

TOP-
SC/Schelling

Ivan Sendin

News

Teoria dos Jogos

Schelling

Schelling Coin

Kleros

Use case

Funcionamento

Futuro

$P + c$

Smart Contracts Schelling Coin

Ivan Sendin

FACOM - Universidade Federal de Uberlândia
ivansendin@yahoo.com, sendin@ufu.br

3 de outubro de 2024

- Cinco frases clássicas escritas por Satoshi Nakamoto
- Deep Web: O Lado Sombrio das Criptomoedas
- Sobre cotação e moedas fiat/lastreadas: reserva em Dolares da China (Google)
- Sobre aplicações de SC: Uber e StopClub
Aqui e aqui

- Teoria dos Jogos
- Pessoas racionais
Não necessariamente morais!
- Maximizar o lucro
diferente de correto, de justo,...
- Prisioneiros...
- A Blockchain é baseada em TJ!!
E funciona!??

Prisioneiros...

TOP-
SC/Schelling

Ivan Sendin

News

Teoria dos Jogos

Schelling

Schelling Coin

Kleros













Use case

Funcionamento

Futuro

$P + \epsilon$

- O Dilema dos Prisioneiros
- Albert Tucker/RAND Corporation
- Dois individuos são detidos
- e estão sendo interrogados (em salas separadas)
- Cada um deles é informado que existem provas para uma condenação por um crime “menor”
1 ano de condenação
- É feita a seguinte proposta:
“Se voce testemunhar contra o seu cúmplice, voce sai livre e ele pega 3 anos”
- Tem uma pegadinha...
Ambos podem ficar 2 anos presos...

A \ B	B B stays silent 	B testifies 
A stays silent 	  R=1 R=1	  S=3 T=0
	  T=0 S=3	  P=2 P=2
A testifies 		

Prisioneiros...

TOP-
SC/Schelling

Ivan Sendin

News

Teoria dos Jogos

Schelling

Schelling Coin

Kleros

Use case

Funcionamento

Futuro

$P + \epsilon$

- Pessoais racionais com um função de minimização simples
- A estratégia ótima é a delação
- Equilibrio de Nash
- (nem sempre ocorre)

- Thomas Schelling
- Coordenar o comportamento sem comunicação
- Ponto de Schelling ou Ponto Focal
- Exemplo: “Duas pessoas precisam se encontrar em Nova Iorque amanhã”
- Que horas?? Onde??
- (E em Uberlândia?!?)

- SchellingCoin: A Minimal-Trust Universal Data Feed - Vitalik Buterin
- Decentralized data feed - Oráculo
- Cotações, opiniões, resultados, computação,....
- As pessoas(jurados) votam nos resultados
- O resultado vencedor é tido como **verdade!**

Tabela de beneficios do jurados:

Resultado / Voto	Sim	Nao
Sim	P	0
Não	0	P

P é o pagamento pela “correta” escolha feita pelo jurado.

- A idéia é que uma opinião tecnica de diversos tecnicos deve “converger” para a verdade conforme o numero de tecnicos aumente
- A remuneração deve incetivar o jurado e fazer a escolha tecnica correta

- Kleros
- “Quem controla as cortes...controla o Estado” - Aristóteles
- “decision protocol for a multipurpose court system able to solve every kind of dispute”
- Honestidade X Teoria dos Jogos
- “...based on a fundamental insight from legal epistemology: a court is an epistemic engine, a tool for ferreting out the truth about events from a confusing array of clues. “

- Alice contrata Bob para desenvolver um website
- Países diferentes, Bob pode ser um endereço Ethereum
- Como resolver disputas??
- Alice faz o pagamento previo para o contrato
- O Bob deve deixar uma caução no contrato

- O contrato pode ter uma função `desisti`, chamada por Bob que devolve os valores
- O contrato pode ter uma função `servicoFeito` que faz o pagamento para o Bob e devolve a caução
- O contrato pode ter uma função `parcial` que define um “meio termo”
Recebo metade..OK?
- O contrato pode....inúmeras soluções de acordo.

- Não havendo acordo...
- O contrato tem um “botão disputa” que transfere a decisão para o Kleros
- (Junto com uma documentação)

- A disputa vai para o sistema do Kleros
dinheiro fica sob controle do Kleros
Kleros é um contrato
- Cada jurado endossa 2000 PNK
Token proprio
- Os jurados decidem com base na documentação
- O pagamento é feito
Uma parte fica com Kleros
ruim para os dois participantes..certo?
- Os jurados são remunerados

- O uso do token (deve) impede o *sybil attack*
- Quem “erra” no voto perde parte(?) dos Tokens
- Quem acerta ganha
- $\text{Voto} = \text{hash}(\text{vote}, \text{salt}, \text{address})$
- Fase de revelar (com punição)

- As taxas são pagas pelo contrato cliente Configurável!
- Possível fazer apelação
- Numero de jurados crescendo exponencialmente $3, 7, 15, \dots (2n+1)$
- Custo também cresce...

- *Bribe resistance*
Será?

Futuro

TOP-
SC/Schelling

Ivan Sendin

News

Teoria dos Jogos

Schelling

Schelling Coin

Kleros

Use case

Funcionamento

Futuro

$P + \epsilon$

- Privacy of Contracts
- Improved Random Number Generation
Hj é o blockchash
- Penalizing Jurors Who Reveal Their Vote Too Early

- Nem tudo são flores...
- Ataque do $P + \epsilon$
- Alguem oferece um ganho **garantido** de $P + \epsilon$ para quem votar no **Sim**

Resultado / Voto	Sim	Nao
Sim	$P + \epsilon$	0
Não	$P + \epsilon$	P

Um participante racional, visando o lucro vota em **Sim**.

- Um participante racional, visando o lucro vota em **Sim**.
- O valor do ϵ pode ser muito pequeno!
- Quanto será gasto em suborno??
- Refs: artigo, Blog Vitalik, Artigo 2
- Depois: implementação do SC
A rigor vc nao confia em quem paga suborno

<https://www.cs.cmu.edu/~arielpro/15896/docs/paper11a.pdf> Condorcet Theory of Voting HP Young
<https://dl.acm.org/doi/10.1145/3488932.3497758>
<https://arxiv.org/pdf/1911.08774.pdf>
<https://orbi.uliege.be/bitstream/2268/232444/1/PID5765419.pdf>