FINE 434: FinTech

Lecture 13

Professor Fahad Saleh

McGill University - Desautels

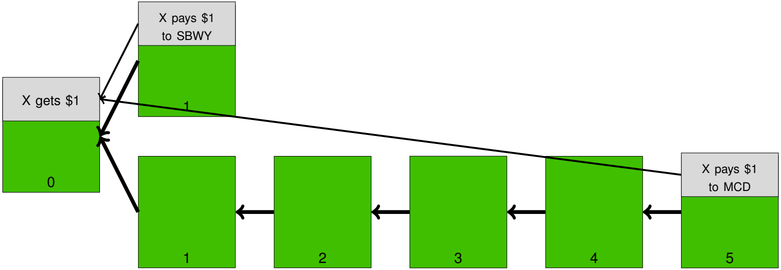
Double Spending Problem (DSP)

“The problem of course is the payee can’t verify that one of the owners did not double-spend the coin.”

“We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don’t care about later attempts to double-spend.”

Executing a Double Spend

“the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it... back to himself after some time has passed.”



Nakamoto's Solution

- **Transparency**
  "transactions must be publicly announced"
  $\Longrightarrow$ Public Blockchain

- **Consensus Protocol**
  "a system for participants to agree on a single history"
  Nakamoto's Solution: Proof-of-Work (PoW)

Aside: Dwork and Naor (1992) introduced PoW. Jakobsson and Juels (1999) coined the term "Proof-of-Work." Nakamoto cites Back (2002).

Goals

- Solve DSP
- Liveness
- Eventual Consensus

Nakamoto argues heuristically and focuses on the double spending problem. Nakamoto uses neither “liveness” nor “eventual consensus” within the paper. Nakamoto focuses upon economics rather than computer science but approaches the problem as a non-economist.

Nakamoto’s Description

“The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits.”

Nakamoto's Description

"The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits."

"we implement the proof-of-work by incrementing a [number] in the block until a value is found that gives the block's hash the required zero bits."

Nakamoto's Description

"The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits."

"we implement the proof-of-work by incrementing a [number] in the block until a value is found that gives the block's hash the required zero bits."

An approximate mathematical analog:

Given $T \in \mathbb{N}_+$, find $n \in \mathbb{N}$ such that $Int(Hex(Hash(n))) \leqslant T$

Honest Majority Assumption

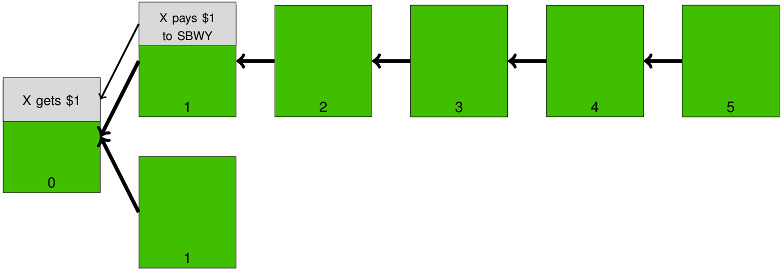
“The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.”

“[Honest nodes] always consider the longest chain to be the correct one and will keep working on extending it.”

“[Honest nodes] are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them.”

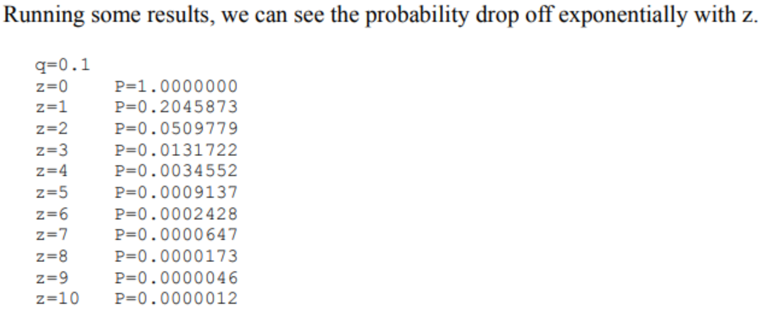
DSP and Eventual Consensus

“the recipient of a new transaction needs to wait before being sufficiently certain the sender can’t change the transaction.”



“an attacker would have to redo the proof-of-work [to] surpass the work of the honest nodes... the probability ... diminishes exponentially as subsequent blocks are added”

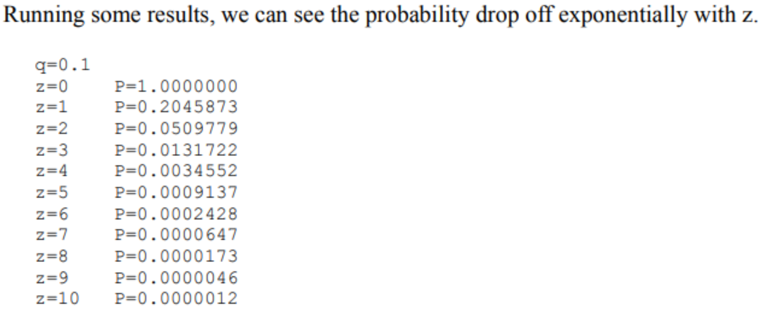
Attacker Success Probabilities



Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0    P=1.0000000
z=1    P=0.2045873
z=2    P=0.0509779
z=3    P=0.0131722
z=4    P=0.0034552
z=5    P=0.0009137
z=6    P=0.0002428
z=7    P=0.0000647
z=8    P=0.0000173
z=9    P=0.0000046
z=10   P=0.0000012
```

Attacker Success Probabilities



Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0      P=1.0000000
z=1      P=0.2045873
z=2      P=0.0509779
z=3      P=0.0131722
z=4      P=0.0034552
z=5      P=0.0009137
z=6      P=0.0002428
z=7      P=0.0000647
z=8      P=0.0000173
z=9      P=0.0000046
z=10     P=0.0000012
```

... why does this even imply that PoW overcomes DSP?

More Questions

- What about liveness - why would any node even work to solve the PoW puzzle?
- Why would honest nodes control the majority CPU power?
- Are there some hidden assumptions in Nakamoto's argument?
- What about economic relevance?

We take on each of these questions in subsequent lectures...