Cryptocurrency, Imperfect Information, and Fraud

Yiting Li Chien-Chiang Wang

October 9, 2020

Introduction

- Cryptocurrency is a new payment system that maintains a public transaction ledger in a distributed manner
- Everyone can have their own version of the ledger. Payers make payments by sending transaction messages to other participants
- In some cryptocurrency such as Bitcoin, record makers or traders are required to solve difficult hash problems to update the ledger, called **proof-of-work (PoW)**
- In some other cryptocurrencies, the updating of the ledger requires some deposits or stakes, called **proof-of-stake (PoS)**
- PoW and PoS generate a loss to the provider but does not directly benefit anyone

Imperfect Network: Consensus Algorithm

- If the message sending is perfect, then the message sending system itself can serve as a perfect settlement system (Yap island stone money)
- Why do we need PoW and PoS in cryptocurrency?
- In cryptocurrency, the messages are sent through the internet, which is an imperfect message sending system (missing, delay, and error)
- Through the imperfect system, participants may not receive messages as the order they were sent (disagreement)
- Consensus algorithms are applied to create agreements

Imperfect Network: Double Spending

- This imperfection also provide traders incentives to disrupt the consensus system and take advantage by sending inconsist messages
- The double spending fraud:
  - an attacker initially sends a message to make a payment to a merchant, receive goods, and then sends another message (double-spending message) to transfer her balance to another account owned by herself (or another merchant)
  - if the double spending message instead of the original message is recognized as the real one by the consensus system, the merchant will not receive the payment

Literature

- Computer science literature: Bitcoin protocol satisfies consistency if the computing power owned by adversary players is less than 50% (Pass, Seeman, shelaty 2016, Garay, Kiayias, Leonardosy 2017)
- The thing missing in computer science literature: rationality of players
- Literature in monetary search: Chiu and Koeppl 2017
- Counterfeiting/fraud: Wallace and Nosal 2007, Rocheteau, Li, Weill 2012

Main Results

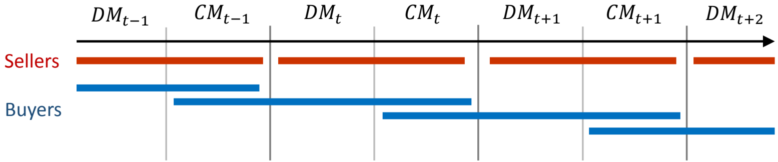
- We study the relationship between PoW, PoS, and the imperfectness of message sending
- PoW and PoS can deterring double spending and may improve the efficiency of cryptocurrency
- PoW and PoS are costly. Imposing a high PoW or PoS to deter double spending may not be optimal in some circumstance
- When the network imperfectness diminishes, cryptocurrency can serve as an efficient means of payment

The Model

- Lagos and Wright (2005), Rocheteau and Wright (2005)
- Two types of agents: buyers and sellers
- $t = 0, 1, 2, 3, \ldots$. Each period has two subperiods:
  - DM: a buyer and a seller meet bilaterally (trade stage)
  - CM: centralized market (settlement stage)

The Model

- Agents are short-lived in the economy
- Buyers enters at the CM, consumes at the next DM and leaves at the next CM
$$X_t + \beta \left[u_t(x_{t+1}) + X_{t+1} \right]$$
- Sellers enters at the DM, produce at the DM and leaves at the CM
$$-l_t + H_t$$
- Buyers and sellers can produce and consume at the CM

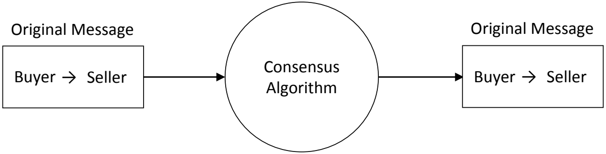


Cryptocurrency System

- No physical assets. No commitment. Traders are anonymous. No credit
- There is a cryptocurrency system
  - A set of digital addresses
  - A consensus algorithm
- Agents can create accounts on the addresses freely. They make payment between accounts by sending transaction messages
- We do not model details about consensus formations or blockchains and miners

Consensus Algorithm

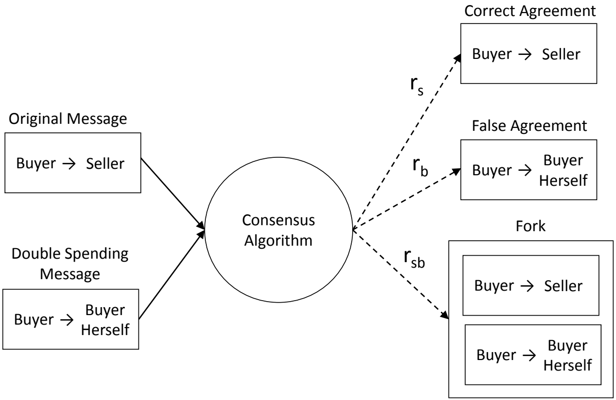
- We abstract the consensus algorithm as an imperfect message sending system
- People send messages to all others through the system. The outcome of the system is observable by all others (agreement)
- If the buyer sends only one transaction message (the original message), the message will be included in the consensus outcome (recognized by the system) for sure



▸ Appendix

Consensus Algorithm

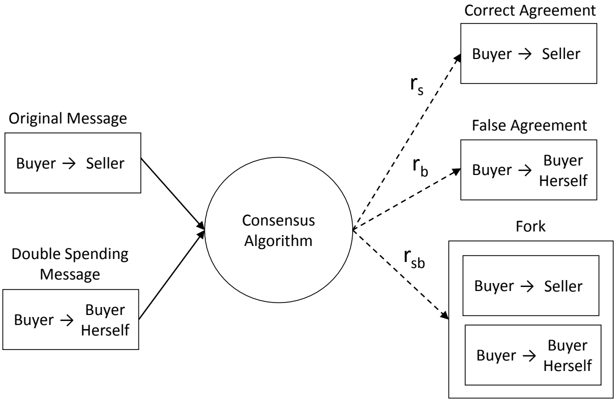
- The buyer can send a double spending message after the transaction to transfer the balance to another account owned by her
- Three mutually exclusive consensus outcomes may occur:



▸ Consensus

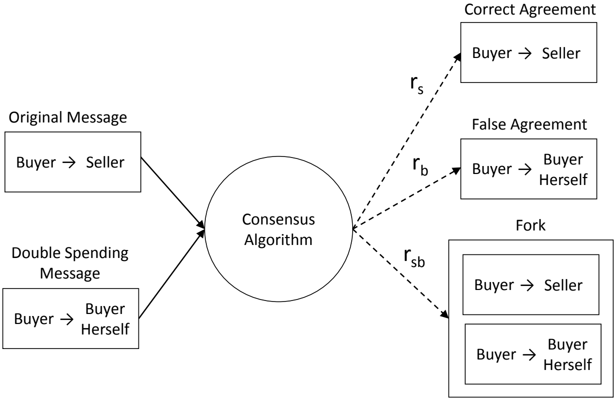
Consensus Algorithm

- (r_s, r_b, r_{sb}) is exogenously determined (by the development of the network)
- Assumption 1: $r_s > r_b$
- Assumption 2: $r_s + r_b + r_{sb} = 1$



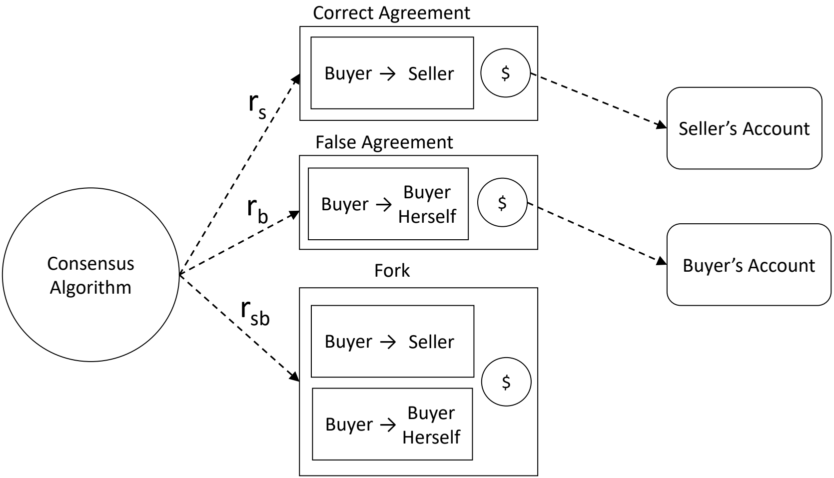
Consensus Algorithm

- Agents cannot distinguish an original message from a double spending messag, so they cannot tell whether the outcome is a correct agreement or a false agreement.
- They can only distinguish a single outcome from a fork
- Thus, forks can be applied as signals to detect double spending

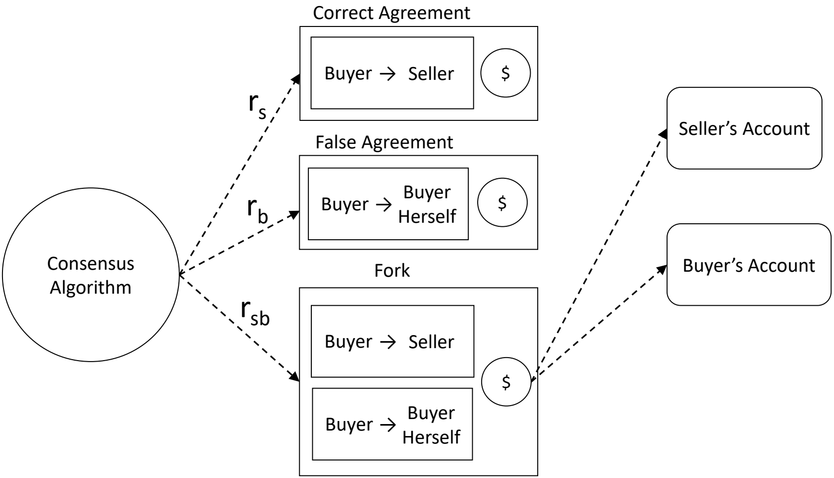


- Message sending is frictionless at the CM

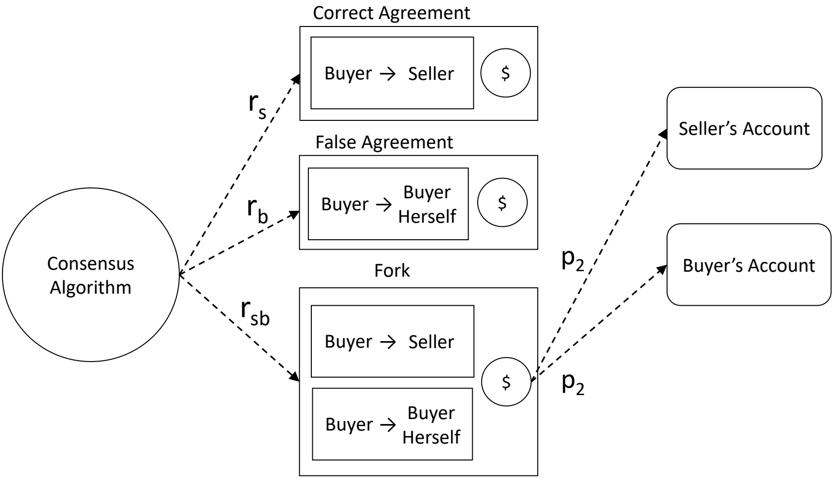
Consensus Algorithm



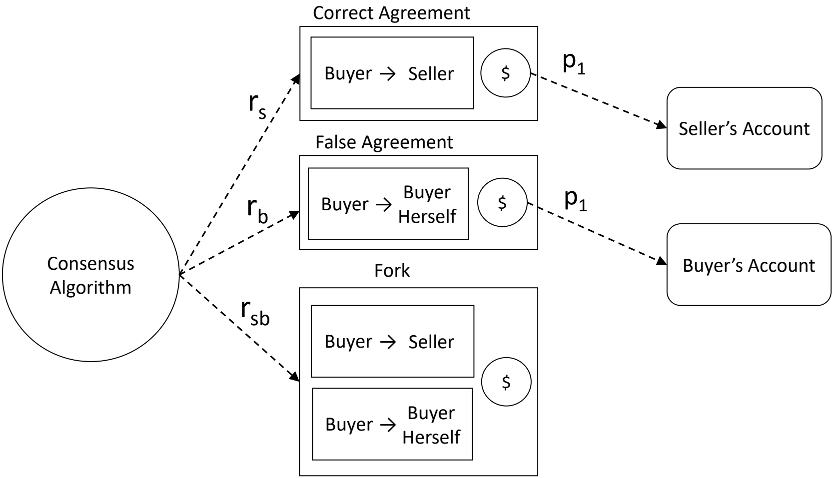
Consensus Algorithm



Consensus Algorithm



Consensus Algorithm



Preventing Double Spending

- If sending messages is costless, double spending will be a dominant strategy
- **PoW**: sending a message costs the payer k units of disutility
- **PoS**: the payer is required to put δ units of balance as deposits
- The return of the deposit can also be conditional on the consensus outcome, denoted by (q_1, q_2)

Preventing Double Spending

- $(k, \delta, p_i, q_i, \pi, \tau)$ is the mechanism
- The inflation rate: π
- Transaction subsidy: τ
- Let $\hat{z} \equiv z + \tau$ be the post-subsidy payment
- The transfer, $\hat{z}$, is observable in a message, so (p_i, q_i) can also depend on, $\hat{z}$ (Hu-Kennan-Wallace mechanism)
- Our goal is to solve for the optimal mechanism given the environment (r_s, r_b, r_{sb})

The Timeline

- We first analyze the trading game given the environment (r_s, r_b, r_{sb}) and the mechanism $(k, \delta, p_i, q_i, \tau, \pi)$

1. CM: Buyer purchases balance
2. DM: Three substages
   a. Offer stage: buyer provides a TIOLI offer $(\hat{z}, x)$ to the seller
   b. Response stage: Seller decides to accept or reject the offer
   c. Post-trade stage: buyer decides to double spend or not

Post-Trade Strategy

- Buyer's post-trade strategy (σ): the probability that the buyer is honest is determined by the cost and benefit of double spending

$$\sigma \in B(\hat{z}) = \begin{cases} 1 & \text{if } \theta_d^b \hat{z} < k + (\eta_h - \eta_d)\delta \\ [0,1] & \text{if } \theta_d^b \hat{z} = k + (\eta_h - \eta_d)\delta \\ 0 & \text{if } \theta_d^b \hat{z} > k + (\eta_h - \eta_d)\delta \end{cases}$$

where

θ_d^b : Pr (buyer receives the payment| buyer double spends)

η_d : Pr (buyer receives the deposit return| buyer double spends)

η_h : Pr (buyer receives the deposit return| buyer is honest)

$$\begin{aligned} \theta_d^b &= p_1 r_b + p_2 r_{sb} \\ \eta_d &= q_1 \\ \eta_d &= q_1 (r_s + r_b) + q_2 r_{sb} \end{aligned}$$

TIOLI Offer

- Under a TIOLI offer, the equilibrium DM production x^* must be equal to the seller's expected payoff

$$x^* = \tilde{x}(\hat{z}^*, \sigma^*) \equiv [\sigma^* \theta_h^s \hat{z}^* + (1 - \sigma^*)\theta_d^s \hat{z}^*]$$

where

θ_h^s : Pr (seller receives the payment| buyer is honest)

θ_d^s : Pr (seller receives the payment| buyer double spends)

$$\begin{aligned} \theta_h^s &= p_1 \\ \theta_d^s &= p_1 r_s + p_2 r_{sb} \end{aligned}$$

Pareto optimal SPE

- We consider the Pareto optimal SPE of the sequential game
- The equilibrium strategy $\left(\hat{z}^*, \sigma^*\right)$ maximizes the buyer's expected value at the CM

$$\left(\hat{z}^*, \sigma^*\right) = \arg\max_{\hat{z}, \sigma \in B(\hat{z})} \bar{V}(\hat{z}, \sigma) \qquad \text{(IC)}$$

where

$$\bar{V}(\hat{z}, \sigma) = \left\{ \begin{array}{c} -(1+\pi)\left(\hat{z} - \tau + \delta\right) \\ +\beta\left\{u\left[\tilde{x}(\hat{z}, \sigma)\right] - k + \varphi(\hat{z}, \sigma)\right\} \end{array} \right\},$$

  - $\varphi(\hat{z}, \sigma)$ is the post-trade gain

$$\varphi(\hat{z}, \sigma) = \sigma\left[\eta_h \delta\right] + (1-\sigma)\left[\theta_d^b \hat{z} + \eta_d \delta - k\right]$$

Money Market Clearing

- CM money market clearing condition

$$\underbrace{\left\{ \begin{array}{c} \left[\sigma\theta_h^s\hat{z} + (1-\sigma)\theta_d^s\hat{z}\right] \\ + \left[\sigma\eta_h\delta + (1-\sigma)\left(\theta_d^b\hat{z} + \eta_d\delta\right)\right] \end{array} \right\}}_{\text{CM money supply}} = \underbrace{(1+\pi)(\hat{z} - \tau + \delta)}_{\text{CM money demand}} \tag{MM}$$

- The CM money supply is equal to the aggregate balance holding at the end of DM (including buyers' and sellers' balance)

Money Market Clearing

$$\underbrace{\left\{\begin{array}{c}[\sigma\theta_h^s\hat{z}+(1-\sigma)\theta_d^s\hat{z}] \\ +\left[\sigma\eta_h\delta+(1-\sigma)\left(\theta_d^b\hat{z}+\eta_d\delta\right)\right]\end{array}\right\}}_{\text{CM money supply}} = \underbrace{(1+\pi)\left(\hat{z}-\tau+\delta\right)}_{\text{CM money demand}} \tag{MM}$$

- Double spending increases the buyer's balance
  1. crowds out the seller's balance holding
  2. increases the aggregate balance ⇒ increases inflation rate or increase the transaction fee ⇒ increases the cost of trade
- Only the balance received by seller can facilitate transactions, but balance received by buyer cannot, so double spending generates inefficiency to cryptocurrency

Stationary Equilibrium

- The participation constraint (IR) for the buyer in CM:

$$\bar{V}(\hat{z}^*, \sigma^*) \geq 0 \quad \text{(IR)}$$

Definition

Given (r_s, r_b, r_{sb}), a stationary equilibrium is a mechanism $(k, \delta, p_i, q_i, \tau, \pi)$, and a strategy $(\hat{z}^*, \sigma^*)$ such that $\frac{1+\pi}{\beta} \geq 1$ and

1. Buyers and sellers are rational: (IC)
2. CM money market clears: (MM)
3. The participation constraint holds: (IR)

Optimal Mechanism

- Given the environment (r_s, r_b, r_{sb}), we solve for the optimal mechanism $(k, \delta, p_i, q_i, \tau, \pi)$ that maximizes the social welfare
- We select two candidates for the optimal mechanism: a **simple honest mechanism** and a **simple double spending mechanism**
- We show that an equilibrium is either dominated by an equilibrium generated by a simple honest mechanism or a simple double spending mechanism
- It is sufficient to solve for the optimal mechanism from the two sets of mechanisms

Simple Mechanisms

1. In a **simple honest mechanism**, we apply PoW and PoS to deter double spending
   - We set $p_2 = q_2 = 0$: payments and deposits are forfeited as off-equilibrium punishment when forks occur $\Rightarrow$ diminishes the gain from double spending
2. In a **simple double spending mechanism**, neither PoW nor PoS is imposed, so buyers will double spend
   - We set $p_2 = 0$: receivers only receive payments in single outcomes but not forks, because sellers has an advantage over buyers in single outcomes ($r_s > r_b$)

▸ mechanisms

Optimal Simple Honest Equilibrium: Pure PoW

- We maximize the social welfare subject to the participation constraint (IR)

$$\max_{x,k} \quad u(x) - x - k$$

$$\text{subject to} \quad \begin{cases} -x + \beta\left[-k + \beta u(x)\right] \geq 0 & \text{(IR)} \\ k = r_b x \end{cases}$$

- Given the trade volume x, the required size of PoW to deter double spending, k, is determined by r_b
- The welfare of PoW equilibrium is determined by r_b
- When $r_b \to 0$, the welfare approaches to efficient level

Optimal Simple Honest Equilibrium: Pure PoS

$$\max_{x,\delta} \quad u(x) - x$$

$$\text{subject to} \quad \begin{cases} -[x+\delta] + \beta[u(x)+\delta] \geq 0 \quad \text{(IR)} \\ r_{sb}\delta = r_b x \end{cases}$$

- Difference between PoS and PoW
  1. PoS does not generate a direct loss to social welfare
  2. PoS applies forks to trigger punishments
- Given the trade volume, how much PoS is needed to deter double spending is determined by $\frac{r_b}{r_{sb}}$
- Given r_b, if r_{sb} is higher, PoS has more advantage over PoW and vice versa

Optimal Simple Honest Equilibrium: PoW and PoS

$$\max_{x,k,\delta} \quad u(x) - x - k \tag{1}$$

$$\text{subject to} \quad \begin{cases} -(x+\delta) + \beta\{u(x) + \delta - k\} \geq 0 & \text{(IR')} \\ k + r_{sb}\delta = r_b x \end{cases}.$$

- We can consider both PoW and PoS into the mechanism, then the trade volume x, can be supported by PoW and PoS all together.
- There is a region in which the optimal simple honest mechanism requires both PoS and PoW

Optimal Simple Double Spending Equilibrium

$$\max_{\hat{z}} \quad u(r_s\hat{z}) - r_s\hat{z}$$

$$\text{subject to} \quad -(r_s + r_b)\hat{z} + \beta\{u(r_s\hat{z}) + r_b\hat{z}\} \geq 0 \quad \text{(IR')}$$

- When the buyer makes $\hat{z}$ unit of payment, the seller only receives $r_s\hat{z}$ units, and the buyer receives $r_b\hat{z}$ units
- The efficiency of the payment system is determined by $\frac{r_b}{r_s}$
- We compare the simple double spending equilibrium and simple honest equilibrium
  - Fixed an r_b, if r_{sb} is high, double spending can be detected more easily, so simple honest mechanism will dominate simple double spending mechanism
  - If r_{sb} is lower, then r_s must be higher, so simple double spending eq will dominate simple honest mechanism

Conclusion

- We construct a model of cryptocurrency in which the main friction is the imperfect information transmission
- The model captures the following:
  - PoW and PoS emerges endogenously to improve efficiency
  - Tradeoff between safety and the cost of trade
  - The required PoW or PoS diminishes as message sending becomes perfect
- Literature: counterfeiting of fiat money (Wallace and Nosal 2007, Rocheteau, Li, Weill 2012)
- This paper: counterfeiting of transaction messages in cryptocurrency
- Coming soon: counterfeiting of transaction accounts in digital payment systems

Simple Honest Mechanism

- Simple honest mechanism M^h :

1. $p_2(\hat{z}) = q_2(\hat{z}) = 0$: **off-equilibrium punishment.** Minimize the gain from double spending and the required size of k and δ
2. $p_1(\hat{z})$ and $q_1(\hat{z})$ are set to be indicator functions, and that is,

$$\mathbb{1}_y(\hat{z}) = \begin{cases} 1 \text{ if } \hat{z} = y \\ 0 \text{ otherwise} \end{cases}, \text{ for some } y > 0,$$

   Punish deviations. If the payment deviates y, the receiver will not receive the payment
3. (k, δ) satisfies $\theta_d^b(y)y = k + [\eta_h(y) - \eta_d(y)]\,\delta$: PoW and PoS are sufficiently high and just enough to prevent double spending fraud

Back

Simple Double Spending Mechanism

- **Simple double spending mechanism**:

1. $k = 0, \delta = 0$: the buyer must double spend
2. $p_1(\hat{z})$ is set to be indicator functions

$$\mathbb{1}_y(\hat{z}) = \begin{cases} 1 \text{ if } \hat{z} = y \\ 0 \text{ otherwise} \end{cases}, \text{ for some } y > 0,$$

3. $p_2(\hat{z}) = 0$: Eliminate payments in forks
   - **Not for off-equilibrium punishment** because forks are not off-equilibrium outcomes
   - Because $r_s > r_b$, a single outcome can be a better signal to identify the seller than a fork

Back

Optimal Simple Honest Equilibrium: PoW

$$\max_{y} \quad u(y) - y - r_b y$$

$$\text{subject to} \quad -y + \beta\left[-r_b y + \beta u(y)\right] \geq 0 \quad \text{(IR)}$$

- The welfare of PoW equilibrium is determined by r_b

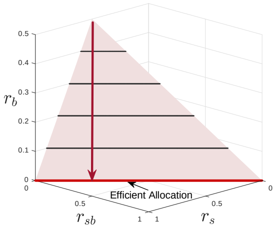


Figure:

Optimal Simple Honest Equilibrium: PoS

$$\max_{y} \quad u(y) - y$$

$$\text{subject to} \quad -\left[y + \frac{r_b}{r_{sb}} y\right] + \beta\left[u(y) + \frac{r_b}{r_{sb}} y\right] \geq 0 \quad \text{(IR)}$$

- The welfare of PoS equilibrium is determined by $\frac{r_b}{r_{sb}}$

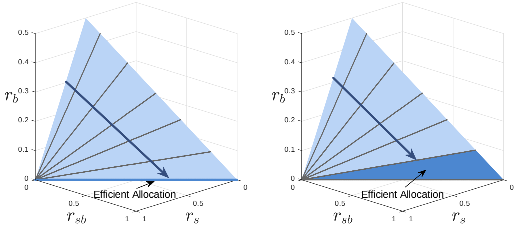


Figure:

Optimal Simple Honest Equilibrium: PoW and PoS

- Given r_b, if r_{sb} is higher, PoS has more advantage over PoW

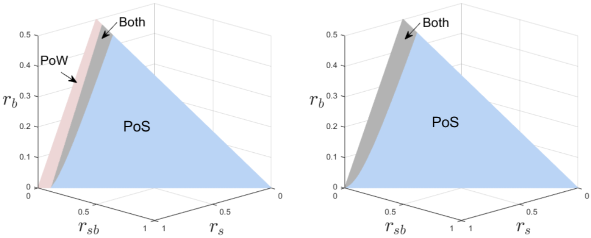


Figure:

Optimal Simple Double Spending Equilibrium

$$\max_{y} \quad u\left(r_s y\right) - r_s y$$
$$\text{subject to} \quad -(r_s + r_b)y + \beta\left\{u\left(r_s y\right) + r_b y\right\} \geq 0 \quad \text{(IR)} \quad .$$

- The ratio $\frac{r_b}{r_s}$ determines the efficiency of cryptocurrency in optimal simple double spending equilibrium

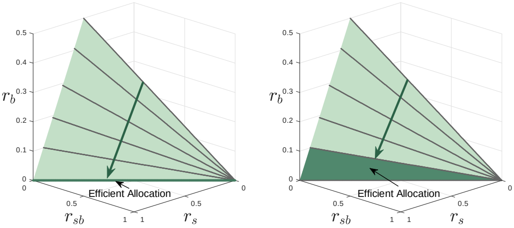


Figure:

Honest Equilibrium vs Double Spending Equilibrium

- Fixed an r_b, when r_{sb} is high, double spending can be detected easily, so simple honest mechanism of preventing the optimal simple honest equilibrium will dominate the optimal simple double spending equilibrium

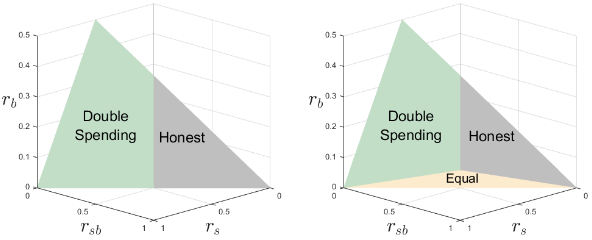
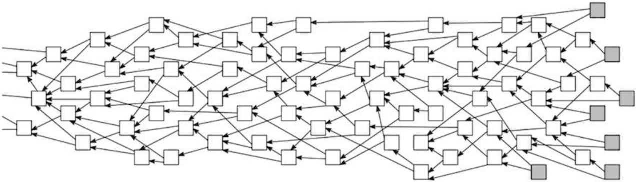


Figure:

Consensus Algorithm

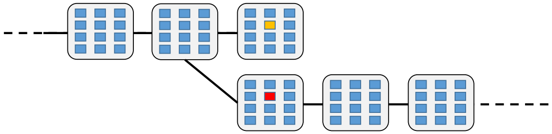
- Alternative public ledger structures:
  - Iota (DAG public ledger, No miners, traders do PoW by themselves)



Back

Double Spending

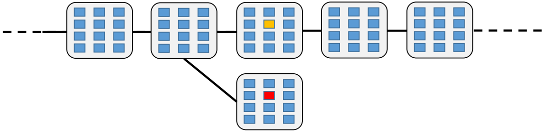
1. In Bitcoin, if the branch including the double spending becomes the longer branch, the payer takes the payment back



Back

Double Spending

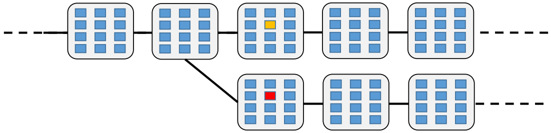
2. If the branch including the original message is the longer branch, then the payment is still received by the merchant



Back

Double Spending

3. Two branches may coexist: a fork



Back