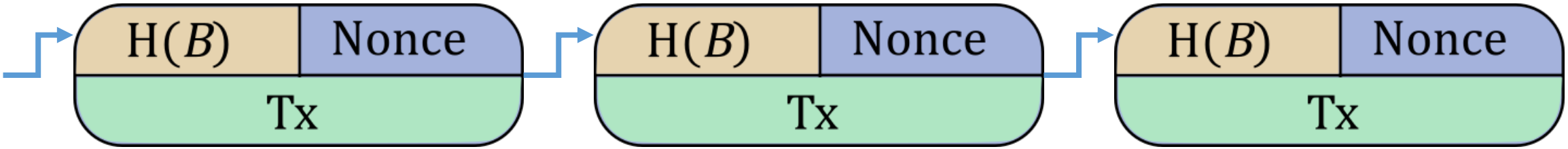
Bitcoin and Cryptocurrencies

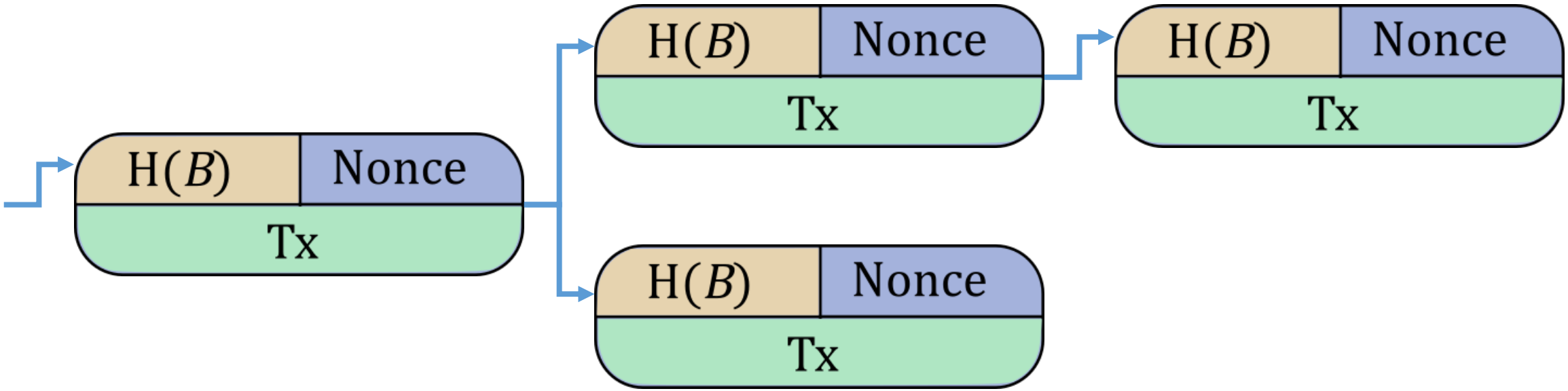
- Lecture 5: Game Theory & Network Attacks: How to Destroy Bitcoin
- Professor Radjabov Mukhammad

Mining



Why do we need miners?

Conflicting Blocks



Consensus

Majority of hashing power has voted for transactions on longest chain.

- It is costly to increase voting power
- Players are not motivated to cheat

The 51% attack!

If any party controls majority of hashing power, they can:

- Undo the past
- Deny mining rewards
- Undermine the currency

We have put a plan in place to see that 51% of all hashing power, will not be maintained by Ghash.IO by executing the following actions:

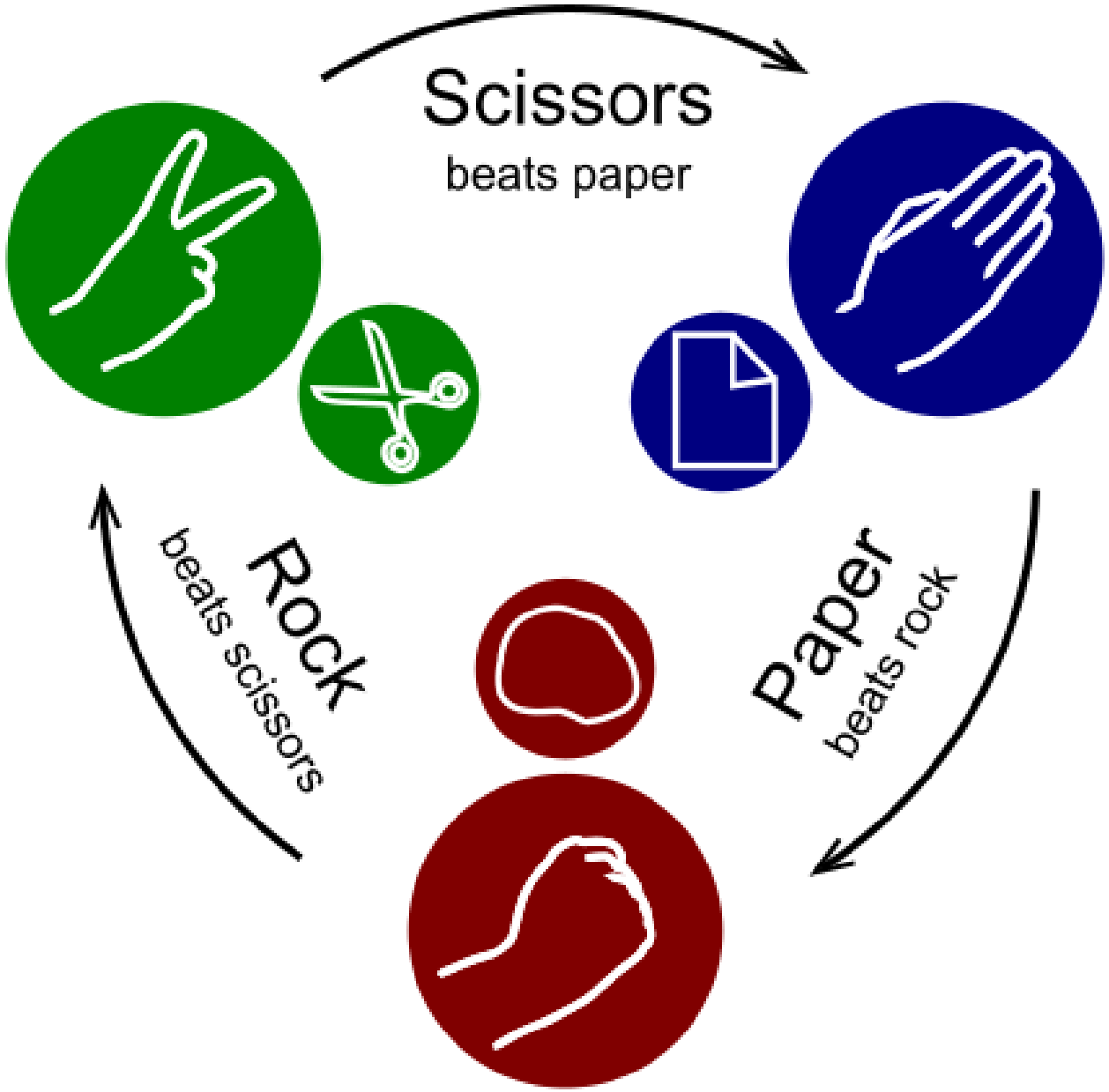
- We will temporarily stop accepting new independent mining facilities to the Ghash.IO pool.
- We will implement a feature, allowing CEX.IO users to mine bitcoins from other pools. So when they purchase GH/s they can put it towards any pool they choose.

We will not be implementing a pool fee, as we believe the pool has to remain free.

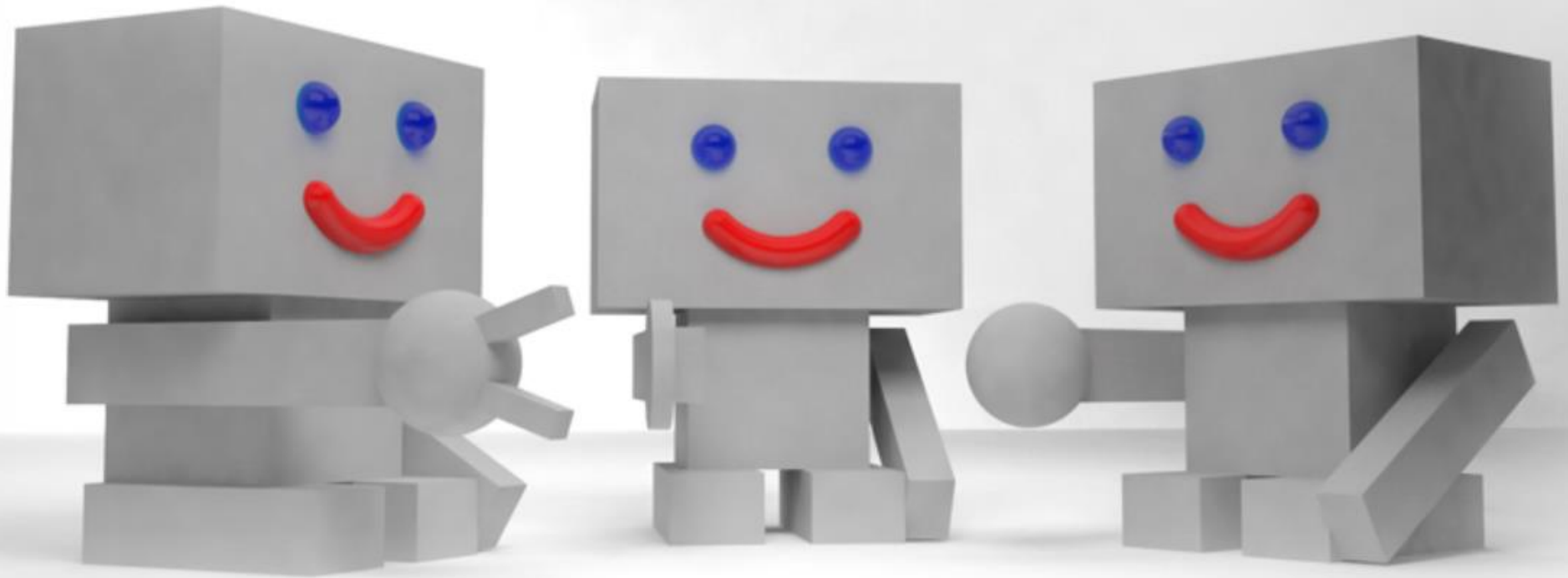
GHash.IO does not have any intentions to execute a 51% attack, as it will do serious damage to the Bitcoin community, of which we are part of. On the contrary, our plans are to expand the bitcoin community as well as utilise the hashing power to develop a greater bitcoin economic structure. If something happened to Bitcoin as a whole it could risk our investments in physical hardware, damage those who love Bitcoin and we see no benefit from having 51% stake in mining.

Nash Equilibrium

Or, can selfish miners keep Bitcoin stable?


Scissors
beats paper
Paper
beats rock
Rock
beats scissors

Rock Paper Scissors Programming Competition



Although rock-paper-scissors (RPS) may seem like a trivial game, it actually involves the hard computational problem of temporal pattern recognition. This problem is fundamental to the fields of machine learning, artificial intelligence, and data compression. In fact, it might even be essential to understanding how human intelligence works.

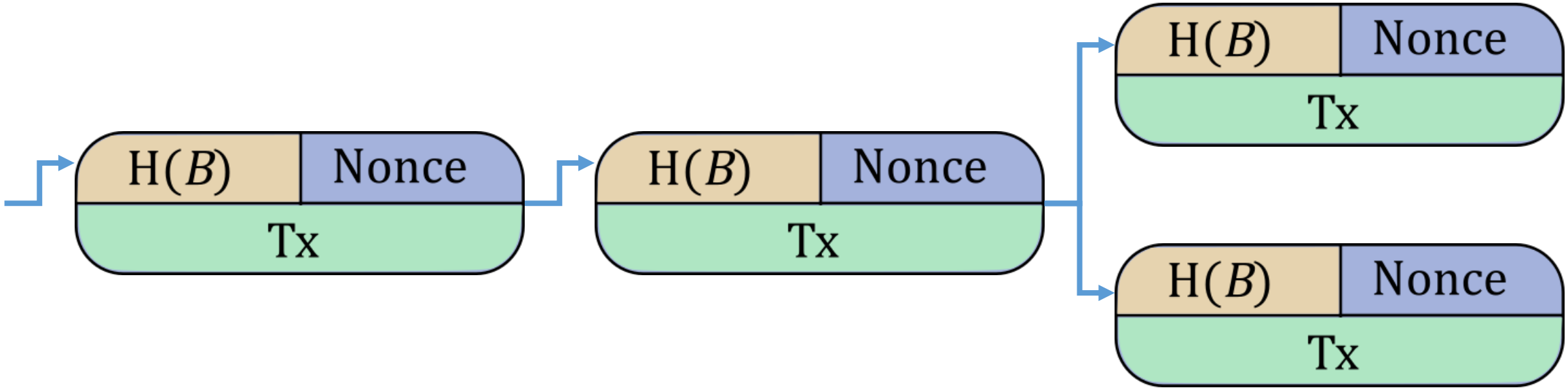
Nash equilibrium

It is a configuration of strategies such that no participant can do better by unilaterally changing their own strategy.

Prisoner's Dilemma

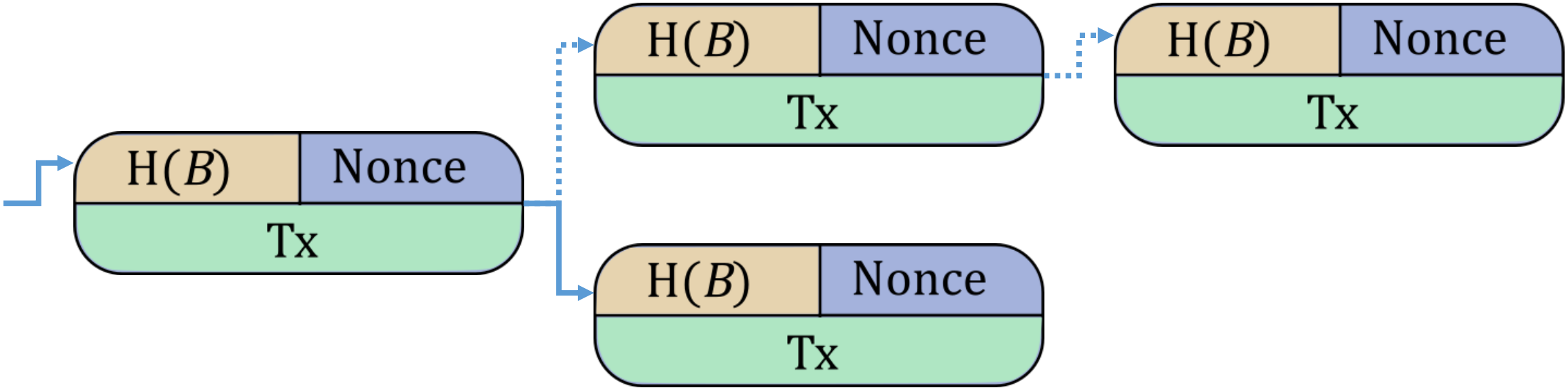
	B stays loyal	B defects
A stays loyal	1,1	3,0
A defects	0,3	2,2

Bitcoin mining … equilibrium?

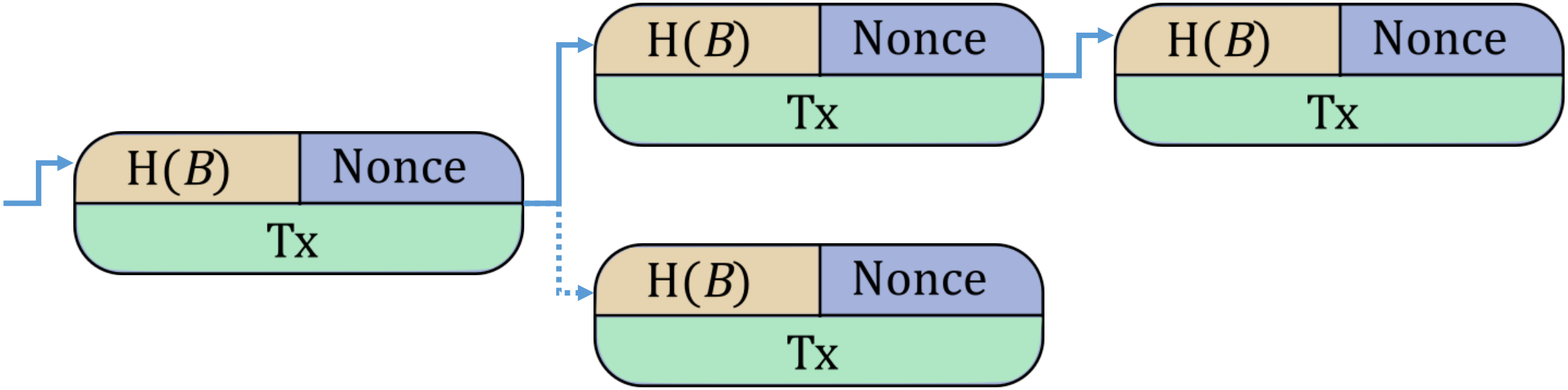


Selfish mining

I’ll keep these blocks for myself!



I’ll keep these blocks for myself!



if we gain a lead:

  withhold blocks
  mine on private chain

else if lead shrinks, but is still at least 2:

  reveal blocks to keep abreast with public chain

else if lead drops below 2:

  reveal all blocks
  mine on public chain

Worries

“Rational miners will prefer to join the selfish miners, and the colluding group will increase in size until it becomes a majority. At this point, the Bitcoin system ceases to be a decentralized currency.”

Majority is not Enough: Bitcoin Mining is Vulnerable

Ittay Eyal, and Emin Gün Sirer

Reaction

```
From: Gavin Andresen <gavinandresen@gmail.com>
Date: Thu, 7 Nov 2013 14:56:56 +1000

> P.S: If any large pools want to try this stuff out, give me a shout. You
> have my PGP key - confidentiality assured.
>

If I find out one of the large pools decides to run this 'experiment' on
the main network, I will make it my mission to tell people to switch to a
more responsible pool.
```

Legal and Regulatory Risk

- Law-abiding user might lose their funds if an exchange is shut down for criminal activity

- Uncertain tax treatment of gains/losses due to currency fluctuations

- Let’s talk about Bitcoin’s regulatory environment

Overview

- Risks in Bitcoin
- Digression on deanonymizing transactions
- **Regulating Bitcoin**

Regulating Bitcoin

- Bitcoin's original vision is in tension with regulation and government control
- Strong cyber-libertarianism streak
-
- The decentralized design makes it harder, but by no means impossible, to regulate

Making the case for oversight

- Untraceable digital cash defeats capital controls

- Country can’t stop Bitcoin value from flowing in or out

- Government countermeasure: disconnect BTC world from financial institutions
- Example: China

Making the case for oversight

- Untraceable digital cash facilitates some crimes:
- kidnapping and extortion
- tax evasion
- sale of illegal items

Welcome! | Silk Road

Silk Road

anonymous marketplace

Welcome [redacted]

messages(0) | orders(0) | account(฿0.00) | settings | log out

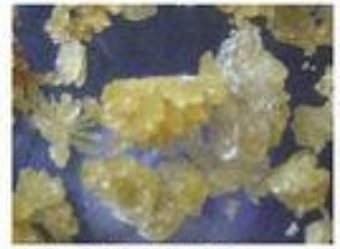
search | (0)

Shop by category:

- Drugs(1249)
  - Cannabis(410)
  - Ecstasy(86)
  - Dissociatives(47)
  - Psychedelics(142)
  - Opioids(92)
  - Stimulants(107)
  - Other(150)
  - Benzos(96)
- Lab Supplies(23)
- Digital goods(93)
- Services(107)
- Money(71)
- Weaponry(9)
- Home & Garden(4)
- Food(1)
- Electronics(11)
- Books(76)
- Drug paraphernalia(46)
- XXX(48)
- Medical(3)
- Computer equipment(19)
- Art(1)
- Apparel(8)
- Sporting goods(3)
- Tickets(1)
- Forgeries(13)
- Fireworks(2)

1g Tangerine Kush Bubble Hash

฿60.96



-NN- DMT YELLOW CLASSIC (500mg)

฿19.39

Barcode Manipulation scam keeping...

฿2.31

3.5g OG Kush

฿22.17

MDMA and MDEA mixure 1 gram

฿23.44

Guerrilla Warfare Book's

฿0.46

co-codamol 30mg codeine / 500mg...

฿4.59

CASH BLOWOUT!! Vendors, SYG is...

฿0.01

Super BOMB Jolly Rancher 1/8...

฿24.20

News:

- Site **glitches**
- Missing **deposits**
- Site **restored**
- Forum bugs **addressed**
- Pricing and hedging **improvements**
- Escrow hedging **update**
- New feature to help protect **sellers**
- Seller ranking and feedback **overhaul**

Silk Road

- largest online market for illegal drugs
- ran as a Tor hidden service
- payment in Bitcoins
- site held BTC in escrow while goods shipped
- eBay-like reputation system
- run by “Dread Pirate Roberts”

operated February 2011 to October 2013

Ross Ulbricht
operator of Silk Road

Arrested October 2013
Charged with money laundering, computer hacking, conspiracy to traffic narcotics
Convicted and sentenced to life imprisonment in 2015

He tried to cover his tracks, but they connected the dots

government seized 174,000 BTC
auctioned them to the public

lessons:

hard to keep real and virtual separate
hard to stay anonymous for a long time
Feds can “follow the money”
⇒ money becomes untouchable

Making the case for oversight

- Consumer protection
- When Mt. Gox collapsed, lost $300M in bitcoins
- Need orderly process to distribute assets equitably
- Risk of collapse motivates need to disclose risks
- Information asymmetries among providers are rife
-
- Irreversible bitcoin payments run counter to many protections developed for traditional methods

Regulatory Options for Exchanges

- 1. Already, US FinCEN has issued guidance requiring exchanges to register as “money-services businesses” and comply with regs
- 2. No consumer protection thus far for dealing with fraudulent transactions
- 3. FDIC-style deposit insurance and authority to wind down failing exchanges possible, but not under consideration

Detecting selfishness

- Orphaned blocks
- Timing hints

More at: *“How to detect selfish miners”* by Ittay Eyal, and Emin Gün Sirer, http://hackingdistributed.com/2014/01/15/detecting-selfish-mining/

Reference

- The Bitcoin Standard: The Decentralized Alternative to Central Banking – Illustrated, April 24, 2018 by Saifedean Ammous
- The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Crypto Trading, Derivatives, Digital Assets) – Illustrated, September 15, 2018 by Antony Lewis (Author)
- Blockchain Bubble or Revolution: The Future of Bitcoin, Blockchains, and Cryptocurrencies – June 12, 2019 by Neel Mehta (Author), Aditya Agashe (Author), Parth Detroja (Author)
- Cryptocurrency Investing For Dummies – March 6, 2019 by Kiana Danial
- Cryptocurrency Mining For Dummies– Illustrated, December 5, 2019 by Peter Kent
- Cryptocurrency Mining: A Complete Beginners Guide to Mining Cryptocurrencies, Including Bitcoin, Litecoin, Ethereum, Altcoin, Monero, and Others – February 21, 2018 by Crypto Tech Academy (Author)