Game Theory

and its Application to Multi-agent Systems and Blockchain Platforms

Dr. Bastian Blankenburg

Nairobi Women in Machine Learning & Data Science Meetup
Nairobi, 30. June 2018

utu

Introduction - What is Game Theory?

"Game theory is a bag of analytical tools designed to help us understand the phenomena that we observe when decision-makers interact."

- A Course in Game Theory, Osborne and Rubinstein 1994

- Introduced by von Neumann and Morgenstern in 1944 in "Theory of Games and Economic Behavior".
- For "homo economicus" (originally)
- Cooperative / non-cooperative
- John "A Beautiful Mind" Nash

Non-cooperative Game Theory

- Everybody against everybody
- Properties
  - Normal vs. extensive form games
  - Symmetric or not
  - Simultaneous vs. sequential
  - Perfect vs. imperfect information (-> Bayesian games)
  - Zero-sum or not
  - Repeated or one-time only
- Solution: Nash equilibrium with pure or mixed strategies

Applications

- Prisoner's dilemma
- Bargaining
- Auctions and other market place design
- Preventing nuclear apocalypse during the cold war
- "Should I mine for this blockchain or attack it?"

Example: Prisoner's Dilemma

		Player B	
		Talk	Silent
Player A	Talk	8 years A, 8 years B	0 years A, 10 years B
	Silent	10 years A, 0 year B	2 years A, 2 years B

Source: The legacy of John Nash and his equilibrium theory. Stephen Woodcock, 2015, The Conversation, https://phys.org/news/2015-05-legacy-john-nash-equilibrium-theory.html

Example: Prisoner’s Dilemma

		Player B	
		Talk	Silent
Player A	Talk	8 years A, 8 years B	0 years A, 10 years B
	Silent	10 years A, 0 year B	2 years A, 2 years B

Example: Prisoner's Dilemma

		Player B	
		Talk	Silent
Player A	Talk	8 years A, 8 years B	0 years A, 10 years B
	Silent	10 years A, 0 year B	2 years A, 2 years B

Example: Prisoner's Dilemma

		Player B	
		Talk	Silent
Player A	Talk	8 years A, 8 years B	0 years A, 10 years B
	Silent	10 years A, 0 year B	2 years A, 2 years B

Equilibrium ≠ globally best solution!

Repeated Prisoner's Dilemma

What happens if we play the game repeatedly?

		Player B	
		Talk	Silent
Player A	Talk	8 years A, 8 years B	0 years A, 10 years B
	Silent	10 years A, 0 year B	2 years A, 2 years B

Similar: Drug Gang Game

		Colombian gang	
		Exchange	Open Fire
American gang	Exchange	Get money Get drugs	Get money and drugs Shot dead
	Open fire	Shot dead Get money and drugs	Retire injured Retire injured

Game Theory in Christian Perspective. Cooper, 2015, https://www.gordon.edu/ace/pdf/2015%20Spring%20-%20Cooper.pdf

"Homo economicus" assumption doesn't apply to everybody or at all times.

Exercise: Auction Design

Auctions:

- Auctioneer
- Item i to auction
- Bidders B
  - Valuation v(i)
  - Want to pay price $p <= v(I)$
  - Bidder $j \in B$ wins iff $p_j > p_k$ $\forall k \in B, j \neq k$
- How to design an auction protocol so that each bidder should bid it's true value?

Exercise: Auction Design

Auctions:

- Auctioneer
- Item i to auction
- Bidders B
  - Valuation v(i)
  - Want to pay price p <= v(I)
  - Bidder $j \in B$ wins iff $p_j > p_k \ \forall k \in B, j \neq k$
- How to design an auction protocol so that each bidder should bid it's true value?

- Example: English auction:
  - Sequential perfect information game
  - High communication complexity

Cooperative Game Theory

- Binding contracts possible, so agents can cooperate and form “coalitions”.
- Also: coalition games
- Characteristic function form:
  - game (A, v),
  - characteristic function v: $2^A \rightarrow \mathscr{R}$

coalitions C	v(C)
{a1}, {a2}, {a3}	0
{a1, a2}, {a1, a3}, {a2, a3}	10
{a1, a2, a3}	12

Cooperative Game Theory

- Binding contracts possible, so agents can cooperate and form "coalitions".
- Also: coalition games
- Characteristic function form:
  - game (A, v),
  - characteristic function v: $2^A \rightarrow \mathcal{R}$
- Properties:
  - symmetric: all agents equal
  - superadditive: joining 2 disjoint coalitions always profitable
  - convex: joining any coalitions even more profitable

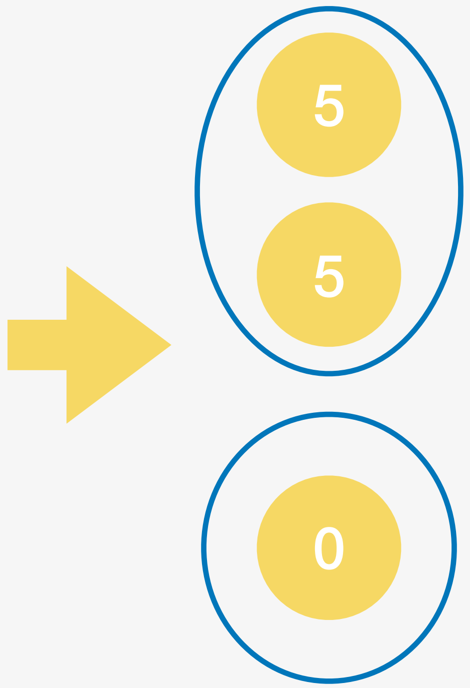
coalitions C	v(C)
{a1}, {a2}, {a3}	0
{a1, a2}, {a1, a3}, {a2, a3}	10
{a1, a2, a3}	12

symmetric, superadditive, not convex

Solution Concepts for Cooperative Games

- Configuration (S, u) of
  - coalition structure S and
  - payoff distribution u.

coalitions C	v(C)
{a1}, {a2}, {a3}	0
{a1, a2}, {a1, a3}, {a2, a3}	10
{a1, a2, a3}	12



Solution Concepts for Cooperative Games

- Configuration (S, u) of
  - coalition structure S and
  - payoff distribution u.
- Some solution concepts:
  - Core: no sub-coalition better off by breaking away.
  - Kernel: balance of arguments "I can obtain more in alternative coalitions without you, than you without me."
  - Shapley Value: "My share of the profit is proportional to the value that I can contribute to the coalition."

coalitions C	v(C)	Kernel, σ
{a1}, {a2}, {a3}	0	each 0
{a1, a2}, {a1, a3}, {a2, a3}	10	each 5
{a1, a2, a3}	12	each 4

$$\sigma(a, v) = \sum_{C \subseteq \mathcal{A}} \frac{(|\mathcal{A}| - |C|)!(|C| - 1)!}{|\mathcal{A}|!}(v(C) - v(C \setminus \{a\}))$$

Cooperative Game Applications

- Applications:
  - Political coalition formation
  - Airport landing fees
  - Sharing costs of public goods (e.g. powerplant)
  - Joint ventures
  - Resource allocation (e.g. sensor networks, power lines)
  - Talmud and Old Testament

Cooperative Game Example

From “Some non-superadditive games, and their Shapley values, in the Talmud”, Aumann, 2010, International Journal of Game Theory 39:3-10:

Ibn Ezra (1146): A man with four sons dies, leaving an estate worth 120 units of money. According to his will,

- 120 go to his eldest son,
- 60 (half the estate) go to the second,
- 40 (a third) go to the third,
- and 30 (a quarter) goto the last.

Cooperative Game Example

From "Some non-superadditive games, and their Shapley values, in the Talmud", Aumann, 2010, International Journal of Game Theory 39:3-10:

Ibn Ezra (1146): A man with four sons dies, leaving an estate worth 120 units of money. According to his will,

- 120 go to his eldest son,
- 60 (half the estate) go to the second,
- 40 (a third) go to the third,
- and 30 (a quarter) goto the last.

Solution according to Ezra:

1. 30 are claimed by all, so split equally between them.
2. The next 10 are claimed by the 3 elders, split equally between them.
3. The next 20 are claimed by the 2 oldest sons, split equally between them.
4. The last 60 are claimed only by the oldest son so he gets it all.

Cooperative Game Example

From "Some non-superadditive games, and their Shapley values, in the Talmud", Aumann, 2010, International Journal of Game Theory 39:3-10:

Ibn Ezra (1146): A man with four sons dies, leaving an estate worth 120 units of money. According to his will,

- 120 go to his eldest son,
- 60 (half the estate) go to the second,
- 40 (a third) go to the third,
- and 30 (a quarter) goto the last.

Solution according to Ezra:

1. 30 are claimed by all, so split equally between them.
2. The next 10 are claimed by the 3 elders, split equally between them.
3. The next 20 are claimed by the 2 oldest sons, split equally between them.
4. The last 60 are claimed only by the oldest son so he gets it all.

Resulting payoffs:

- $60+10+3\frac{1}{3}+7\frac{1}{2}= 80\frac{5}{6}$ for the oldest,
- $10+3\frac{1}{3} +7\frac{1}{2} = 20\frac{5}{6}$ for the second,
- $3\frac{1}{3} +7\frac{1}{2} = 10\frac{5}{6}$ for the third,
- $7\frac{1}{2}$ for the fourth.

Cooperative Game Example

From “Some non-superadditive games, and their Shapley values, in the Talmud”, Aumann, 2010, International Journal of Game Theory 39:3-10:

Ibn Ezra (1146): A man with four sons dies, leaving an estate worth 120 units of money. According to his will,

- 120 go to his eldest son,
- 60 (half the estate) go to the second,
- 40 (a third) go to the third,
- and 30 (a quarter) goto the last.

Cooperative game solution:

1. Define cooperative game:

$$v_1(S) := \min\left(\sum_{i \in S} c_i, e\right);$$

Cooperative Game Example

From "Some non-superadditive games, and their Shapley values, in the Talmud", Aumann, 2010, International Journal of Game Theory 39:3-10:

Ibn Ezra (1146): A man with four sons dies, leaving an estate worth 120 units of money. According to his will,

- 120 go to his eldest son,
- 60 (half the estate) go to the second,
- 40 (a third) go to the third,
- and 30 (a quarter) goto the last.

Cooperative game solution:

1. Define cooperative game:

$$v_1(S) := \min\left(\sum_{i \in S} c_i, e\right);$$

2. Apply Shapley value:

$$\sigma(a, v) = \sum_{C \subseteq \mathcal{A}} \frac{(|\mathcal{A}| - |C|)!(|C| - 1)!}{|\mathcal{A}|!}(v(C) - v(C \setminus \{a\}))$$

Cooperative Game Example

From “Some non-superadditive games, and their Shapley values, in the Talmud”, Aumann, 2010, International Journal of Game Theory 39:3-10:

Ibn Ezra (1146): A man with four sons dies, leaving an estate worth 120 units of money. According to his will,

- 120 go to his eldest son,
- 60 (half the estate) go to the second,
- 40 (a third) go to the third,
- and 30 (a quarter) goto the last.

Cooperative game solution:

1. Define cooperative game:

$$v_1(S) := \min\left(\sum_{i \in S} c_i, e\right);$$

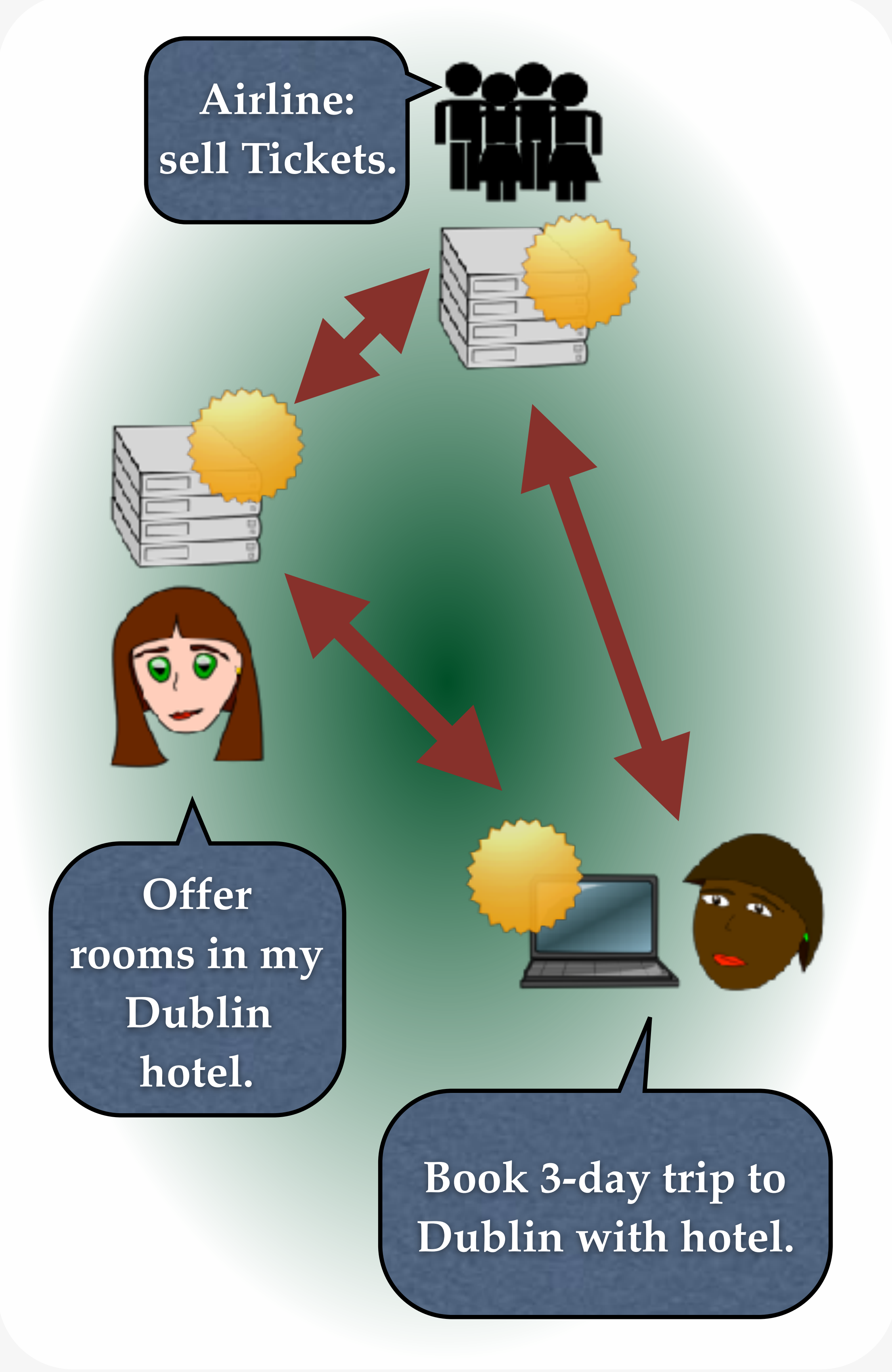
2. Apply Shapley value:

$$\sigma(a, v) = \sum_{C \subseteq \mathcal{A}} \frac{(|\mathcal{A}| - |C|)!(|C| - 1)!}{|\mathcal{A}|!}(v(C) - v(C \setminus \{a\}))$$

Same payoffs! 80⅚, 20⅚, 10⅚, 7½

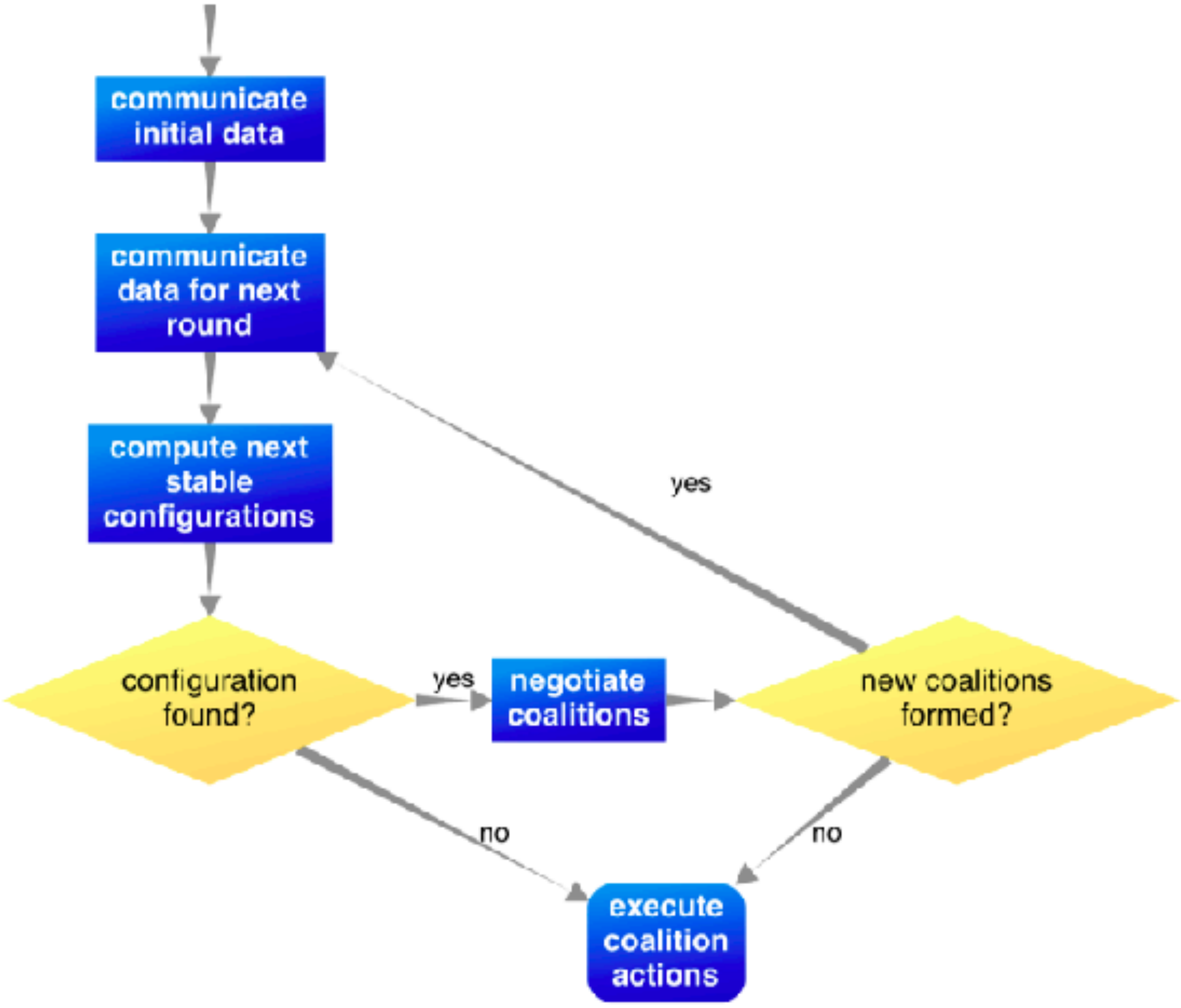
Game Theory in Computer Science (1)

- Generally applicable in multi-agent systems
  - Independent autonomous self-interested agents interacting.
  - Agents are typically assumed to be AIs but can include humans.
- Algorithmic Game Theory
  - Analysis: applying game theory to analyse properties and expected behaviour of agents in multi-agent systems.
  - Design: "(Automated) Mechanism Design", i.e. how to design multi-agent systems such that expected behaviour of (rational) agents is desirable: incentive compatible.
  - Engineering: devising protocols and algorithms that correctly and efficiently implement abstract designs.



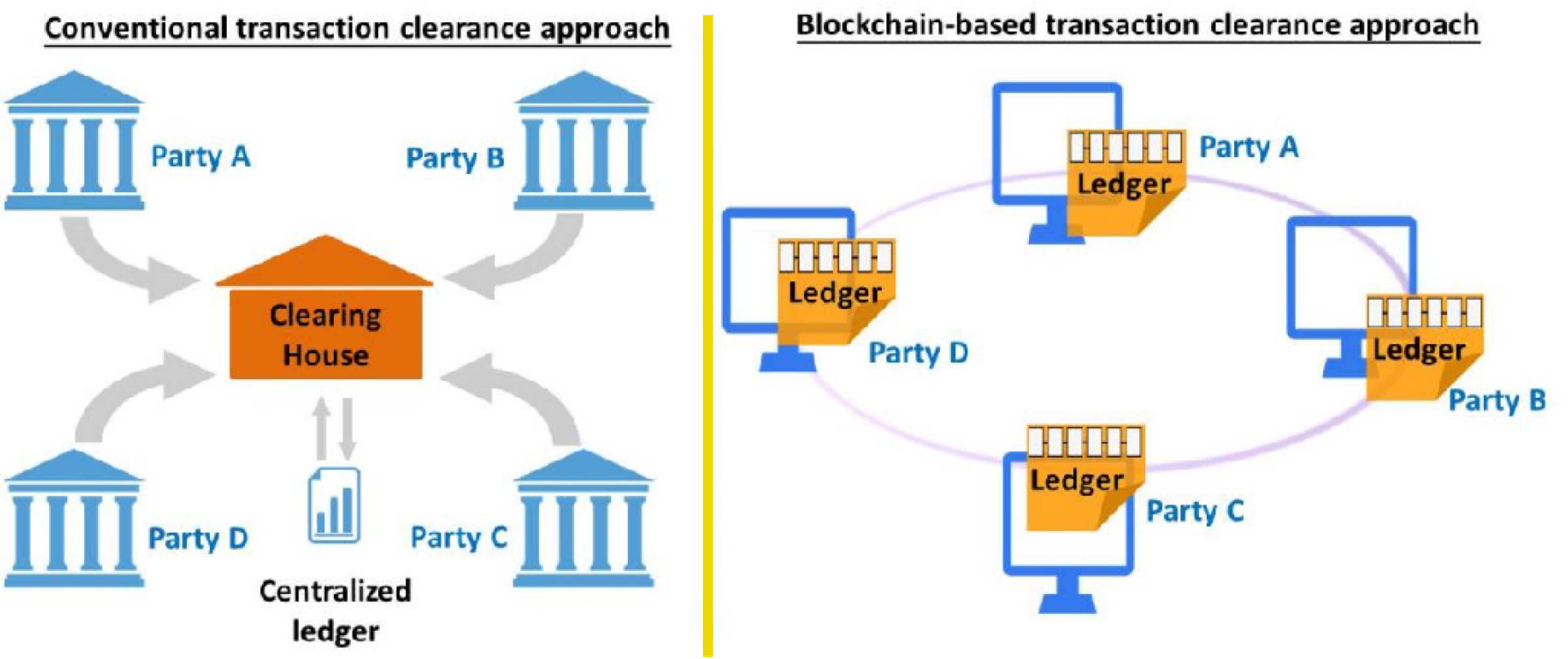
Game Theory in Computer Science (2)

- Extensions / refinements:
  - Reducing computational and communication complexity
    - Compact form games
    - Limits
  - Uncertainty:
    - Bayesian games,
    - reinforcement learning,
    - trust models,
    - possibility theory,
    - financial risk measures
  - Privacy preservation



What is Blockchain?

- Ledger: history of transactions.
- Examples: Bank account, land registry, Facebook, any classical database



Copied from Blockchain technology. Legislative Council of the Hong Kong Special Administrative Region, 2015, http://www.legco.gov.hk/research-publications/english/essentials-1516ise15-blockchain-technology.htm, original source given: Oliver Wyman (2015)

How is Blockchain Secure?

- In “Proof of Work”, “Miners” create blocks.
  (Some alternatives: Proof of Stake, Hashgraph)

- The process of “mining” involves solving some difficult cryptographic puzzle.

  - This introduces a time delay.

  - Therefore the latest blocks have time to be distributed in the network before newer blocks are added.

- Consensus: the longest chain wins.

- Anyone can mine (but ASICs)

- Anyone can create themselves multiple addresses anonymously.

- So why would a miner not

  - create invalid transactions to award themselves some cash?
    A: cryptographically signed transactions, proof, no miner mines on top invalid block.

  - create blocks chained to an older block to double spend?

Double Spending

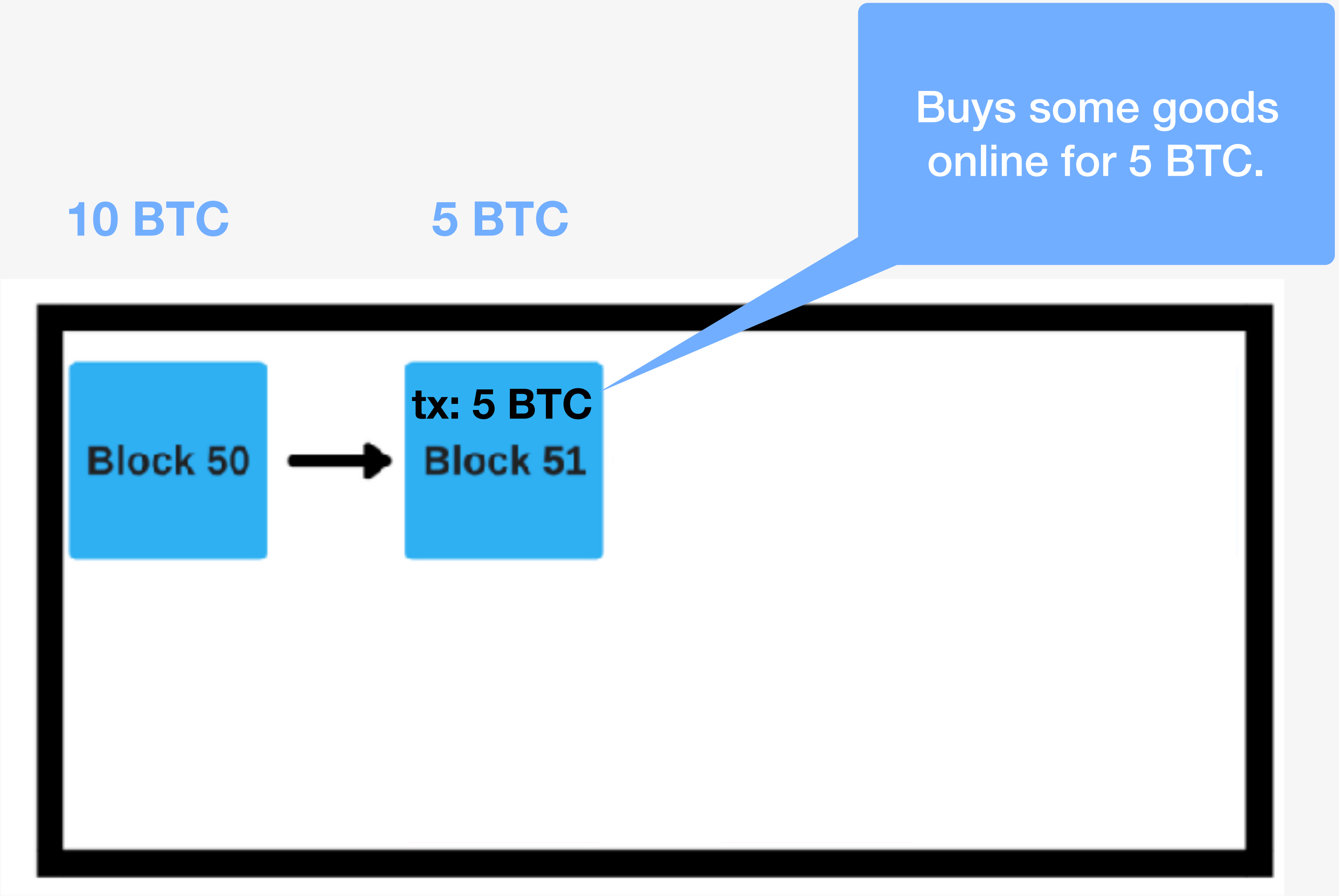
Malicious miner:

Legitimate balance: 10 BTC

Double Spending

Malicious miner:

Legitimate balance: 10 BTC 5 BTC

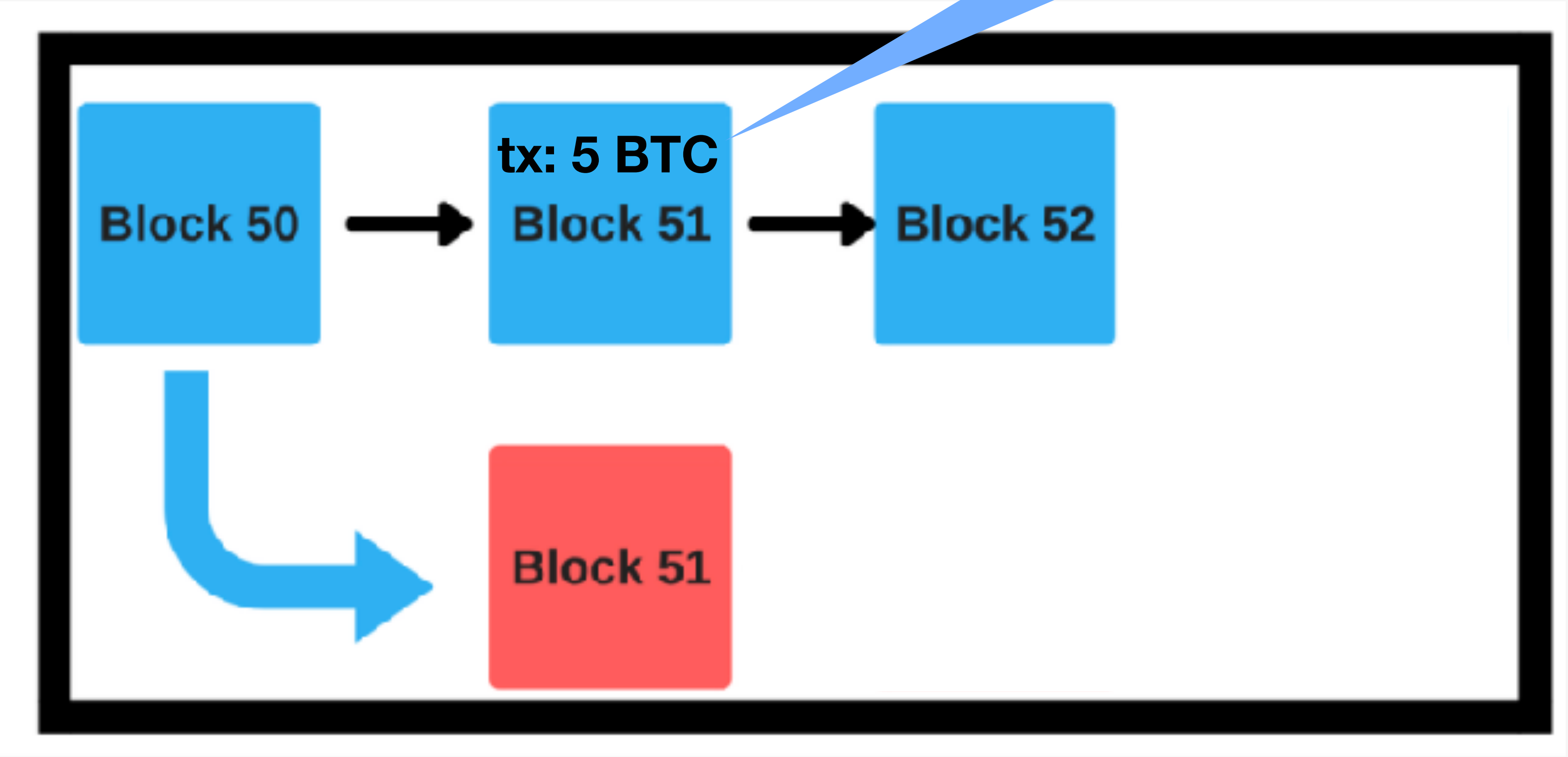


Double Spending

Malicious miner:

Legitimate balance: 10 BTC 5 BTC

Buys some goods online for 5 BTC.



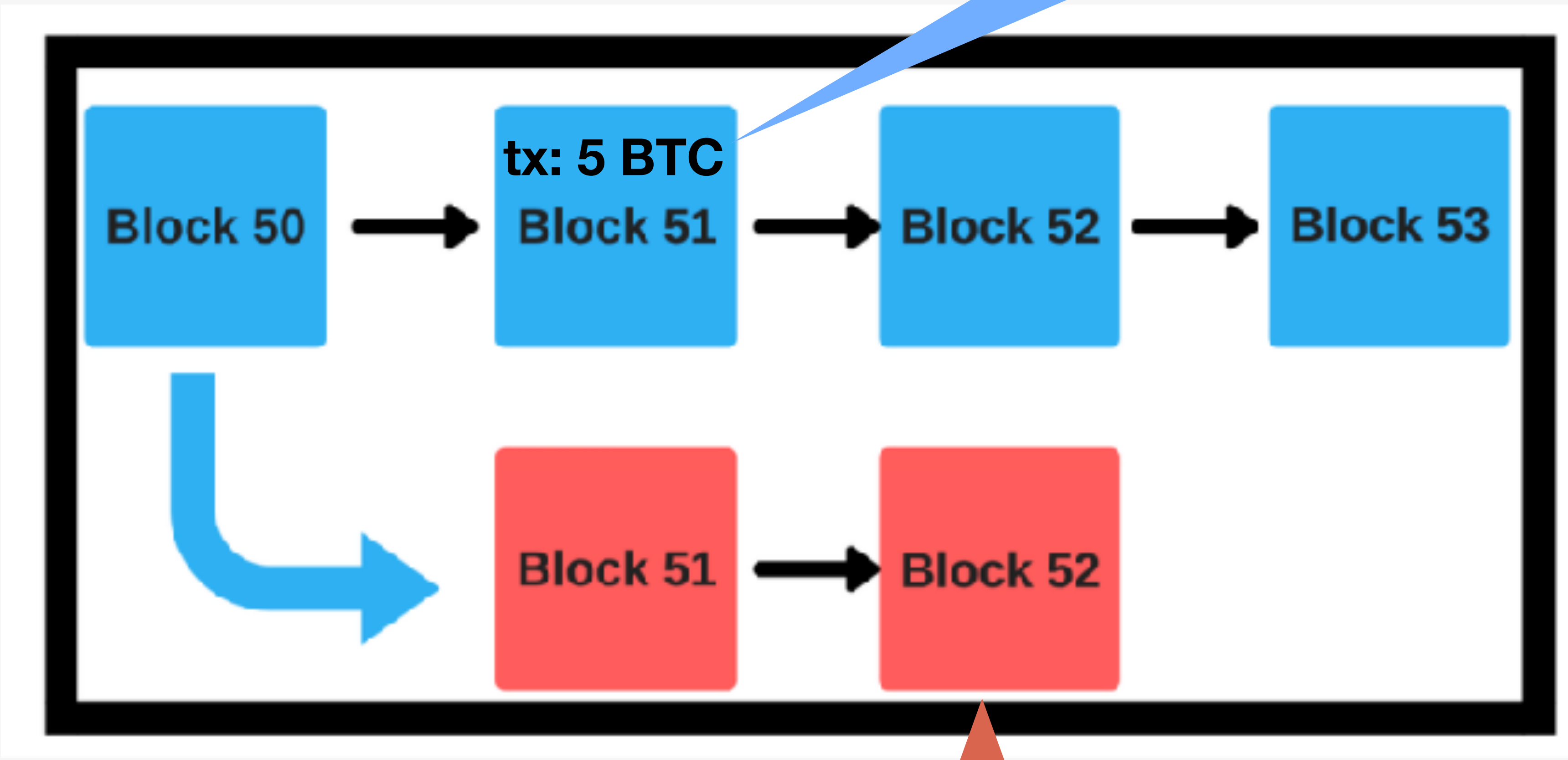
Cheated balance: 10 BTC

Double Spending

Malicious miner:

Legitimate balance: 10 BTC 5 BTC

Buys some goods online for 5 BTC.



Cheated balance: 10 BTC

Cheated chain needs to grow longest to be accepted.

Needs at least **51%** "hash rate".

The 51% Attack

- Nakamoto's original argument: unlikely that a miner (or coalition) reaches >= 51% hash rate.
- But:
  - Bitmain almost there for Bitcoin.
  - Recently a number of 51% attacks happened on smaller chains (e.g. Bitcoin Gold).
  - Vitalik Buterin's recipe for takeover: create a smart contract for a coordinated activity such that:
    - Any miner can join by sending a very large deposit to the contract.
    - Miners send shares of their partially completed blocks to the contract; the contract verifies this and also that you are a miner with sufficient hash power.
    - Before 60% of all miners join, one can leave at anytime.
    - After 60% of all miners join, you will be bound to the contract until the 20 blocks have been added to cheating chain.

The Case Against the 51% Attack

Game-theory:

- “Grim Trigger” Equilibrium: Down with the King! - not.
- Once you killed the 1st king, there’s no reason to not also kill all subsequent kings!
- Once a chain was 51%-attacked, there’s no reason to not do it again for miners in general. However:
    - This only holds if miners have vested interest in keeping the blockchain working in the long term, and not completely destroy its ecosystem.
    - Other chains for which miners don’t care so much can be exploited, then miners move on.
    - The attacks on Bitcoin Gold and other small chains, but not Bitcoin or other big chains seem to confirm this.

The Case Against the 51% Attack

Game-theory:

- "Grim Trigger" Equilibrium: Down with the King! - not.
- Once you killed the 1st king, there's no reason to not also kill all subsequent kings!
- Once a chain was 51%-attacked, there's no reason to not do it again for miners in general. However:
  - This only holds if miners have vested interest in keeping the blockchain working in the long term, and not completely destroy its ecosystem.
  - Other chains for which miners don't care so much can be exploited, then miners move on.
  - The attacks on Bitcoin Gold and other small chains, but not Bitcoin or other big chains seem to confirm this.

Similar considerations have to be made for any blockchain functionality because of the decentralised nature!

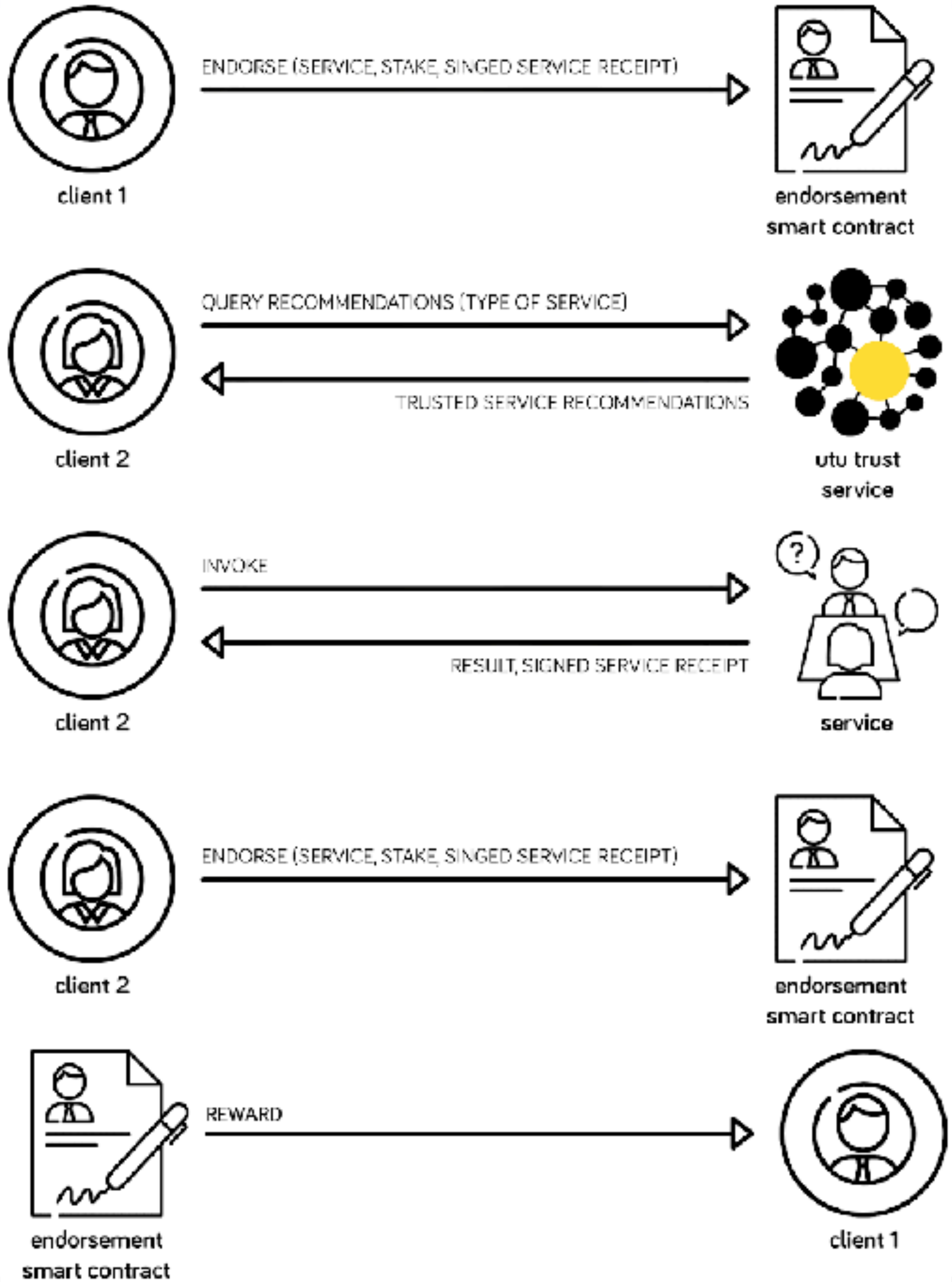
Smart Contracts

- A smart contract
  - is a program that is run as transactions on the chain,
  - has to be “mined” to made available in the chain, which includes assigning it an address,
  - provides functions which are invoked in transactions,
  - has a proper on-chain address, i.e. can hold and transfer coins,
  - is publicly verifiable (because on-chain), and
  - typically costs a transaction fee to execute (“gas”).
- Ethereum most popular smart contract platform (so far).
- Enable coalition formation (cooperative game theory) without requiring an enforcing third party.

Smart Contract Example

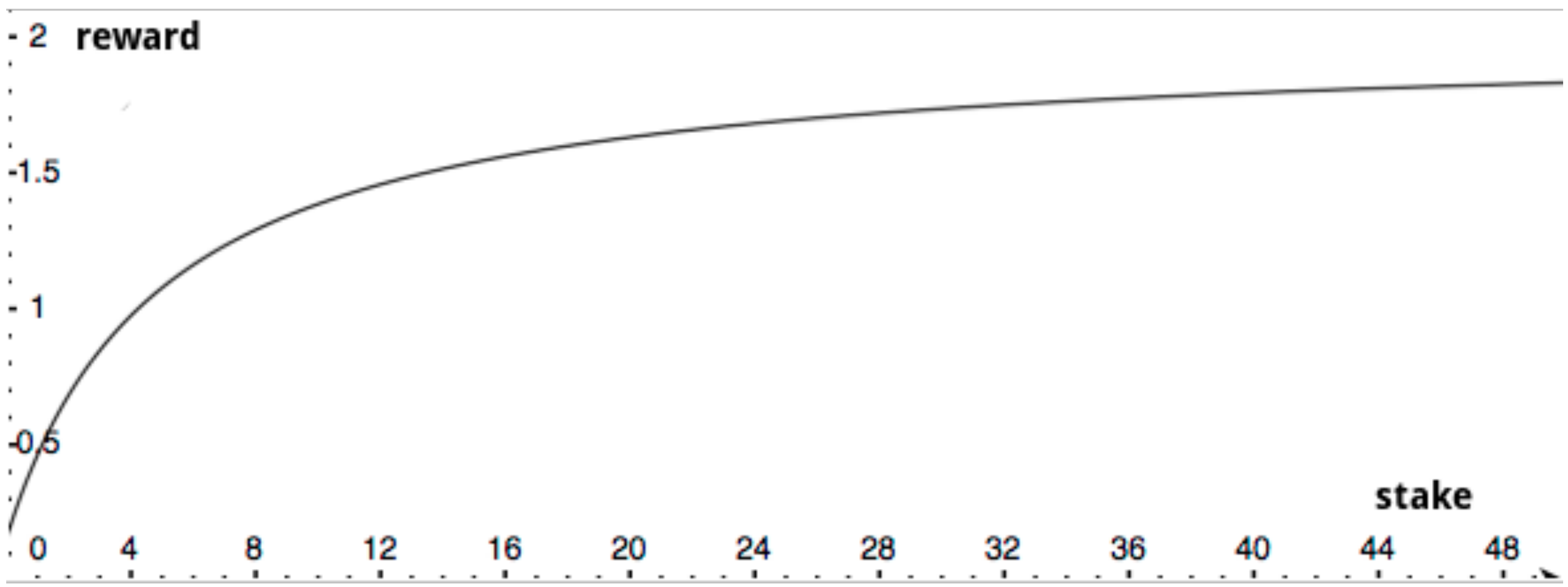
```
contract Purchase {
    uint public value;
    address public seller;
    address public buyer;
    enum State { Created, Locked, Inactive }
    State public state;

    // Ensure that `msg.value` is an even number. Division will truncate if it is an odd
    // number. Check via multiplication that it wasn't an odd number.
    constructor() public payable {
        seller = msg.sender;
        value = msg.value / 2;
        require((2 * value) == msg.value, "Value has to be even.");
    }

    modifier inState(State _state) {
        require(
            state == _state,
            "Invalid state."
        );
        _;
    }

   event PurchaseConfirmed();

    /// Confirm the purchase as buyer. Transaction has to include `2 * value` ether.
    /// The ether will be locked until confirmReceived is called.
    function confirmPurchase()
        public
        inState(State.Created)
        condition(msg.value == (2 * value))
        payable
    {
        emit PurchaseConfirmed();
        buyer = msg.sender;
        state = State.Locked;
    }
…
```

UTU's Service Endorsements



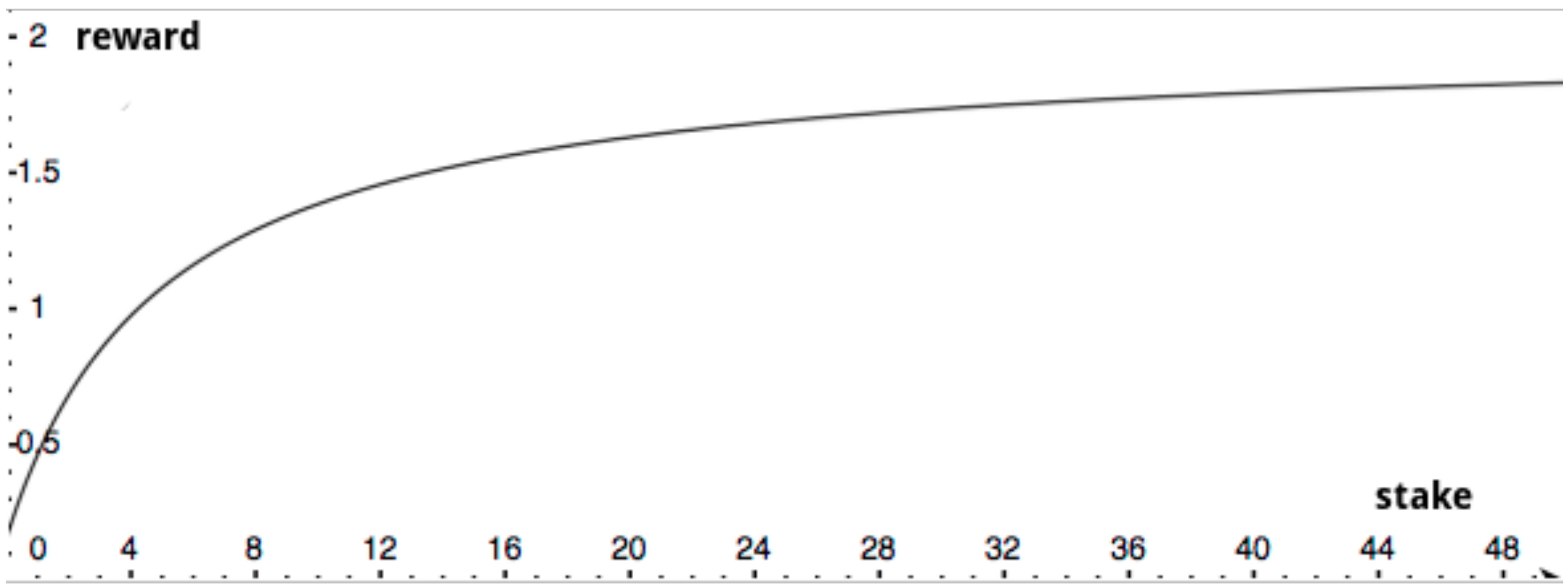
UTU's Service Endorsements - Reward

$$reward := R_{max} \cdot \frac{s_n + D_p s_p}{s_{total}}$$



UTU's Service Endorsements - Reward

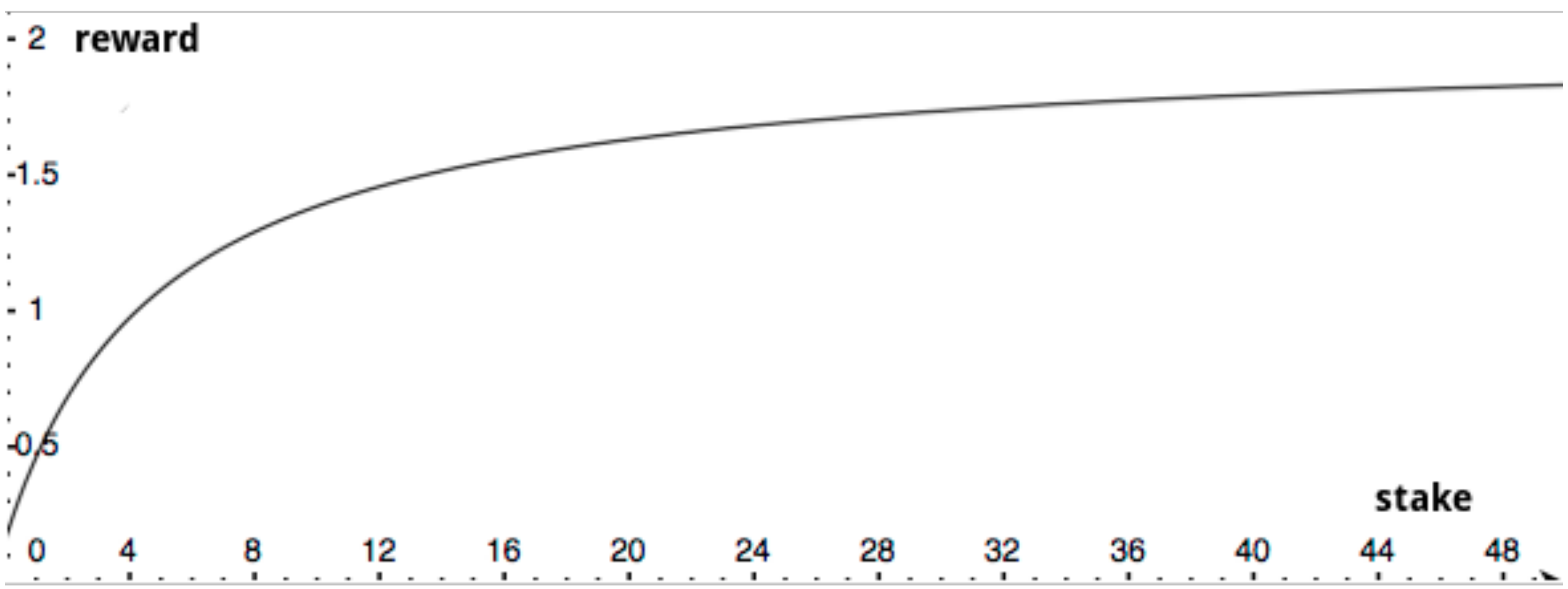
$$reward := R_{max} \cdot \frac{s_n + D_p s_p}{s_{total}}$$



What might be the problem here?

UTU's Service Endorsements - Reward

$$reward := R_{max} \cdot \frac{s_n + D_p s_p}{s_{total}}$$



What might be the problem here?

Sybil attack possible!

Thank you!

utu

Resources for Further Reading

- A Course in Game Theory. Osborne and Rubinstein, 1994, The MIT Press
- Game theory and multi-agent systems:
  - Computational Aspects of Cooperative Game Theory. Chalkiadakis, Elkind and Wooldridge, 2011, Morgan & Claypool Publishers
  - Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations. Shoham and Leyton-Brown, 2008, Cambridge University Press
  - Multiagent Systems (Intelligent Robotics and Autonomous Agents), 2nd edition. Weiss (ed.), 2016, The MIT Press
- Game theory and religion:
  - Some non-superadditive games, and their Shapley values, in the Talmud. Aumann, 2010, International Journal of Game Theory 39:3-10
  - Game Theory in Christian Perspective. Cooper, 2015, https://www.gordon.edu/ace/pdf/2015%20Spring%20-%20Cooper.pdf
- Blockchains:
  - How does blockchain really work? I built an app to show you. https://medium.freecodecamp.org/how-does-blockchain-really-work-i-built-an-app-to-show-you-6b70cd4caf7d
  - Bitcoin: A Peer-to-Peer Electronic Cash System. Nakamoto, https://bitcoin.org/bitcoin.pdf
  - Developing æpps for the æternity blockchain. https://dev.aepps.com
  - What is Cryptocurrency Game Theory: A Basic introduction, https://blockgeeks.com/guides/cryptocurrency-game-theory