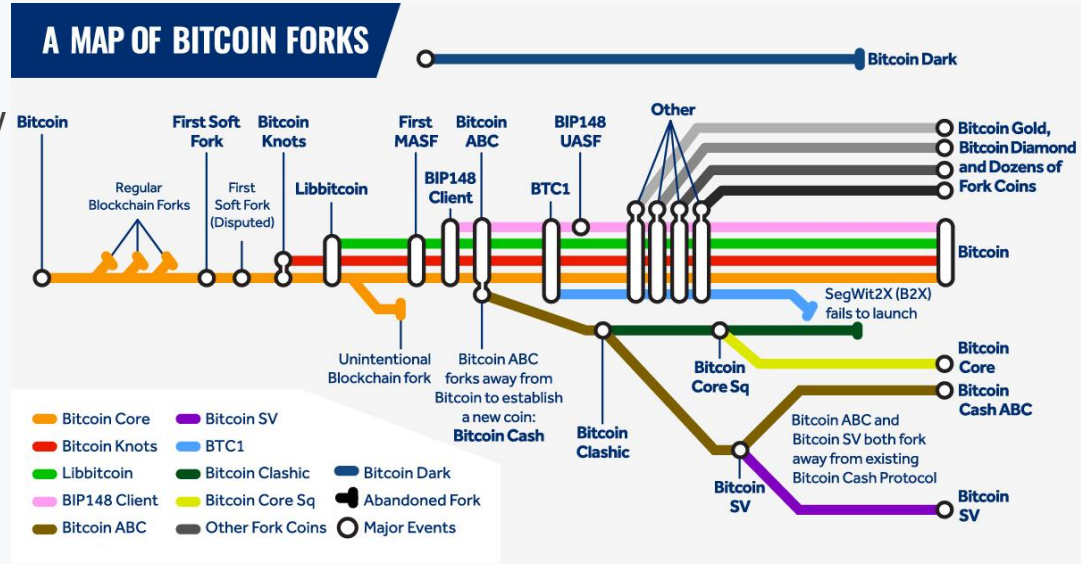
Double Spend

- However, if they do have enough hashing power...
- They can buy something like a nice car while they're accumulating blocks
- Finally, after they buy the car they can reverse the transaction



Hard Fork

- Miners can disagree about consensus/scalability/etc.
- If the sentiment is strong enough, groups of them work together to create a new fork that is a *hard fork*
- These cannot be reconciled with the new blocks on the "main chain"
- Biggest example: BTC and Bitcoin Cash
- Others: Bitcoin SV, Bitcoin Gold, ...



Questions/Comments?

Let's see how we can code a blockchain!