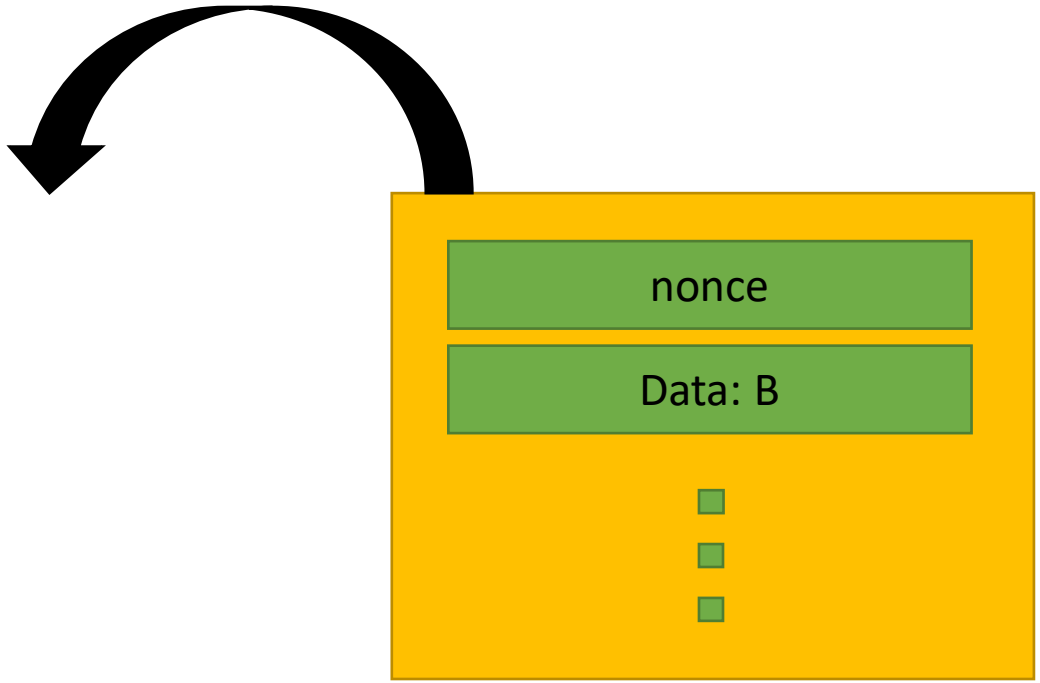
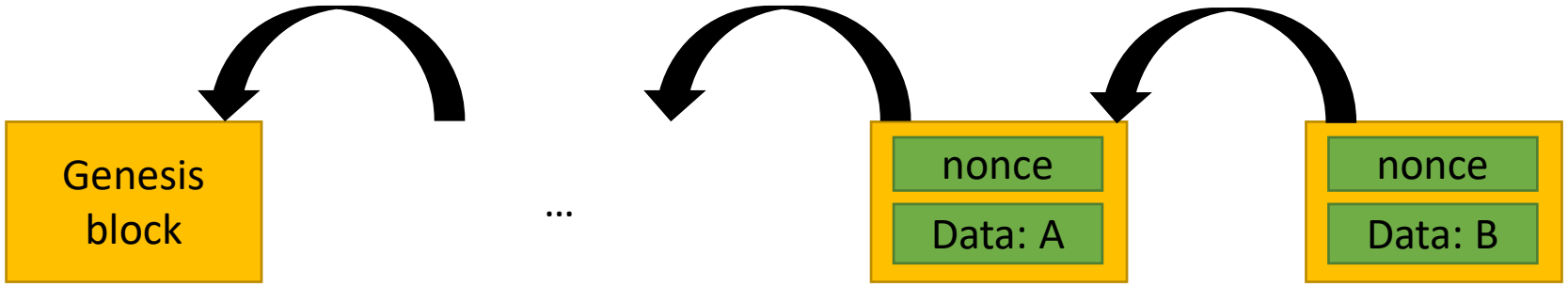
FruitChains

A Fair Blockchain

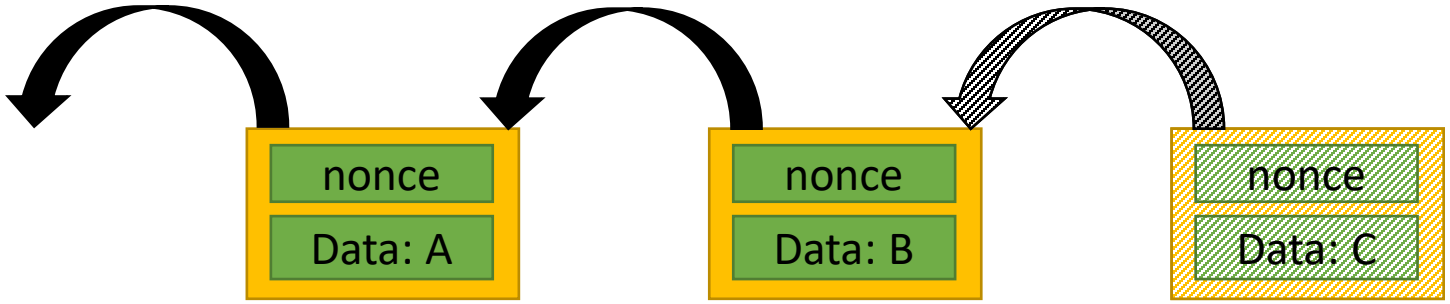
A single Block



Blockchain

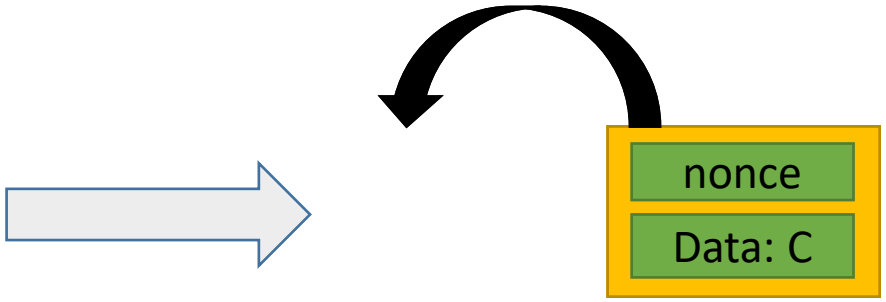


Add a block



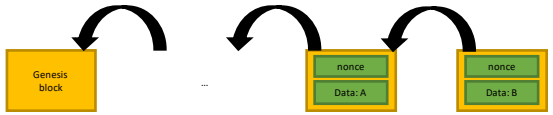
Pointer, Nonce and Data: C

solves the crypto puzzle

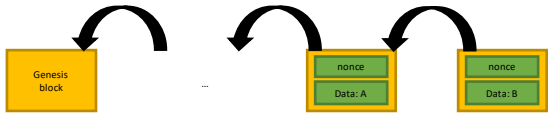


Distributed Setting

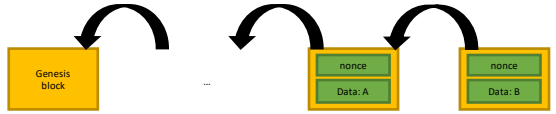
Alice



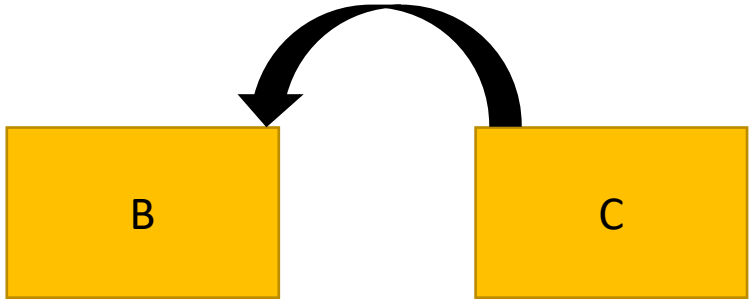
Bob



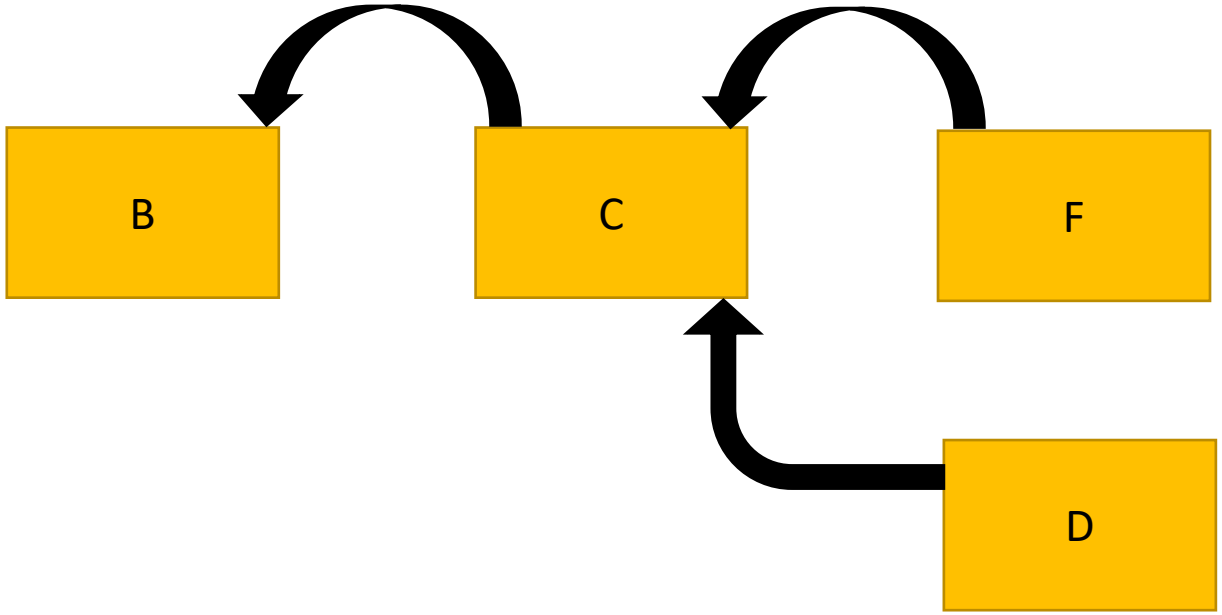
Carol



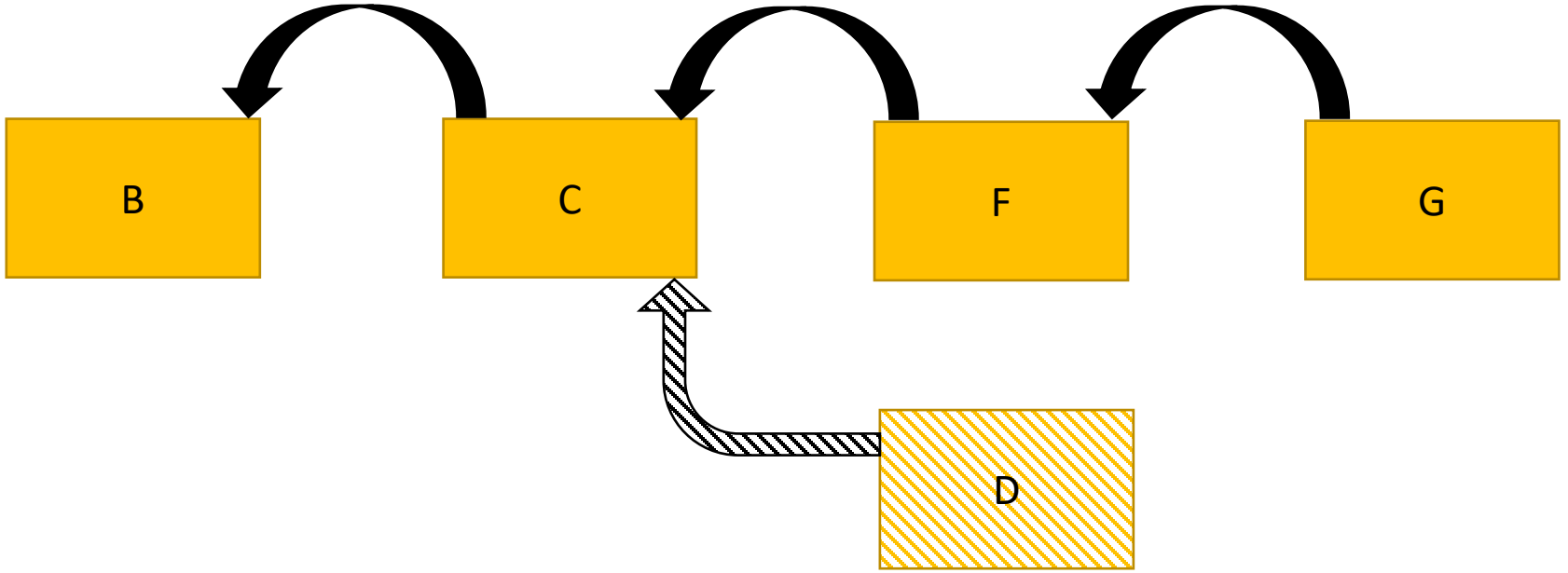
Branches



Branches



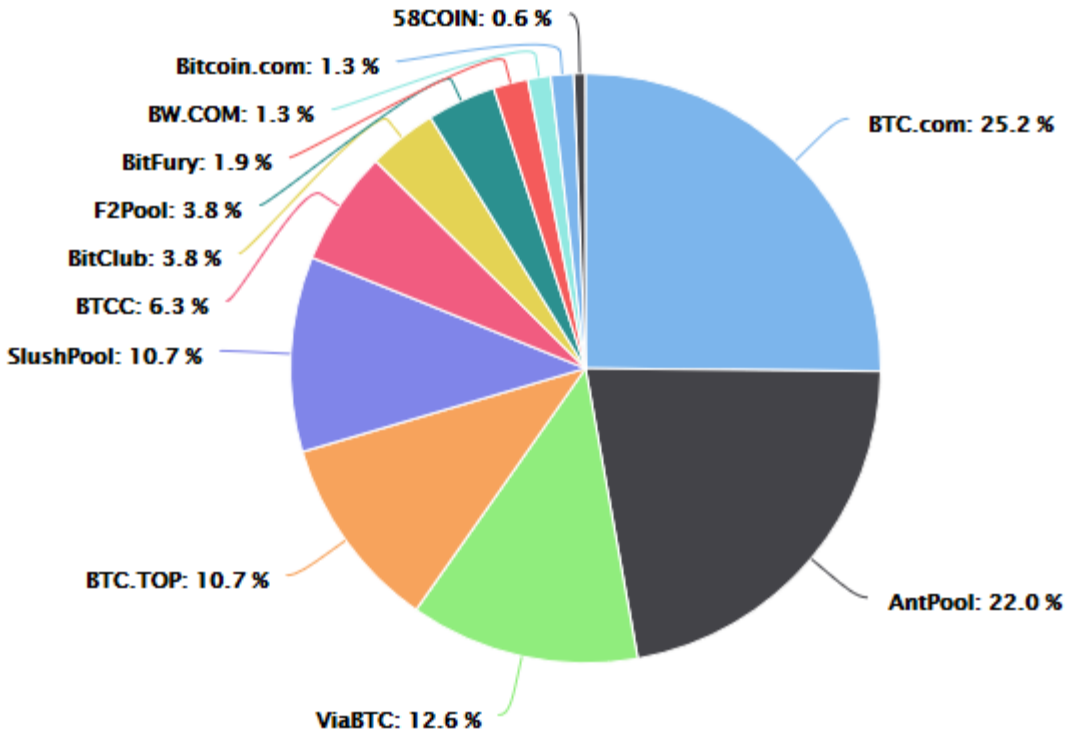
Branches



Rewards (Bitcoin)

- Block Reward
- Transaction Fees

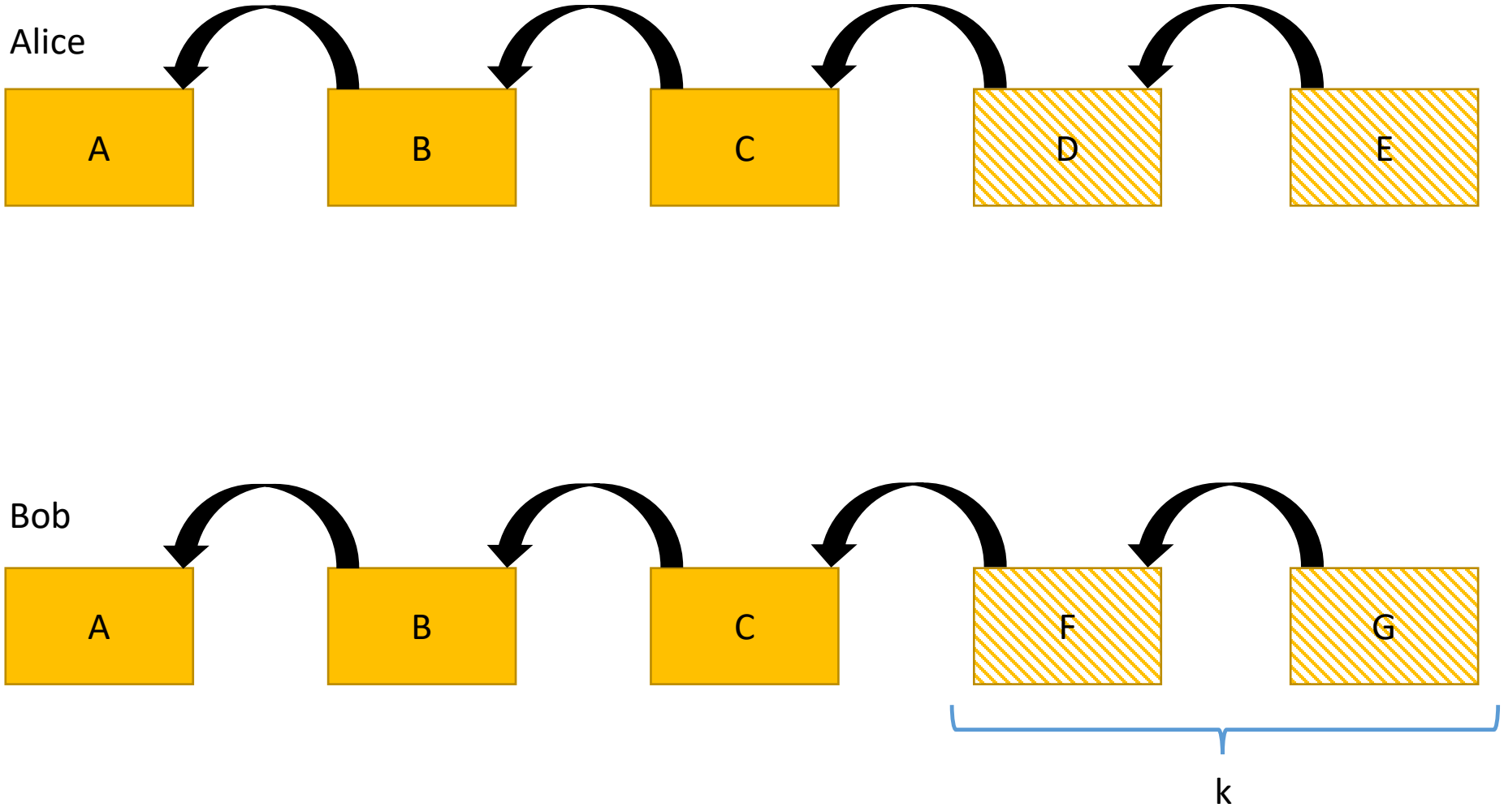
Mining Pools



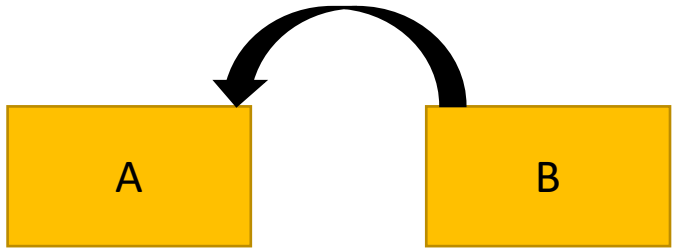
Source: https://btc.com/stats/pool

Security Properties

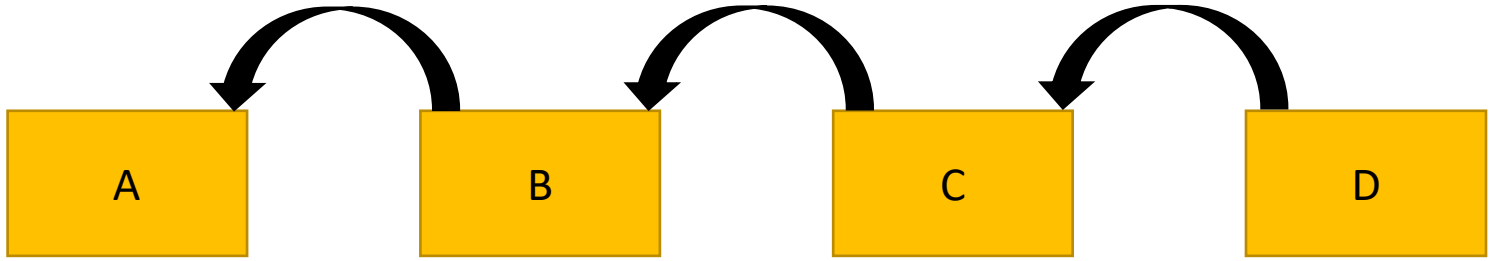
Chain Consistency



Chain Growth

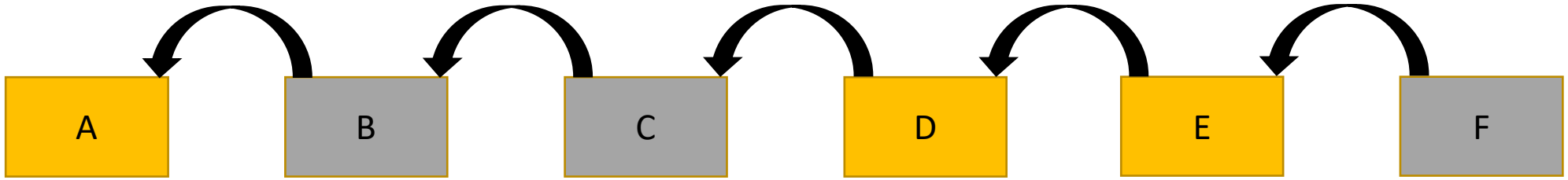


Time T_0



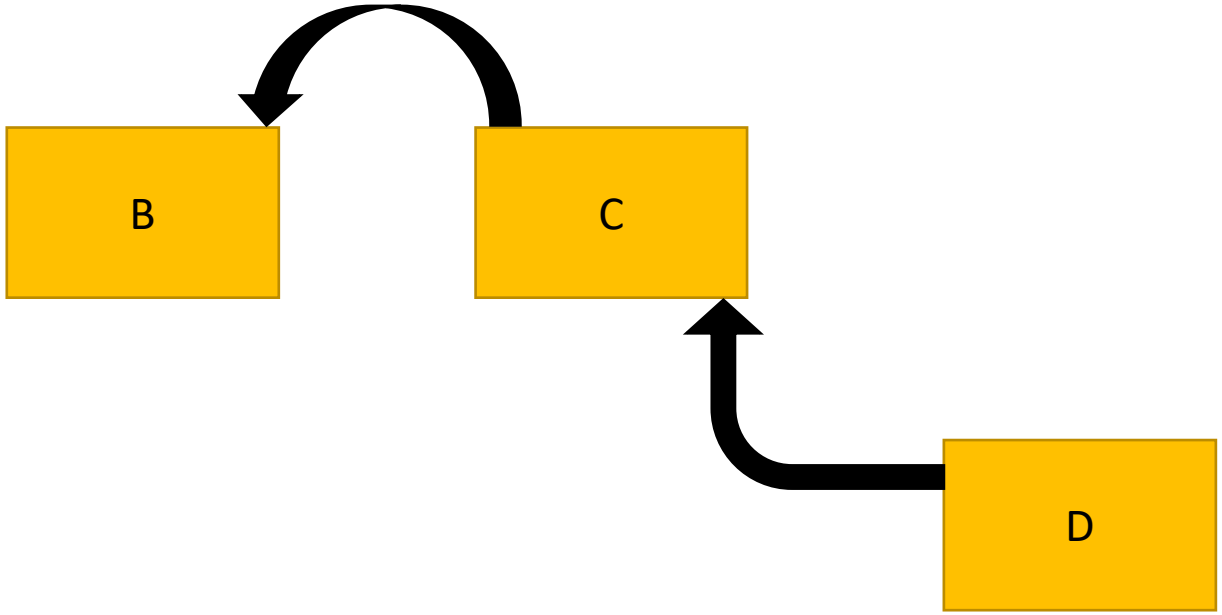
Time $T_1, T_1 > T_0$

Chain Quality



Selfish Mining Attack

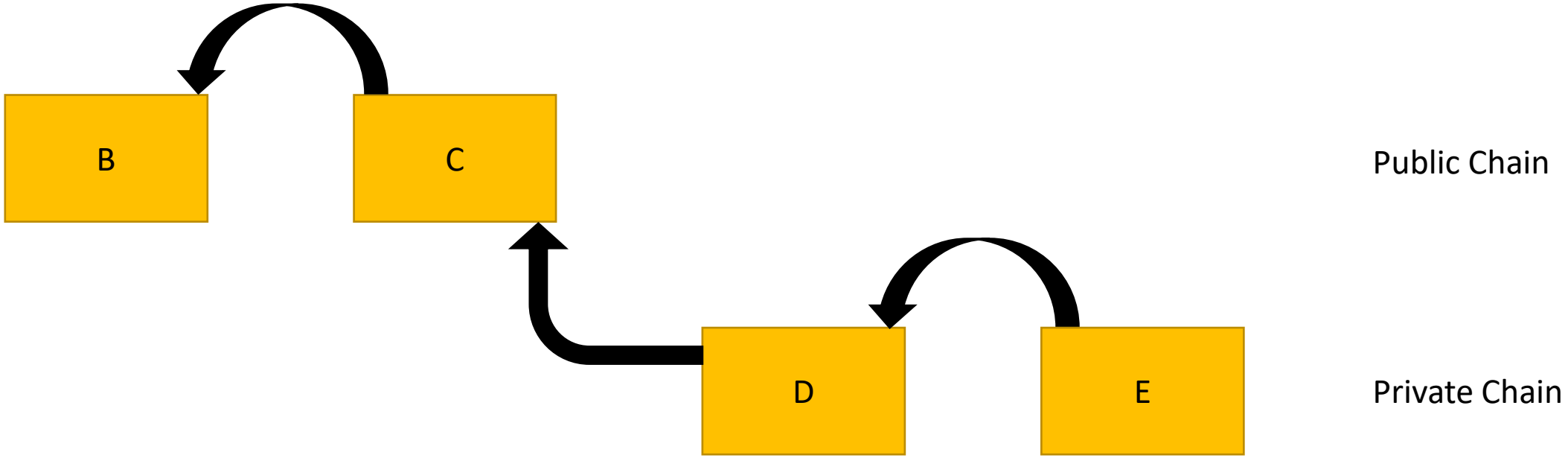
Selfish Mining Attack



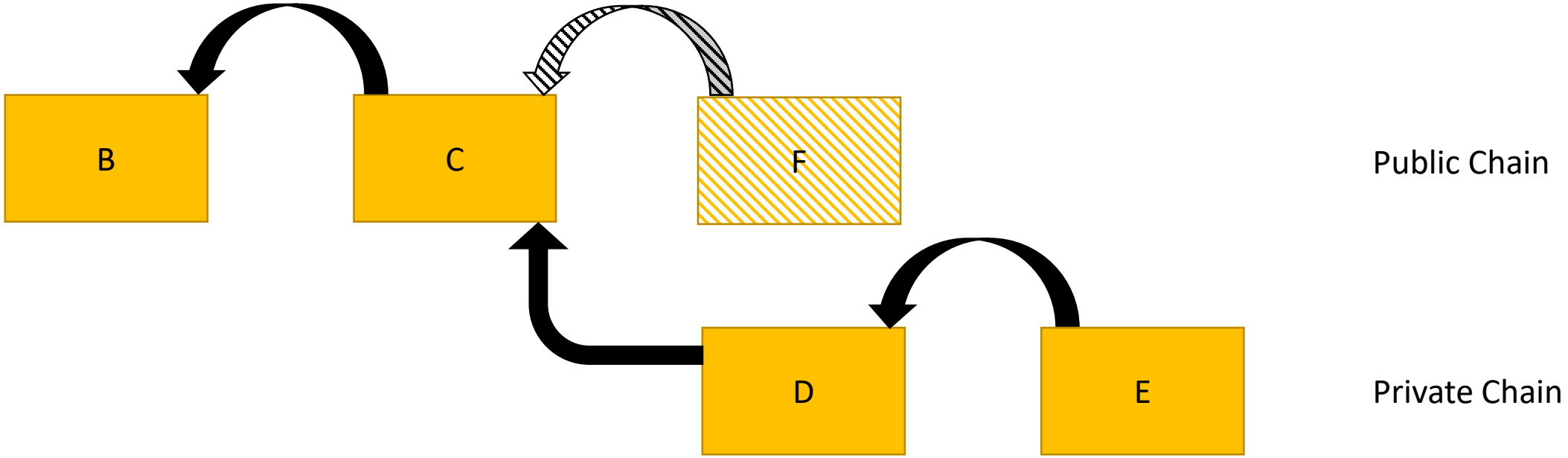
Public Chain

Private Chain

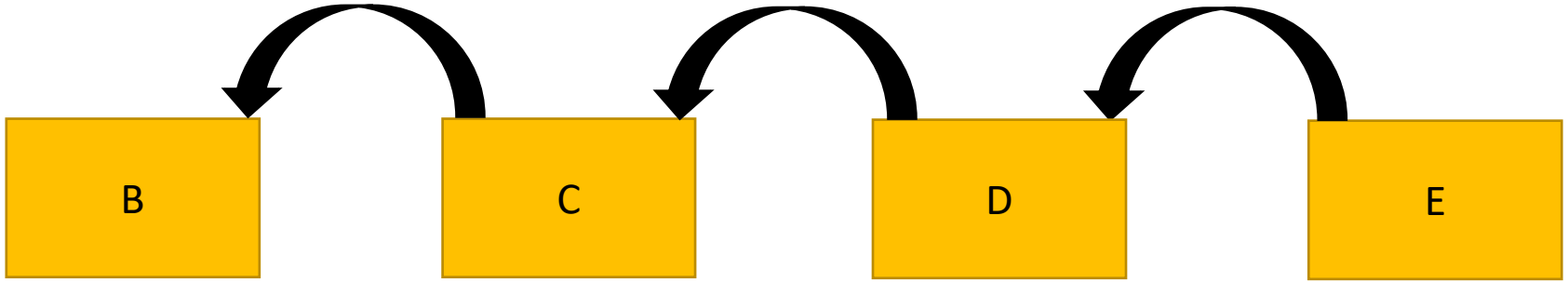
Selfish Mining Attack



Selfish Mining Attack



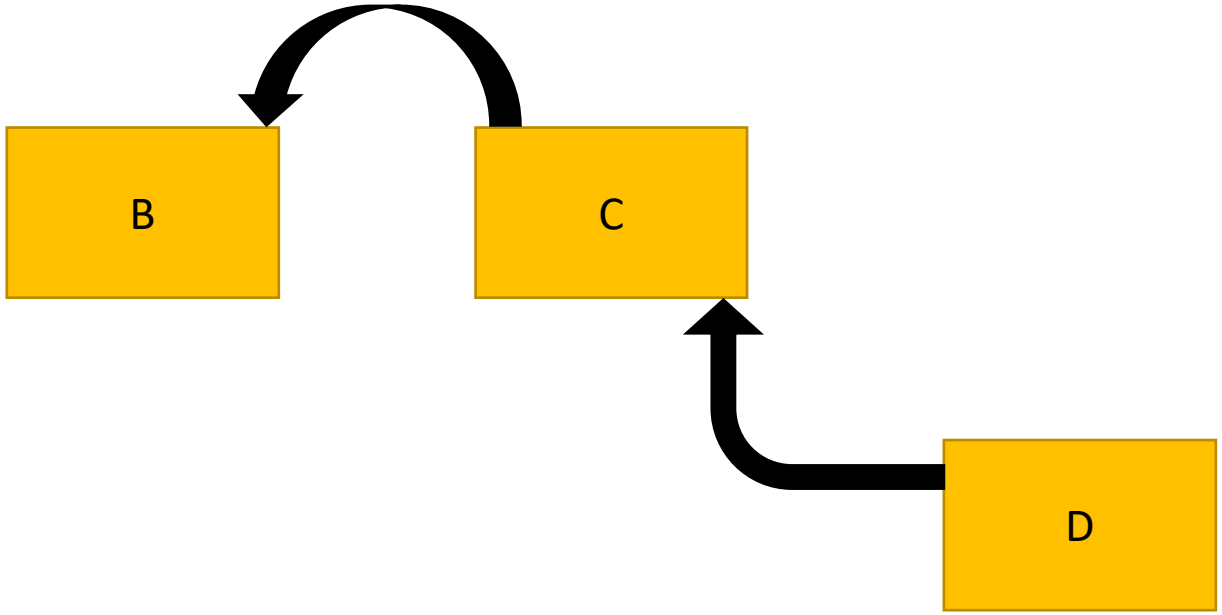
Selfish Mining Attack



Public Chain

Private Chain

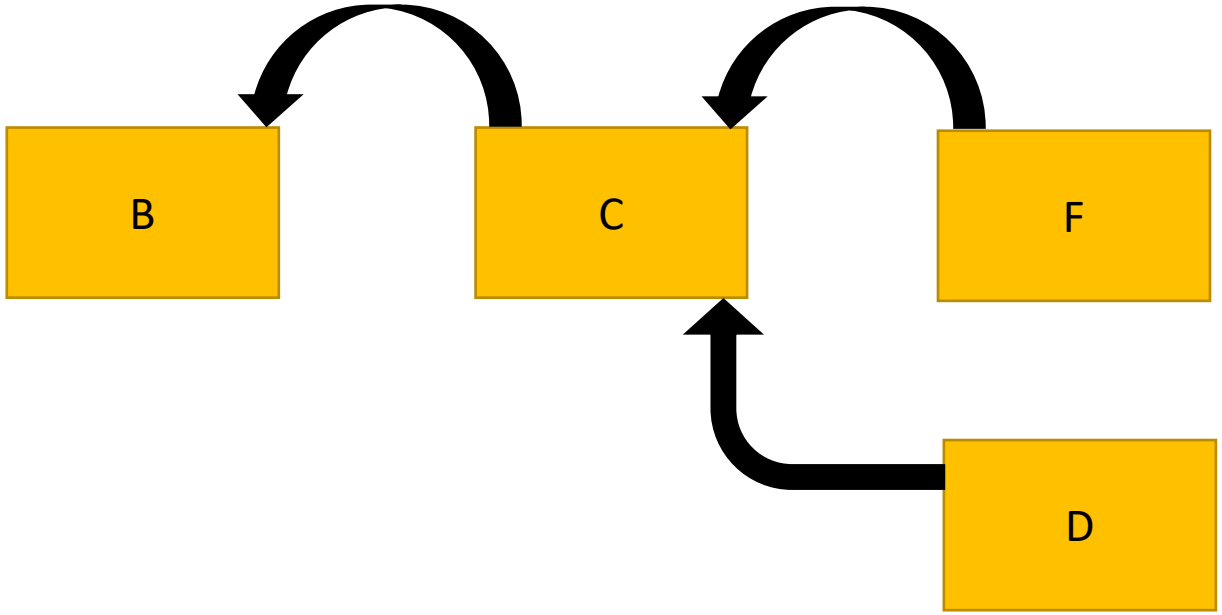
Selfish Mining Attack (Case 2)



Public Chain

Private Chain

Selfish Mining Attack (Case 2)



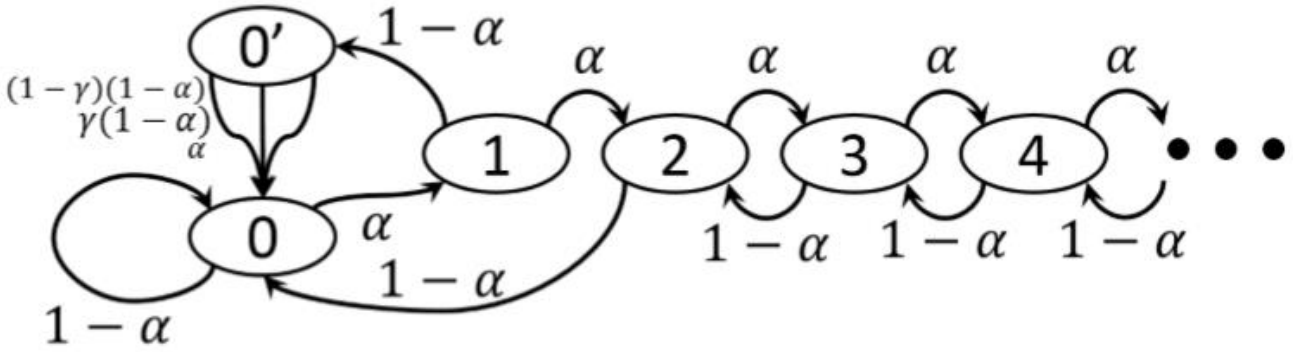
Public Chain

Private Chain

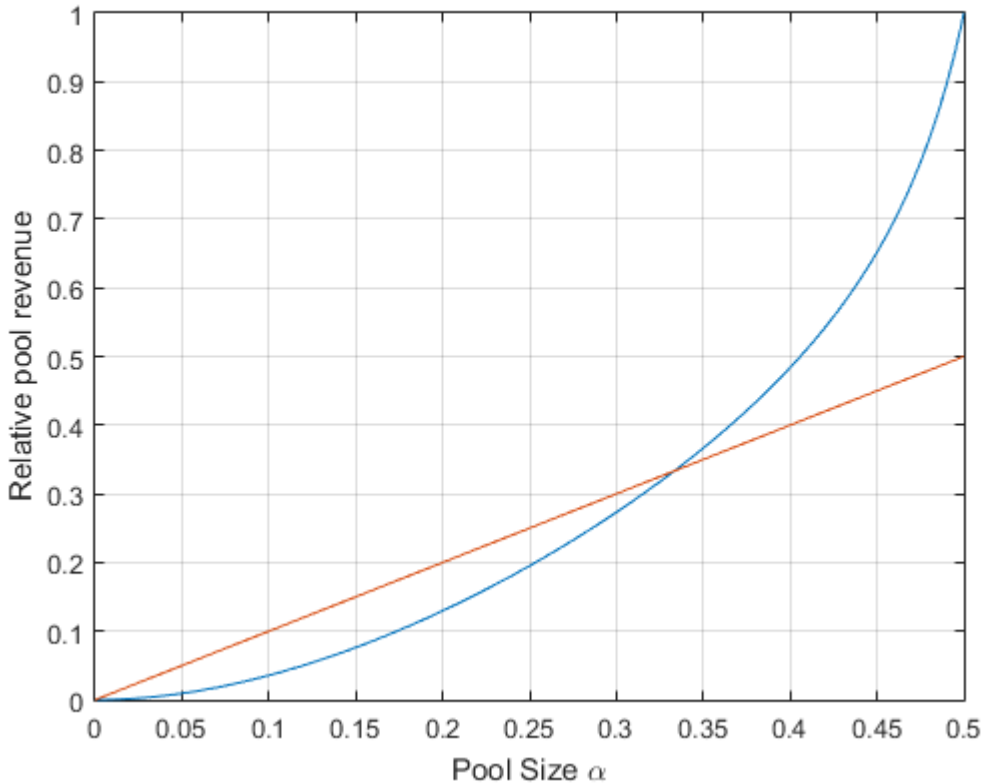
γ: fraction of honest players that mine on block D

Expected Revenue

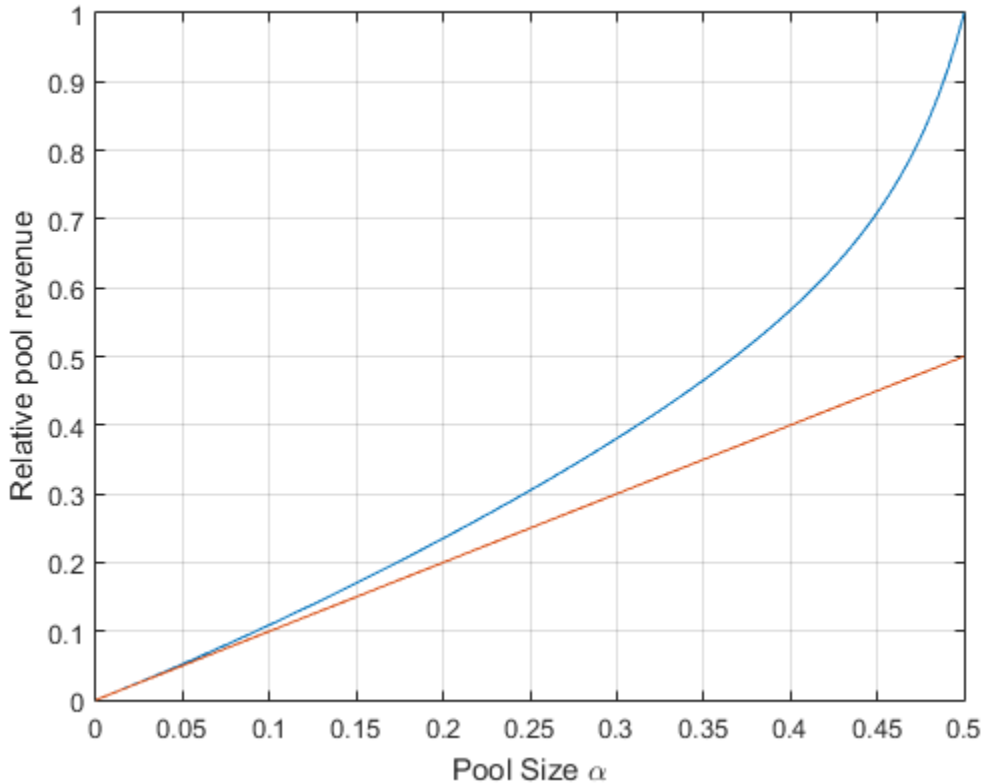
- *Optimal Selfish mining strategies in bitcoin (2016)*
  - *By* Sapirshtein, Sompolinsky, Zohar



Expected revenue

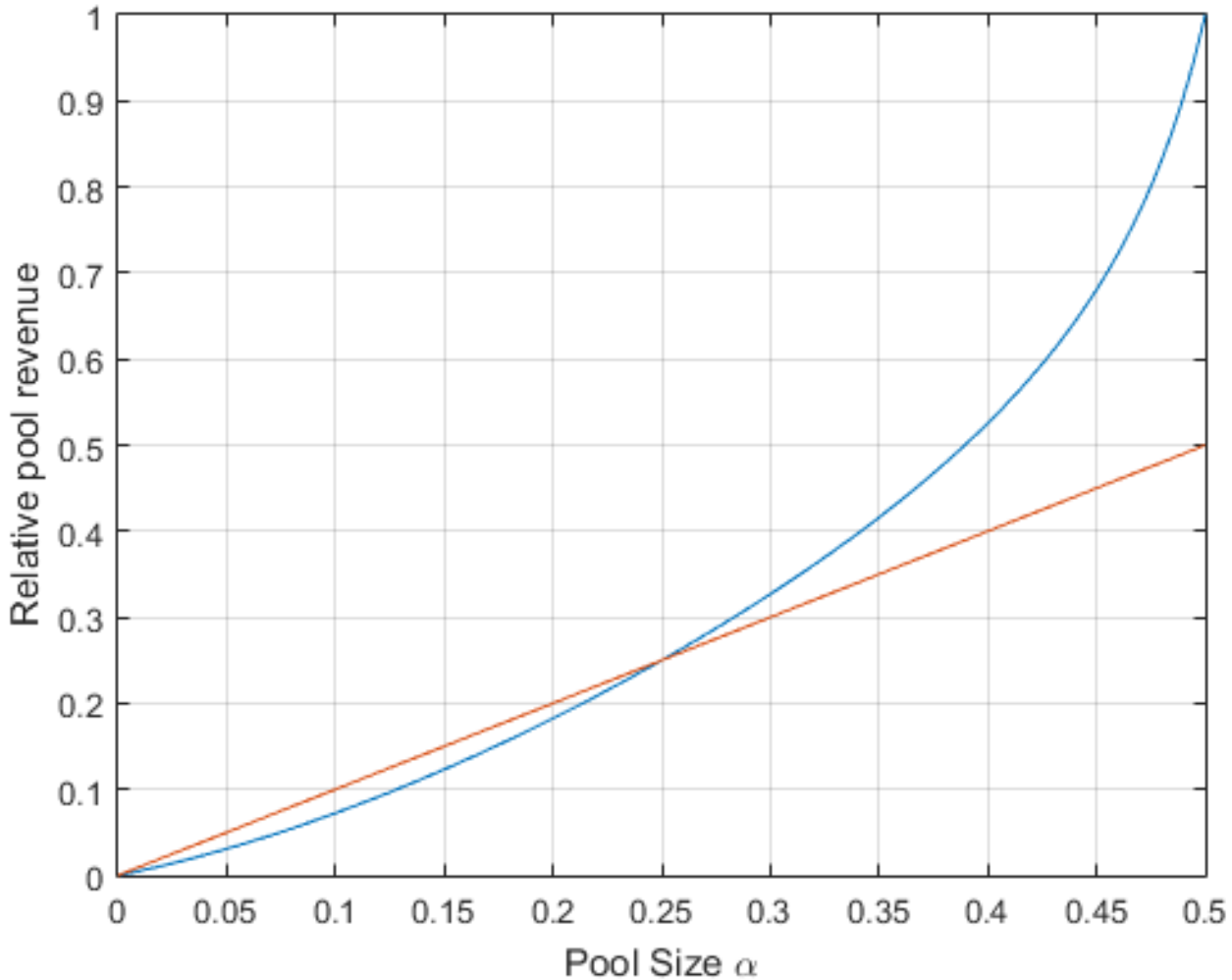


$\gamma = 0$



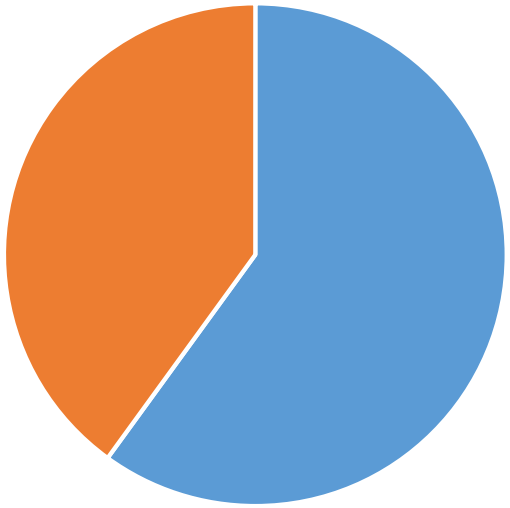
$\gamma = 1$

«Quick Fix» for Selfish Mining

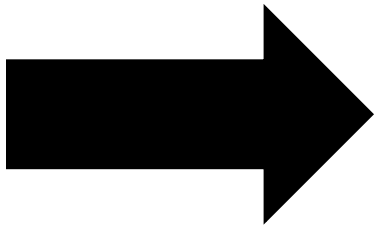


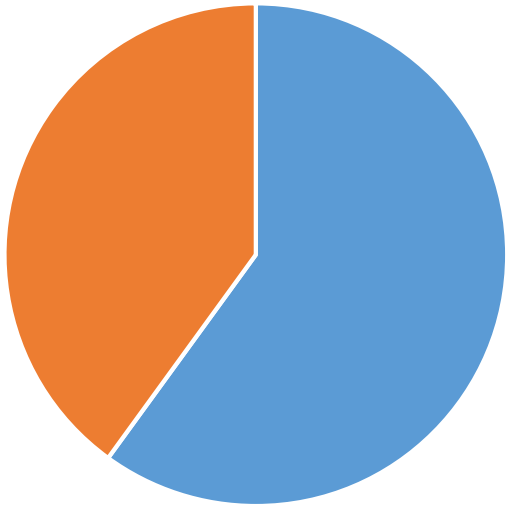
γ = 0.5

FruitChains: A Fair blockchain



Computational Power

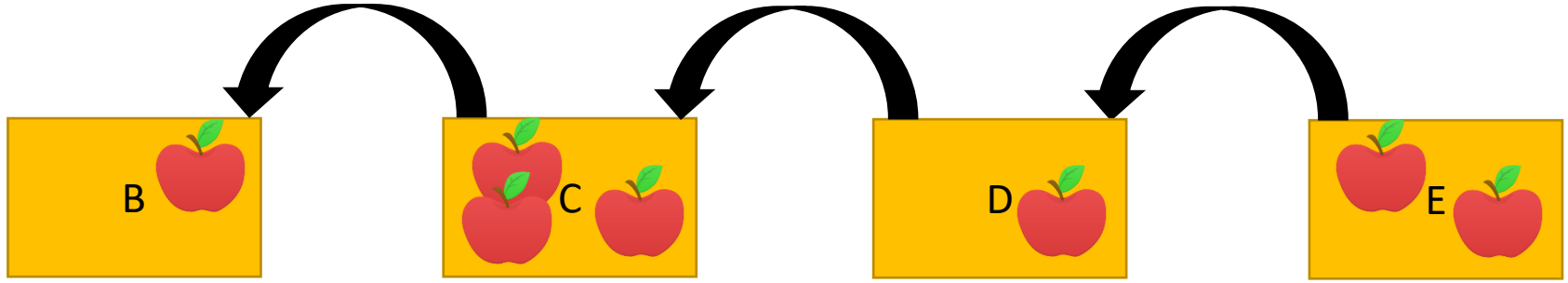


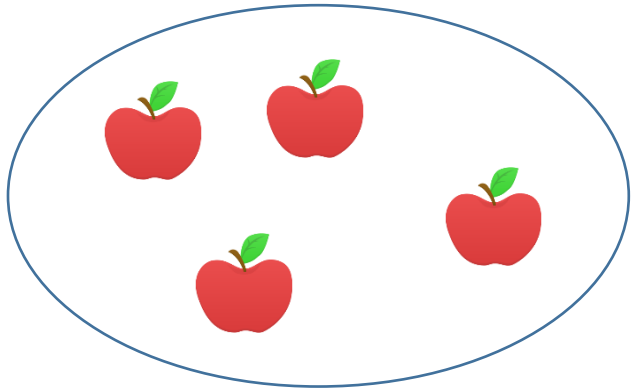


reward

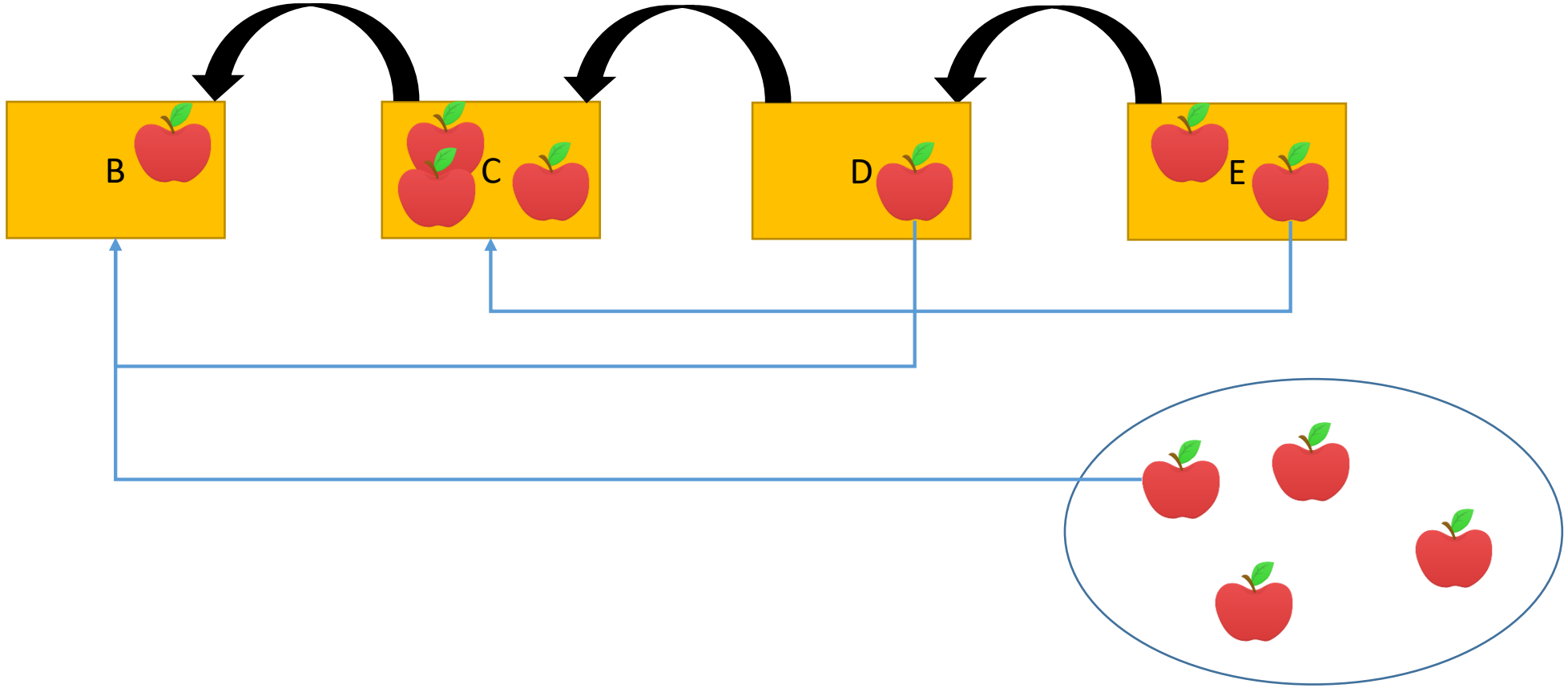
High-level view

Structure





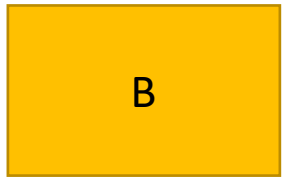
Structure



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

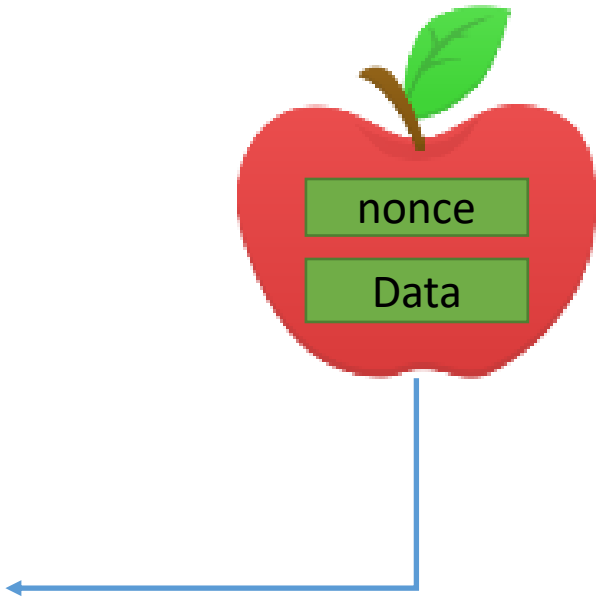


Junk

Fruit

- Verifies data

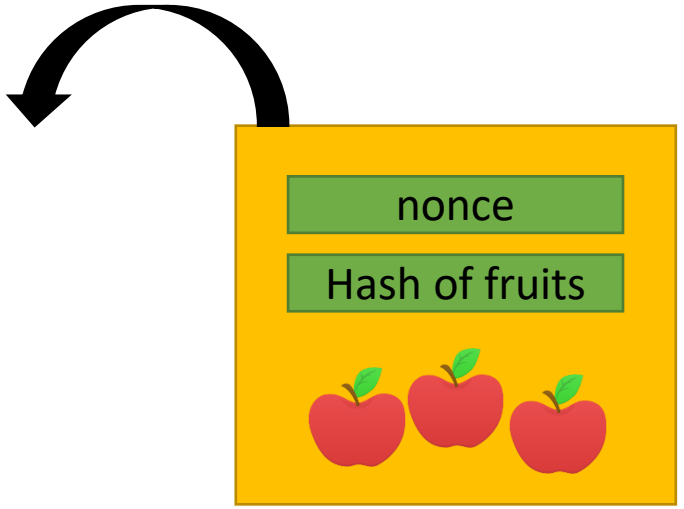
- ~~Pointer to last block~~
- Pointer to a block far “enough” away
- Random nonce
- ~~Hash of the set of recent fruits~~
- Data



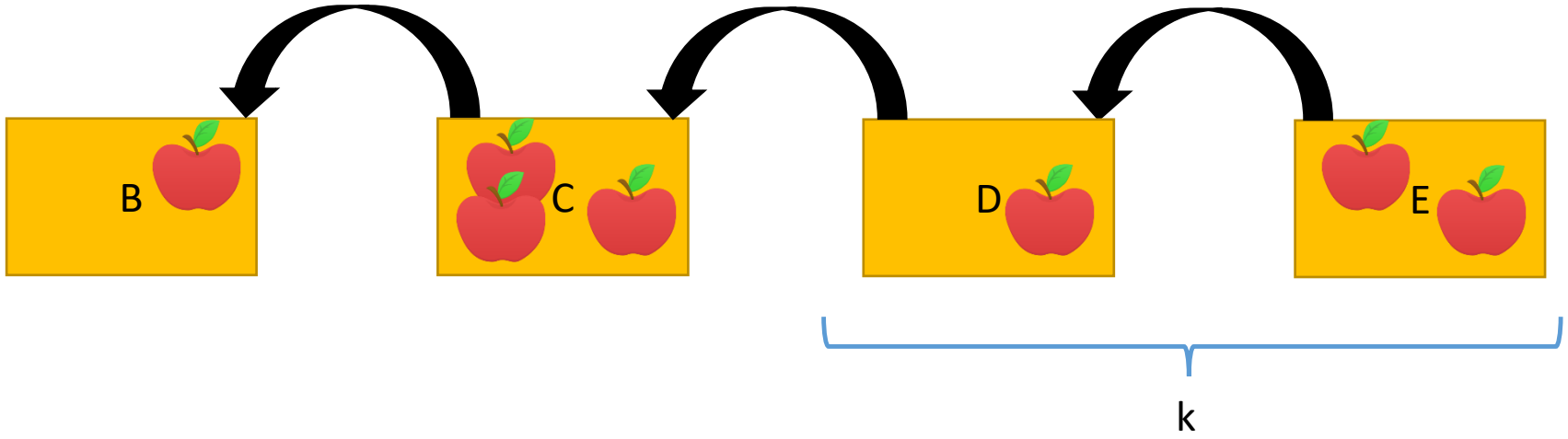
Block

- Verifies fruits

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

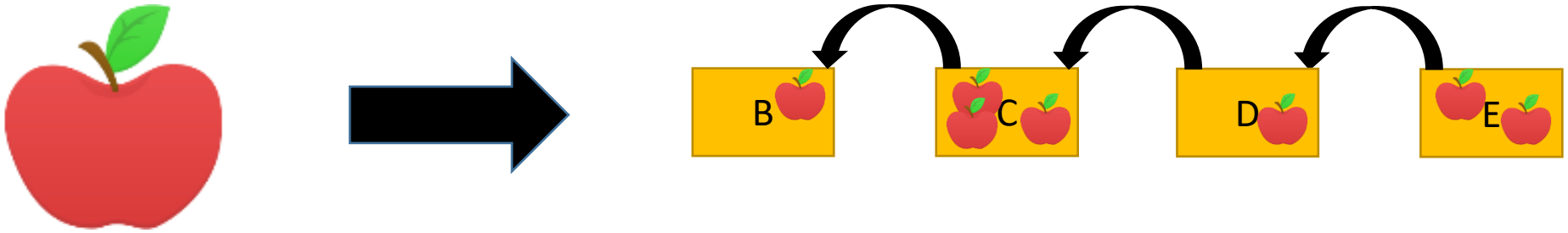


New Reward System

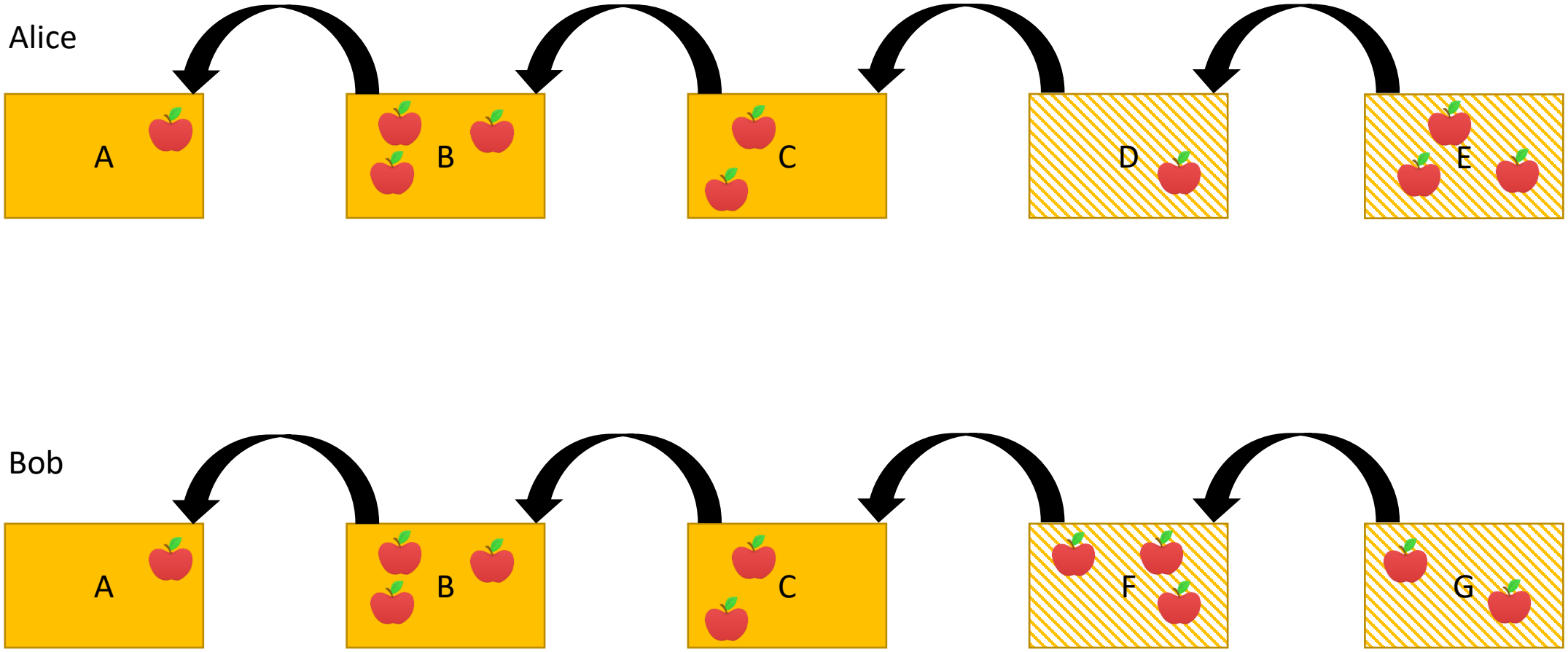


Security Properties

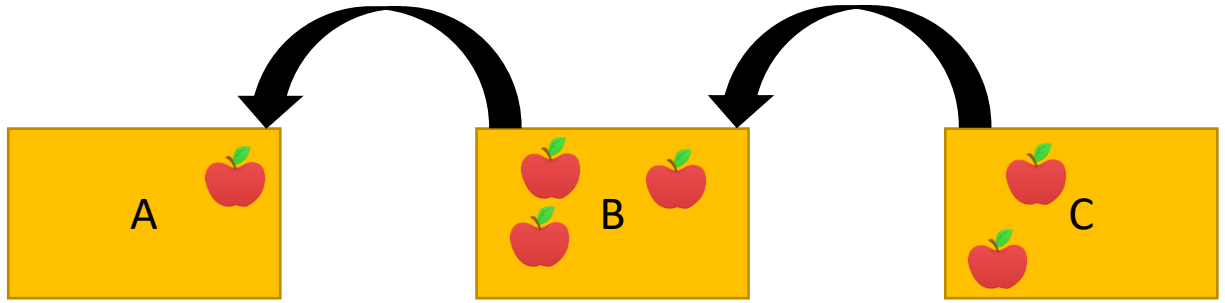
Fruit “Freshness”

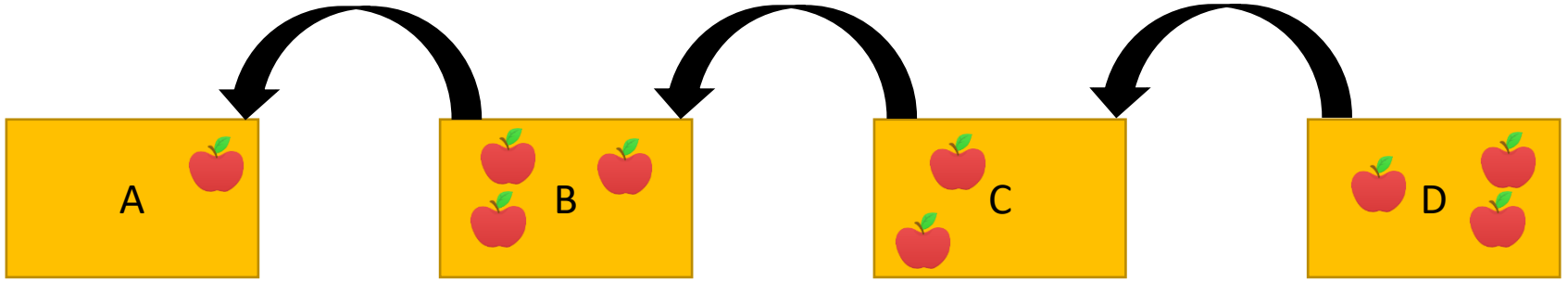


Fruit Consistency

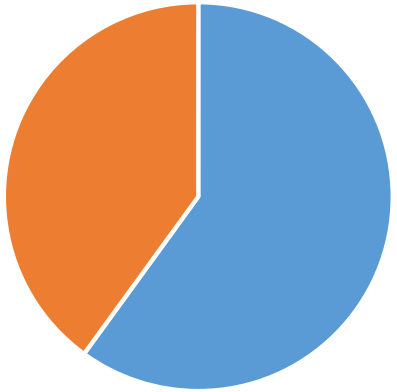


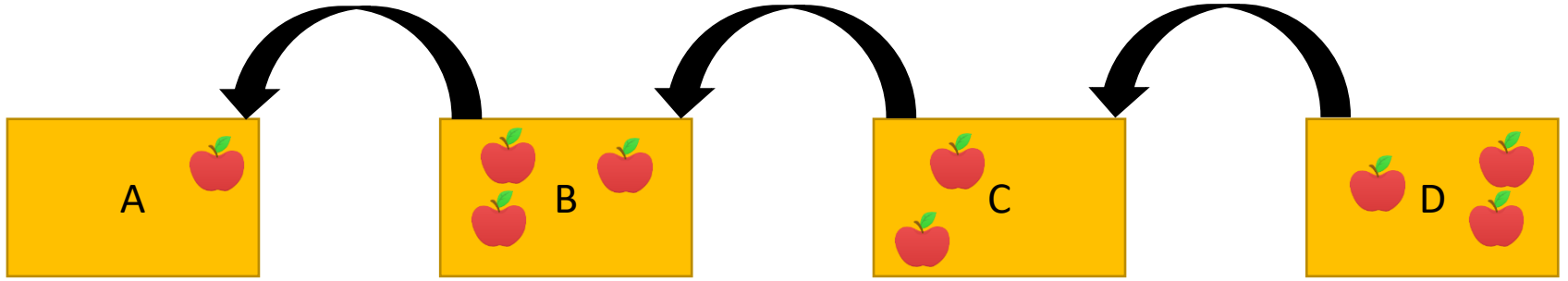
Fruit Growth





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
  - Nakamoto, *Bitcoin: A peer-to-peer electronic cash system* (2008)
  - Pass, Seeman, Shelat, *Analysis of the blockchain protocol in asynchronous networks* (2017)
- Selfish Mining Attack
  - Eyal, Sirer, *Majority is not enough: Bitcoin mining is vulnerable* (2014)
  - Sapirshtein, Sompolinsky, Zohar, *Optimal Selfish mining strategies in bitcoin* (2016)
- FruitChains
  - Pass, Shi, *FruitChains: A Fair Blockchain* (2017)