FruitChains
A Fair Blockchain
A single Block

nonce

Data: B
Blockchain

![Blockchain Diagram]

- Genesis block
- ... (continue with arrows)
- Nonce
- Data: A
- Nonce
- Data: B
Add a block

Pointer, Nonce and Data: C solves the crypto puzzle
Distributed Setting

Alice

Bob

Carol
Branches
Branches

B → C → F

D → C → B

C → F → D
Branches
Rewards (Bitcoin)

- Block Reward
- Transaction Fees
Mining Pools

Source: https://btc.com/stats/pool
Security Properties
Chain Consistency

Alice

A → B → C → D → E

Bob

A → B → C → F → G

k
Chain Growth

A → B

Time $T_0$

A → B → C → D

Time $T_1, T_1 > T_0$
Chain Quality
Selfish Mining Attack
Selfish Mining Attack

Public Chain

Private Chain
Selfish Mining Attack
Selfish Mining Attack

Public Chain

Private Chain

Diagram showing the interaction between nodes B, C, D, E, and F in a blockchain network, with arrows indicating transactions or communication flows.
Selfish Mining Attack

B ➔ C ➔ D ➔ E

Public Chain

Private Chain
Selfish Mining Attack (Case 2)
Selfish Mining Attack (Case 2)

\[ \gamma: \text{fraction of honest players that mine on block D} \]
Expected Revenue

- *Optimal Selfish mining strategies in bitcoin (2016)*
  - By Sapirshtein, Sompolinsky, Zohar
Expected revenue

\[ \gamma = 0 \]

\[ \gamma = 1 \]
«Quick Fix» for Selfish Mining

\[ \gamma = 0.5 \]
FruitChains: A Fair blockchain

Computational Power

reward
High-level view

B contains

contains

Data: A
Structure
Structure
Mining a Fruit/Block

Hash

• Pointer to last block
• Pointer to a block far “enough” away
• Random nonce
• Hash of the set of recent fruits
• Data
Fruit

• Verifies data

• Pointer to last block
• Pointer to a block far “enough” away
• Random nonce
• Hash of the set of recent fruits
• Data
Block

- Verifies fruits

- Pointer to last block
- Pointer to a block far “enough” away
- Random nonce
- Hash of the set of recent fruits
- Data

- Hash of fruits
- nonce
New Reward System
Security Properties
Fruit “Freshness”
Fruit Consistency

Alice

Bob
Fruit Growth
Fruit Fairness
Why does this work?

• Selfish Mining Attack
• Fruit Flooding
Disincentivise Mining Pools

Mining Pools -> Partial Solutions -> FruitChains

Reward mining fruits
Conclusion
References

• Bitcoin / Blockchain

• Selfish Mining Attack
  • Eyal, Sirer, *Majority is not enough: Bitcoin mining is vulnerable* (2014)

• FruitChains