IS4302
Blockchain and Distributed Ledger Technology

Lecture 11

31 Mar, 2023

NUS
National University of Singapore

Overview

- **Blockchain and game theory**
  - Basics
  - Application

- **Key takeaways from the module**

Game theory

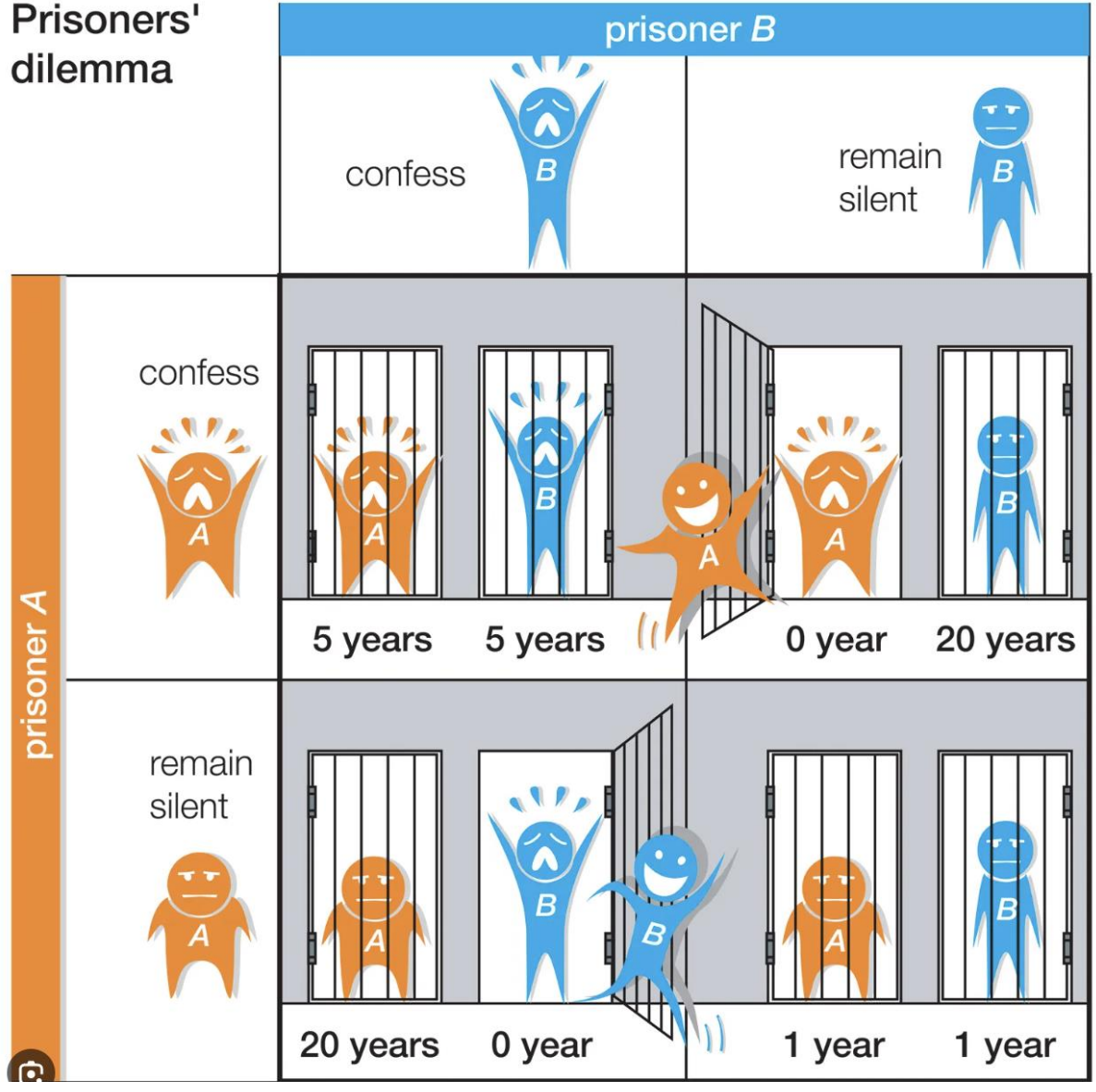
- **Game theory is the study of mathematical models of strategic interactions among rational agents.**
- **Rational: utility/outcome maximization**
- **Bounded rationality: limited information, behavioral aspects, etc.**

Nash equilibrium

- **If each player has chosen a strategy**
  - an action plan based on what has happened so far in the game

- **and no one can increase one's own expected payoff by changing one's strategy while the other players keep theirs unchanged, then the current set of strategy choices constitutes a Nash equilibrium.**

Prisoner's dilemma



Prisoner's dilemma

	confess	remain silent
confess	-5, -5	0, -20
remain silent	0, -20	-1, -1

- **Unique Nash equilibrium: both confess**
- **What if they have other consequences from confessing?**

Multiple equilibria

- **There could be cases where there exist multiple equilibria.**
- **E.g., every car goes on the left is an equilibrium, every car goes on the right is another equilibrium**
- **E.g., battle of sexes**

		WOMAN: Boxing	WOMAN: Shopping
MAN	Boxing	2 , 1	0 , 0
	Shopping	0 , 0	1 , 2

Multiple equilibria

- **What will be the outcome when there are multiple equilibria?**
  - Communication
  - Negotiation
  - Culture
  - …

Game theory and mining

- **Consensus algorithms**
- **In PoW, what is/are the miners' equilibrium(a)?**
- **Lazy mining**
- **Selfish mining**
- **Filling partial blocks**
- **…**

Game theory and decentralized oracles

- **Reminded in ASTREA, there are two sets of participants: voters and certifiers.**
- **When the voters and certifiers' voting results agree with each other, both will be awarded. Otherwise, the voters will break even and the certifiers will be penalized.**
- **How will they vote?**
- **Formal game theoretic analysis is needed there.**

Overview

- **Blockchain and game theory**
  - Basics
  - Application

- **Key takeaways from the module**

What is blockchain?

- **A ledger writing technology, that can records many things, including codes (smart contracts).**
- **Immutability : helps building trust and reputation**
- **Transparency: again, helps building trust and reputation**
- **Decentralization: not a 0,1 thing, has goods and bads, needs to be designed carefully**

Solidity programming

- **Smart contracts**
- **Deployments/transactions**
- **Standards, specifically ERC-20 and ERC-721 for tokens.**
- **Common patterns**
- **Solidity language and environments**

Tokenomics

- **Why tokens have value?**
- **How should they be valued?**
- **Just as other commodities, the value/price depends on supply and demand.**
- **Supply: coin offerings, limited supply, etc.**
- **Demand: real demand, speculative demand**

Oracle problem

- **How to communication off-chain information to the blockchains?**
- **In many case, the desirable features of blockchains cannot be maintained in this process.**
- **Successful applications usually have reasonable solutions to this problem.**
- **Development of decentralized oracles**

DAOs

- **Some are successful, some are not.**
- **Off-chain interactions are critical.**
- **Lack of accountability is a main reason for the failure of many decentralized systems.**
- **The systems need to be carefully designed.**

Regulations and self-regulations

- **Transparency of blockchain does not mean transparency of everything.**
- **Financial frauds are common in the blockchain ecosystem, which is ironic.**
- **Regulations or self-regulations are heavily needed.**

My comments on the ecosystem

- **Not healthy yet.**
- **Needs productive apps.**
- **Needs infrastructure to support productive apps.**
  - Cloud service
  - Oracles
  - …
- **Blockchain is just a framework, the details need to be carefully designed, which is not all there yet.**
- **Be practical, not idealistic or even ideological.**

Thank you!