BANK FOR INTERNATIONAL SETTLEMENTS

Money and coordination

Hyun Song Shin*
Bank for International Settlements

Bank of Finland/CEPR conference "Money in the digital age"
Helsinki, 13 June 2018

* The views expressed here are mine, not necessarily those of the Bank for International Settlements.

Economics of money

- Money as memory (Kocherlakota (JET 1998))
  - Money substitutes for a shared ledger recording the full history of who has paid what to whom
- Inherently worthless tokens perform better in eliciting cooperation than keeping score individually
  - Araujo and Guimaraes (RED 2017): money as a record (of goods delivered/services rendered) is more robust to imperfect information
  - Camera and Casari (AEJ Micro 2014) shows experimental evidence
- Maintaining identical copies of a ledger recording the full history of payments brings us to the discussion on cryptocurrencies

Assessing cryptocurrencies

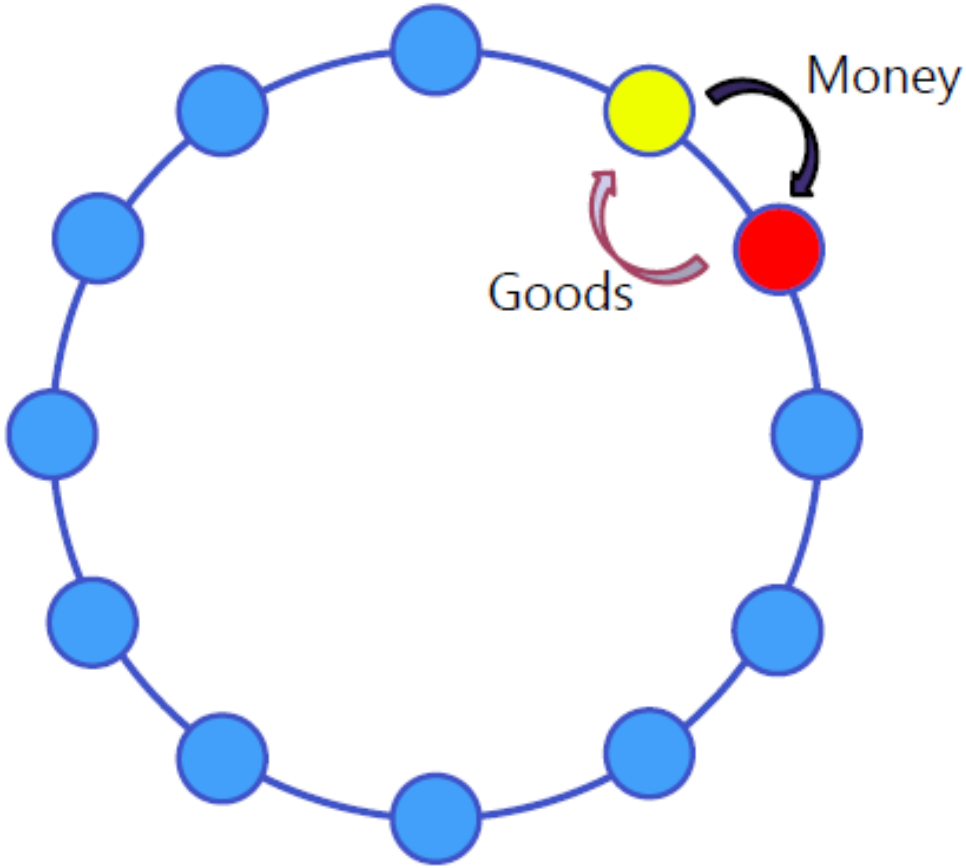
- Focus on the economics, not the technology
  - How well do they serve as money?
  - Can they perform the role played by today's monetary system?
- Two limitations loom large
  - Lacks scalability
  - Lacks guarantee of finality

Ecosystem

- Users who make and receive payments
- Miners who update the ledger

- Two papers in this conference:
  - Game between the miners (Biais, Bisière, Bouvard and Casamatta (2017))
  - Game between the users (Huberman, Leshno and Moellemi (2017))

Economy with high value payments



Finality of payments

- Finality refers to the irreversible and unconditional nature of the payment
  - Cornerstone of a well-functioning payment system
  - Conventional monetary system does this ultimately through the settlement on the central bank's balance sheet.
- Finality is especially important when one payment is dependent on another
  - Otherwise, a buyer "pays" when there is no money
  - Possibility of cascade of voided transactions

Finding consensus in a decentralised system

- How to achieve consensus?
- How to achieve consensus *good enough for action* when there is something at stake?

- These are quite different questions
  - Halpern and Moses (JACM 1990)
  - Rubinstein (AER 1989)
  - Morris, Rob and Shin (Econometrica 1995)

Two node problem

Restatement of the coordinated attack problem (Halpern and Moses (1990))

- Two nodes in a distributed system must certify a payment as being genuine or not
- Two states:
  - Genuine (G), with probability $1 - \delta$
  - Fraudulent (F), with probability δ
- Node 1 knows whether G or F is the case; Node 2 does not
  - However, Nodes 1 and 2 can send messages and confirmations to each other
  - Messages get through with probability $1 - \varepsilon$, with $\varepsilon < \delta$

Payoffs

- Payoffs in state G

	Confirm	Reject
Confirm	$1, 1$	$-M, 0$
Reject	$0, -M$	$0, 0$

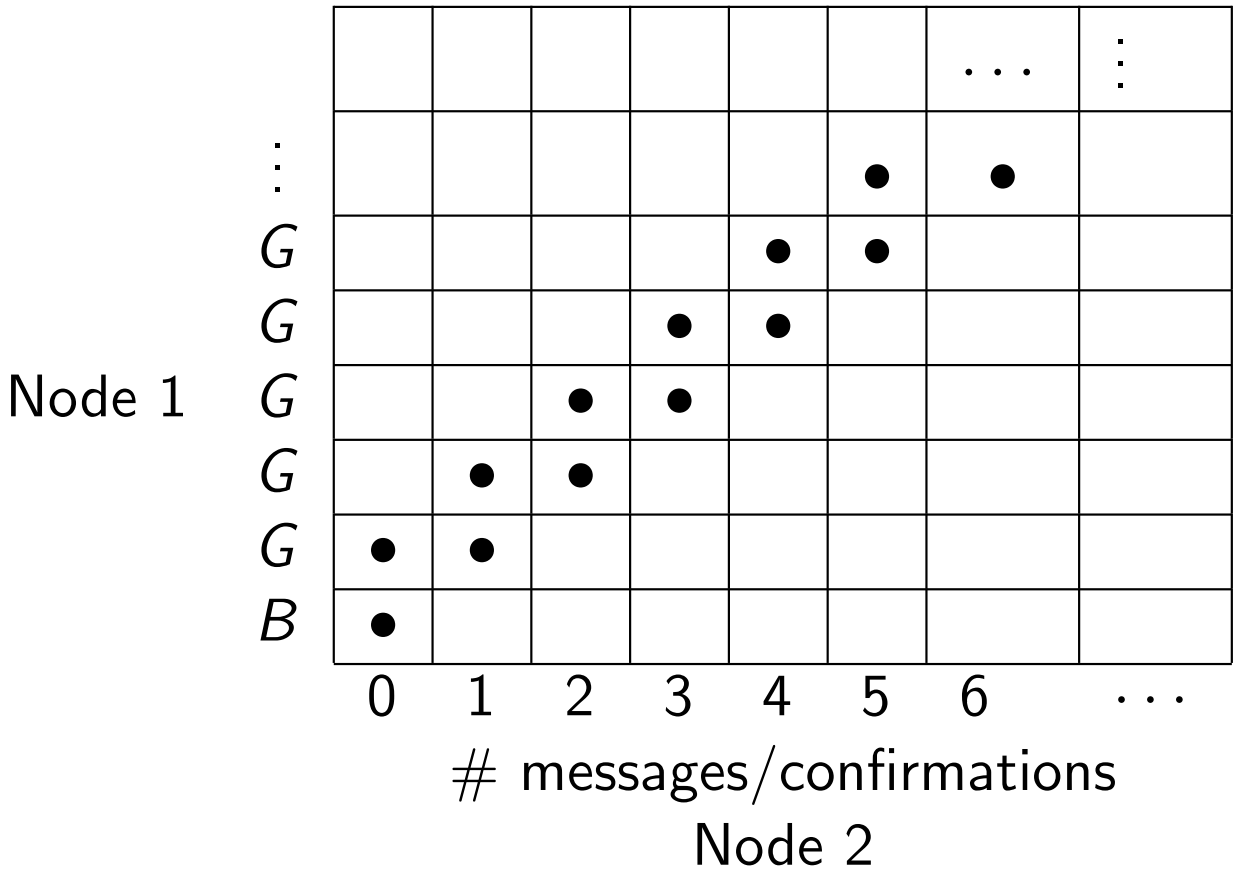
$M > 1$

- Payoffs in state F

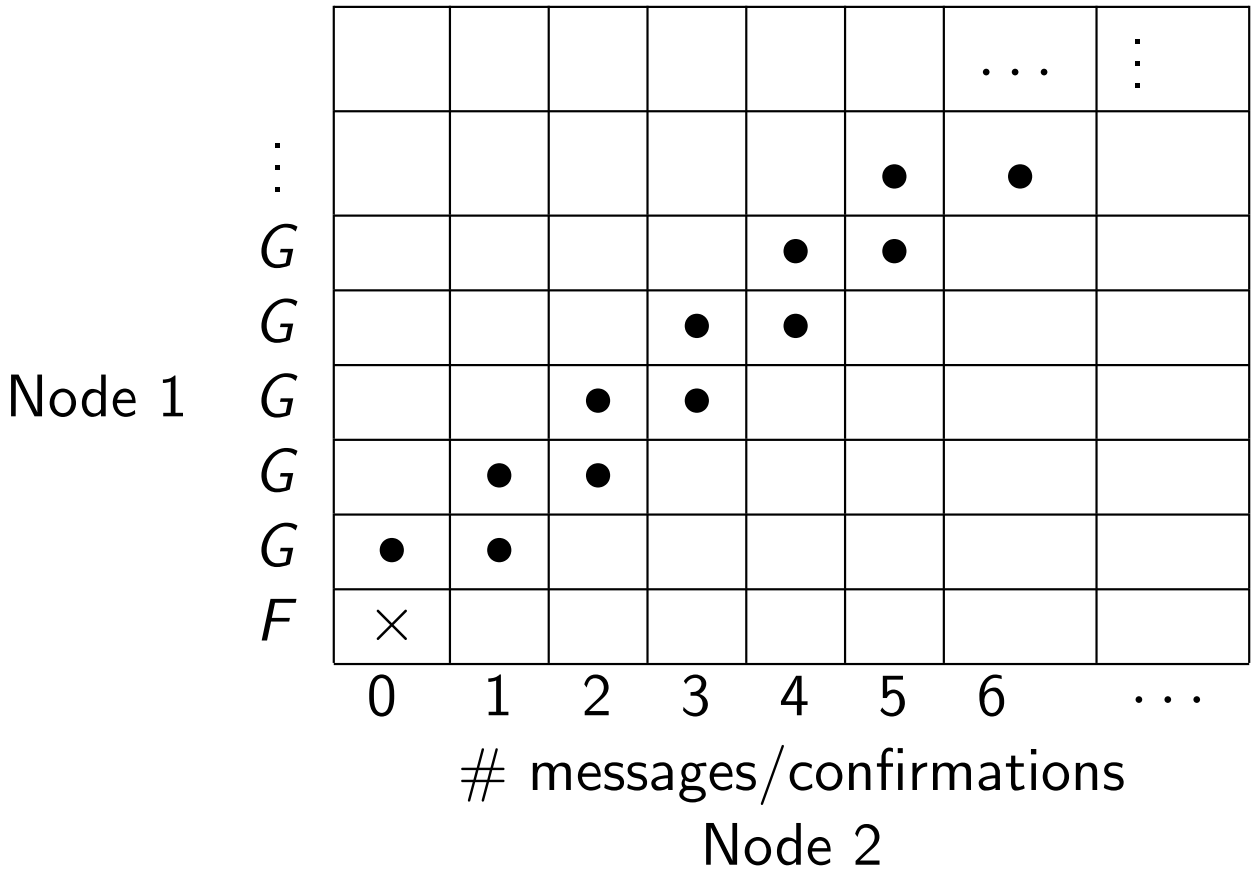
	Confirm	Reject
Confirm	$-M, -M$	$-M, 0$
Reject	$0, -M$	$0, 0$

Confirming genuine payments and rejecting fraudulent ones are best for both nodes

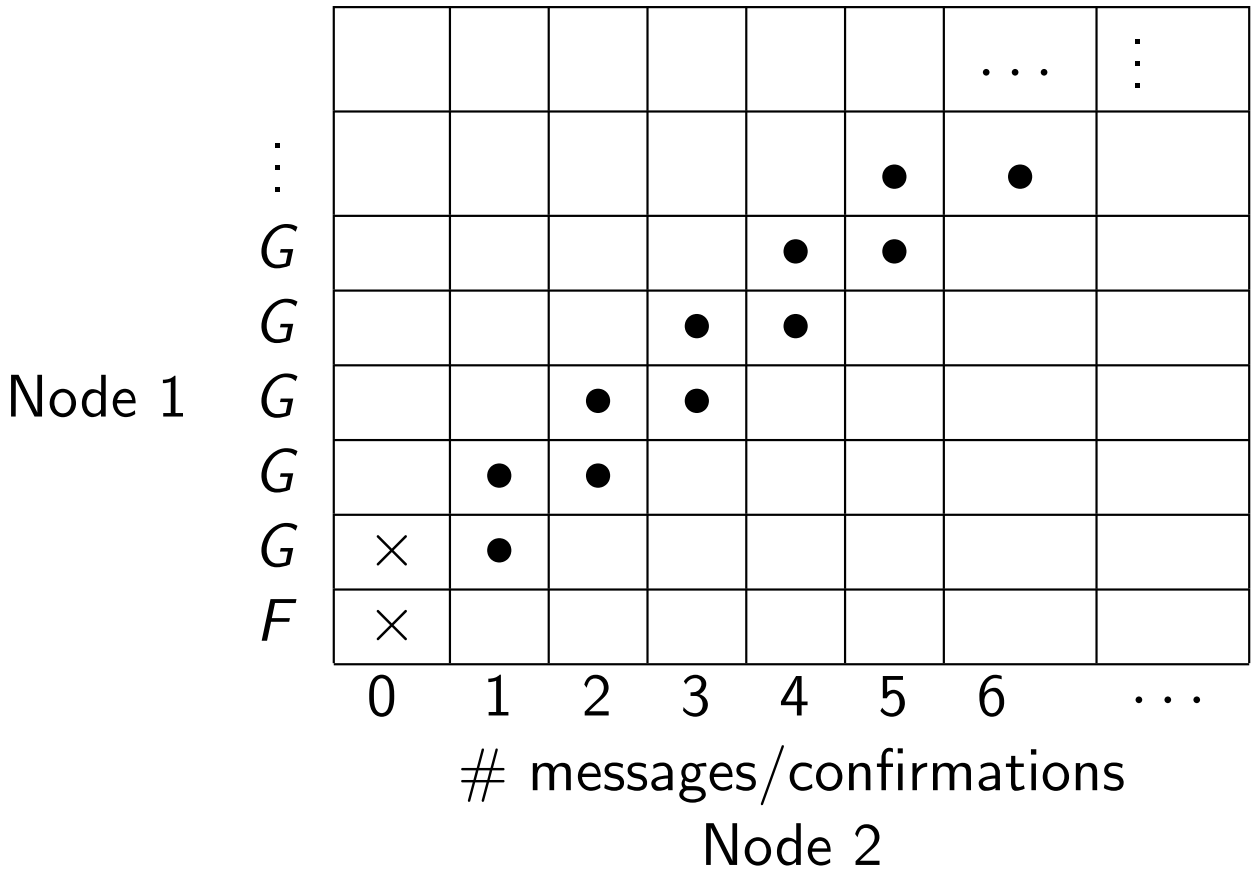
Strategy space



Node 1 rejects in state F

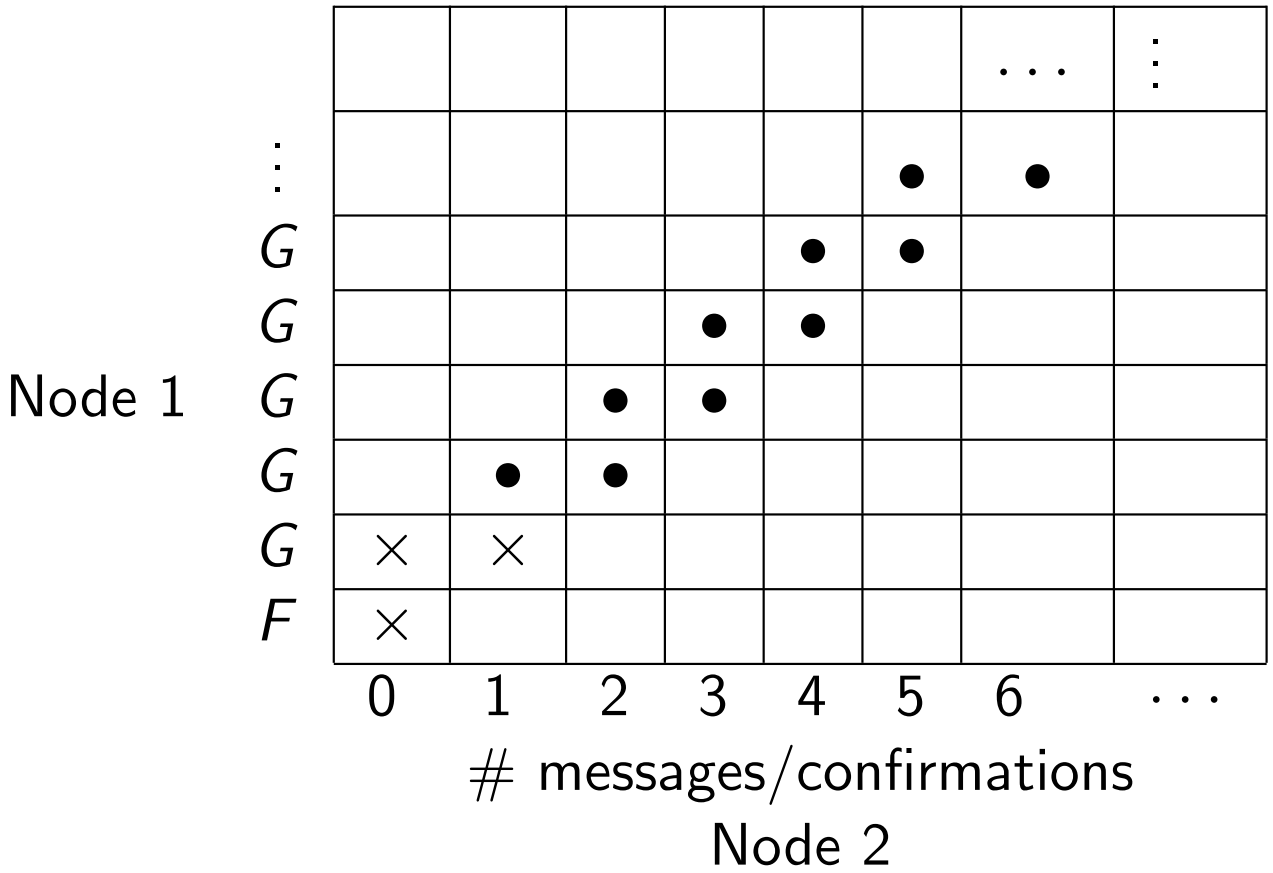


Node 2 rejects when no message arrives



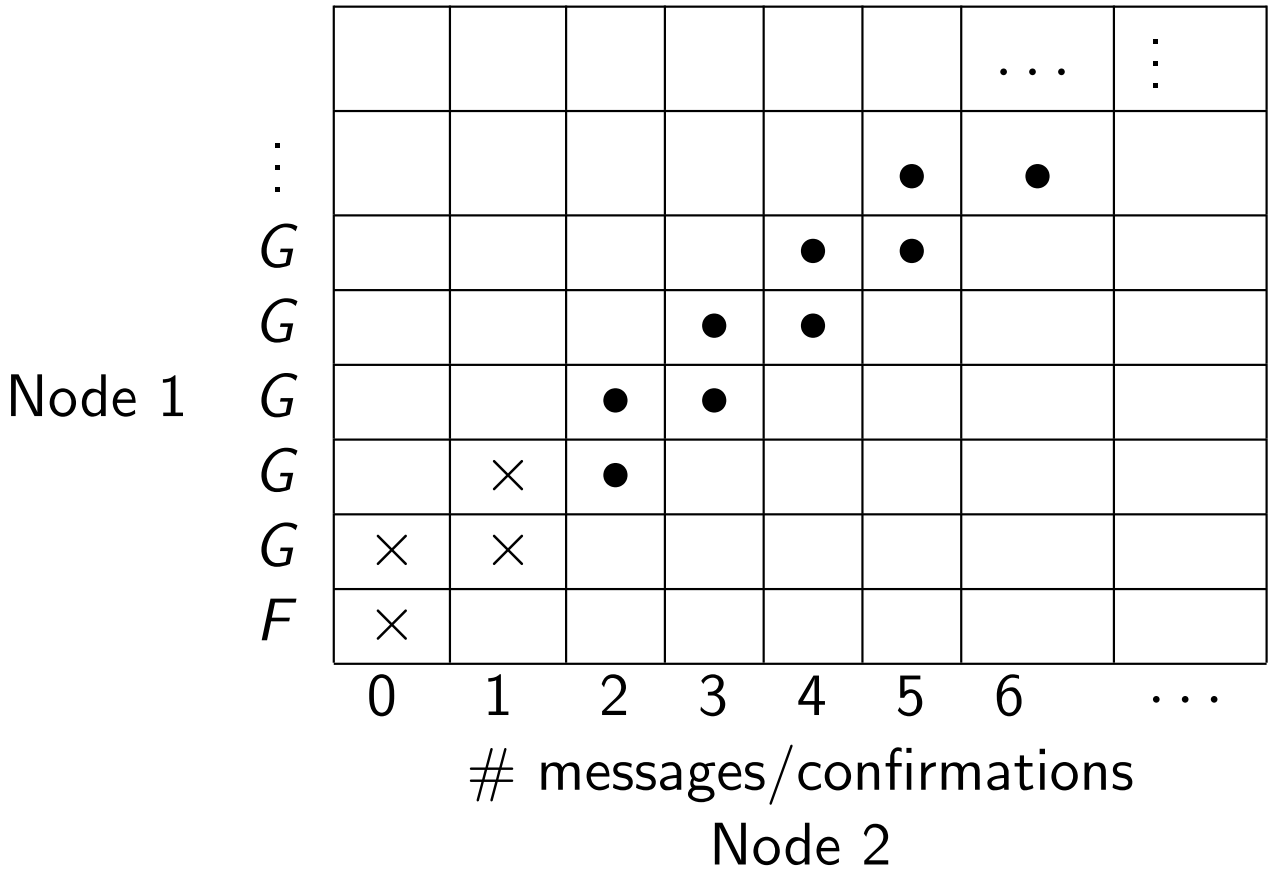
Expected payoff to confirm is $\frac{(1-\delta)\varepsilon-\delta M}{(1-\delta)\varepsilon+\delta} < 0$

Node 1 rejects when message is sent but no confirmation arrives



Either message did not get through ($\frac{(1-\delta)\varepsilon}{(1-\delta)\varepsilon+(1-\delta)\varepsilon(1-\varepsilon)}$) or confirmation did not get through, and the former is more likely
Expected payoff to confirm is $p \cdot 1 - (1-p)\, M < 0$, since $p < 0.5$ and $M > 1$

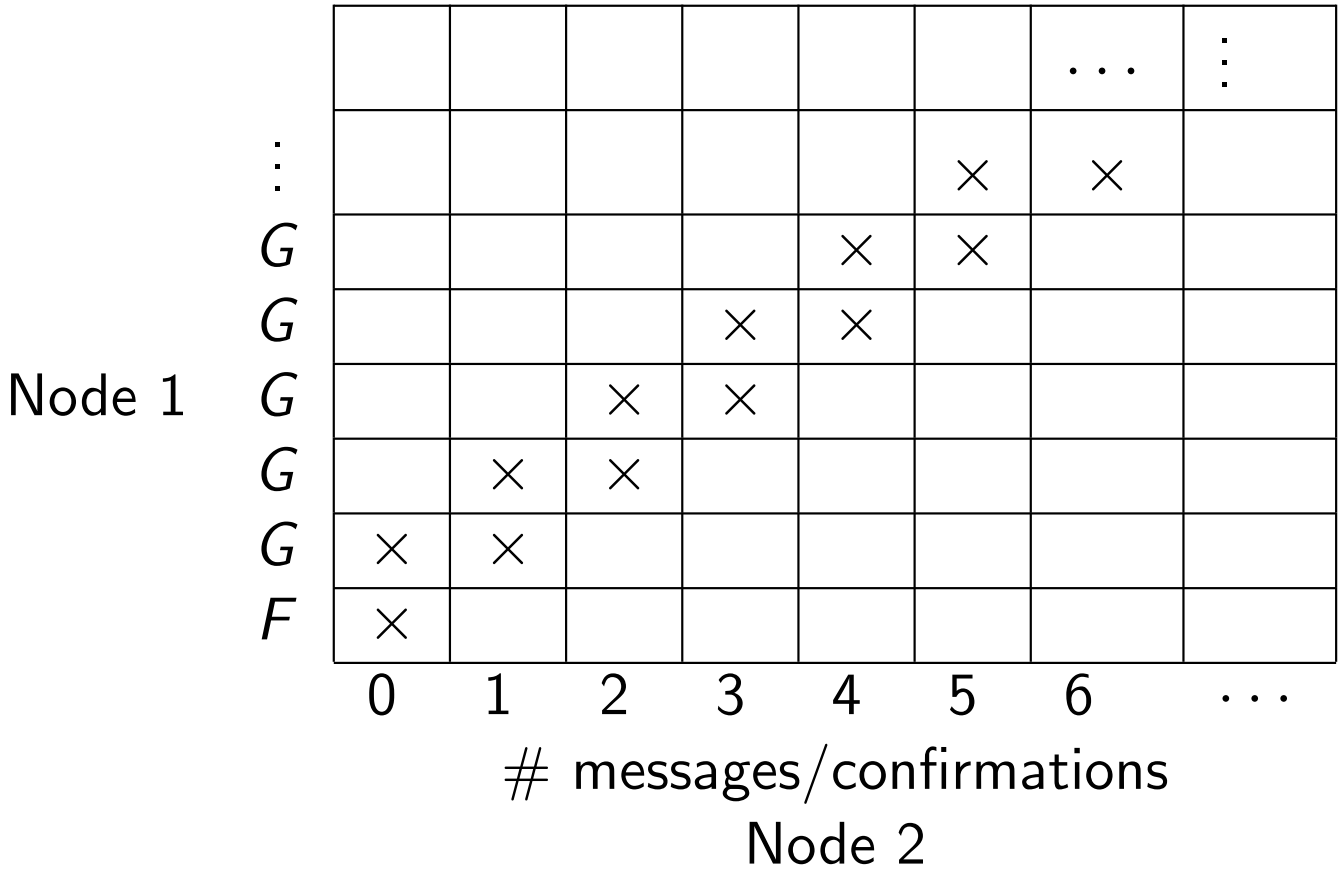
Node 2 rejects when confirmation is sent but no re-confirmation arrives



Either confirmation did not get through or re-confirmation did not get through, and the former is more likely

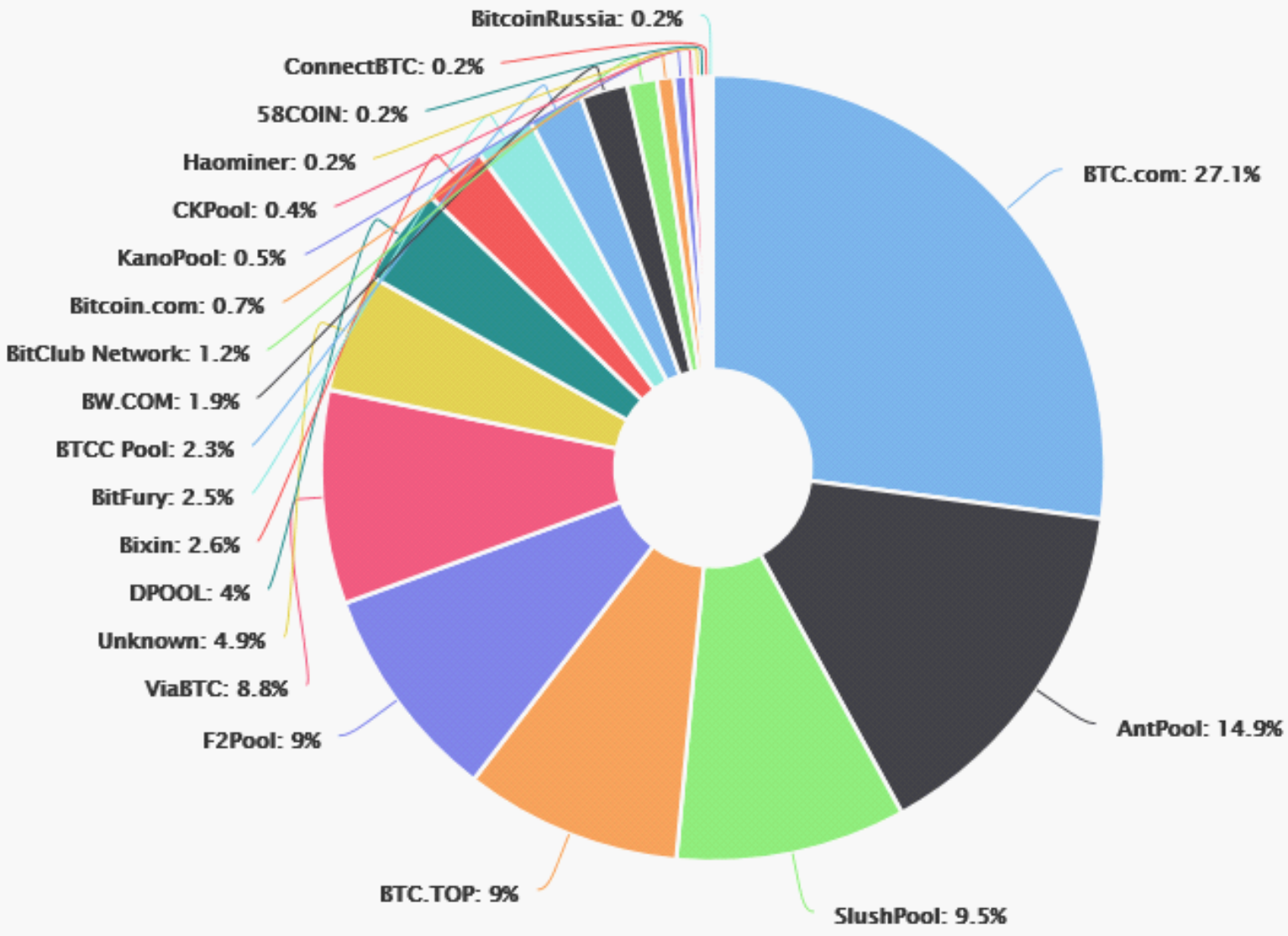
Expected payoff to confirm is $p \cdot 1 - (1 - p) M < 0$, since $p < 0.5$ and $M > 1$

Unique (dominance solvable) equilibrium is for both nodes to reject irrespective of number of confirmations

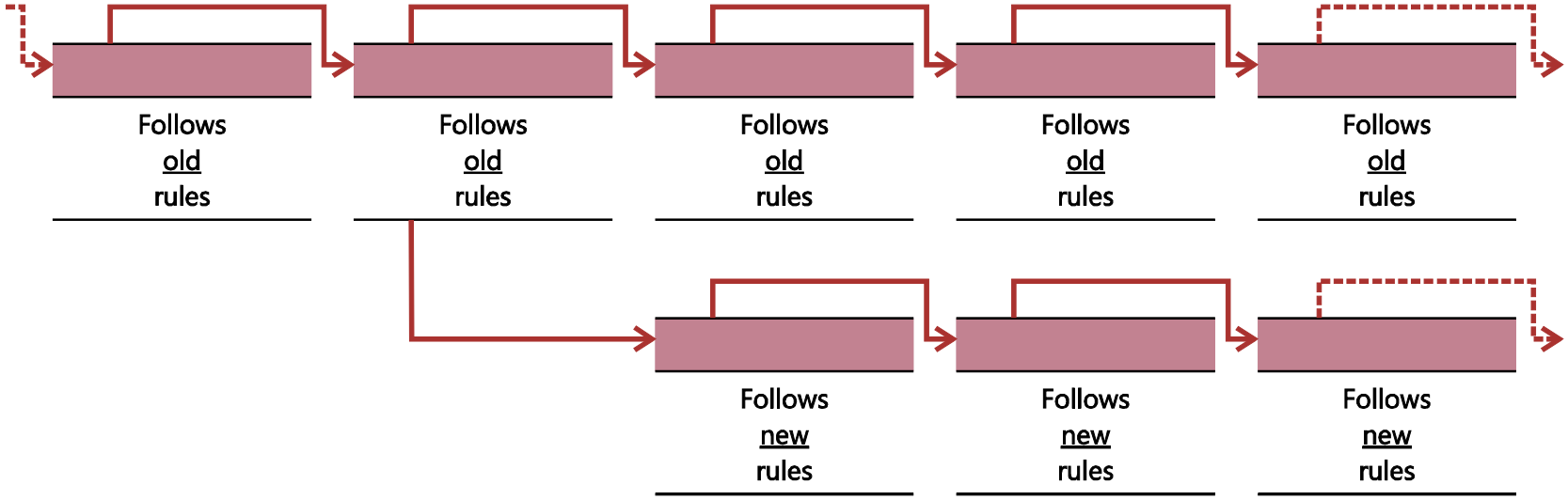


Stark difference between **consensus** and **consensus strong enough for action**

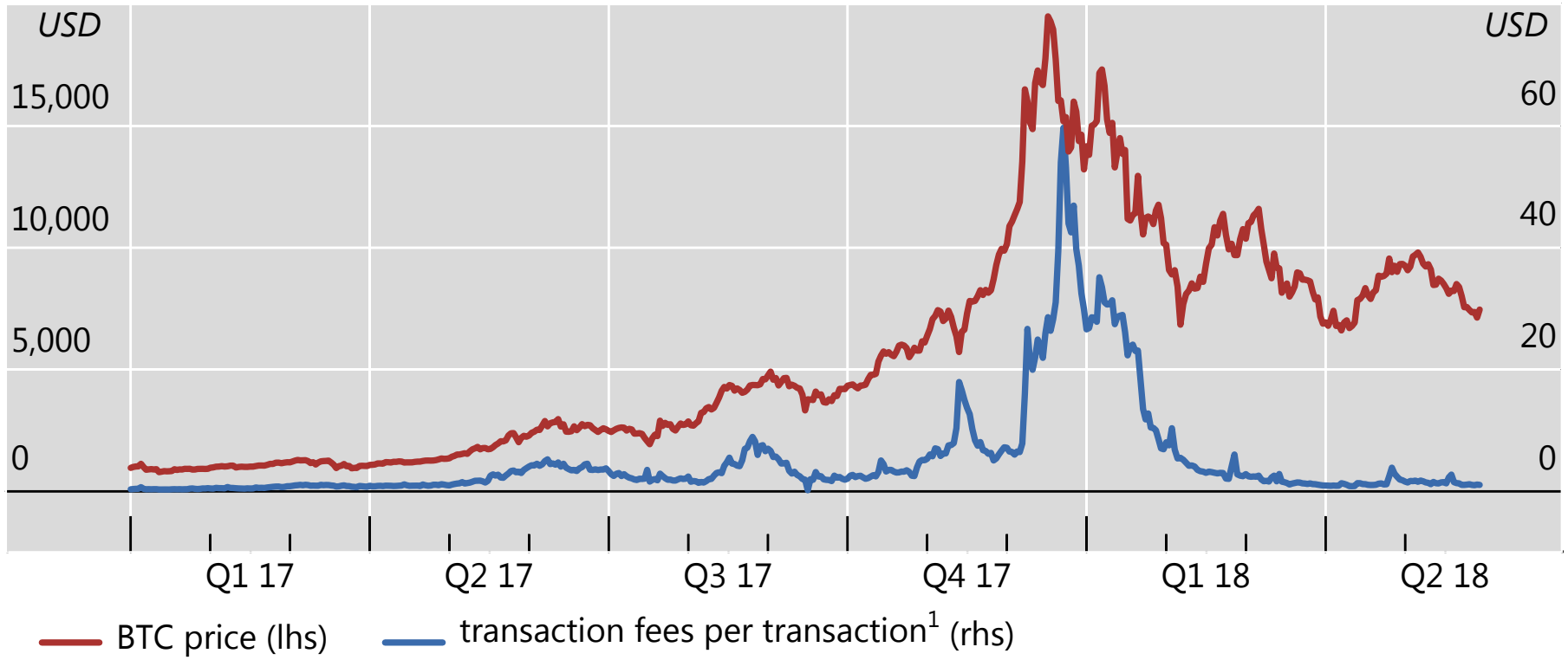
Concentration of mining pools



A “hard fork” in the blockchain

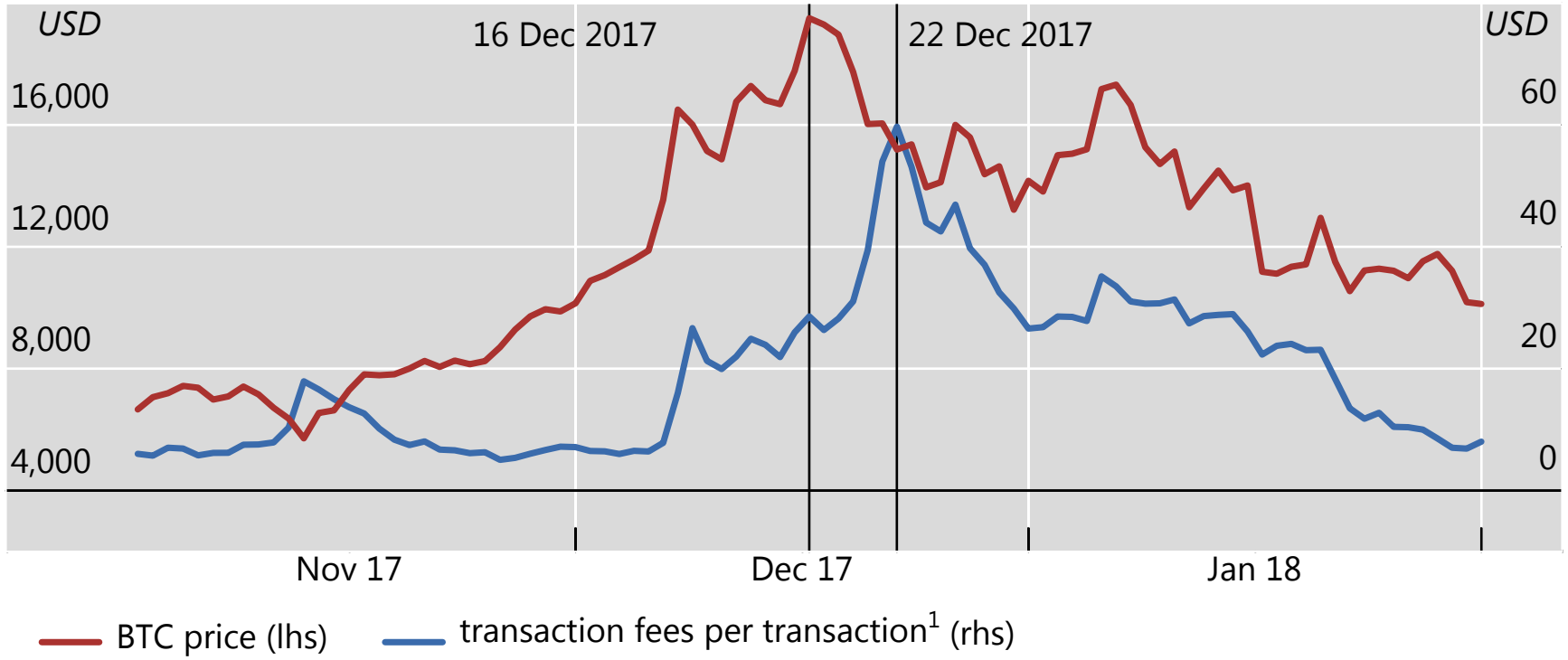


Bitcoin price and transaction fees



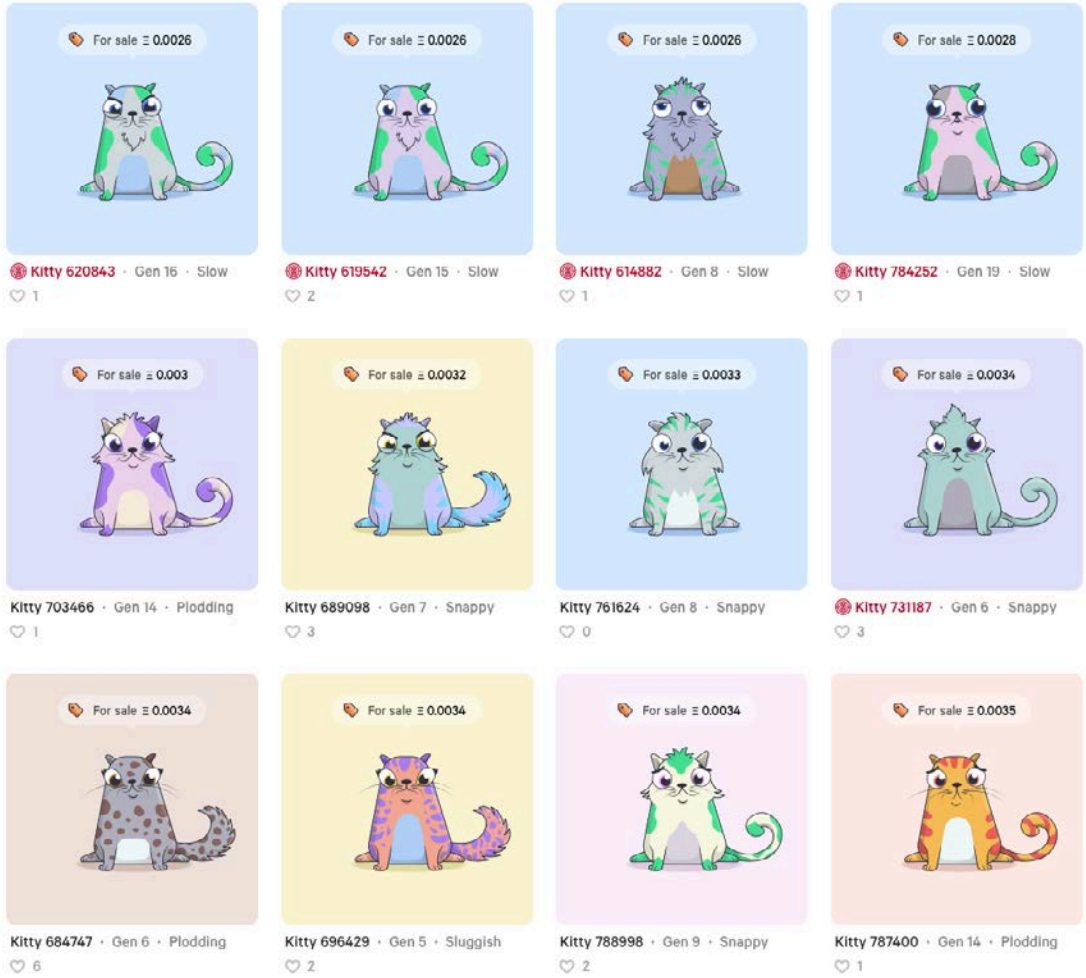
[1] Transaction fees per transaction are computed by dividing the total transaction fees in a given day by the number of daily confirmed Bitcoin transactions.

Bitcoin price and transaction fees

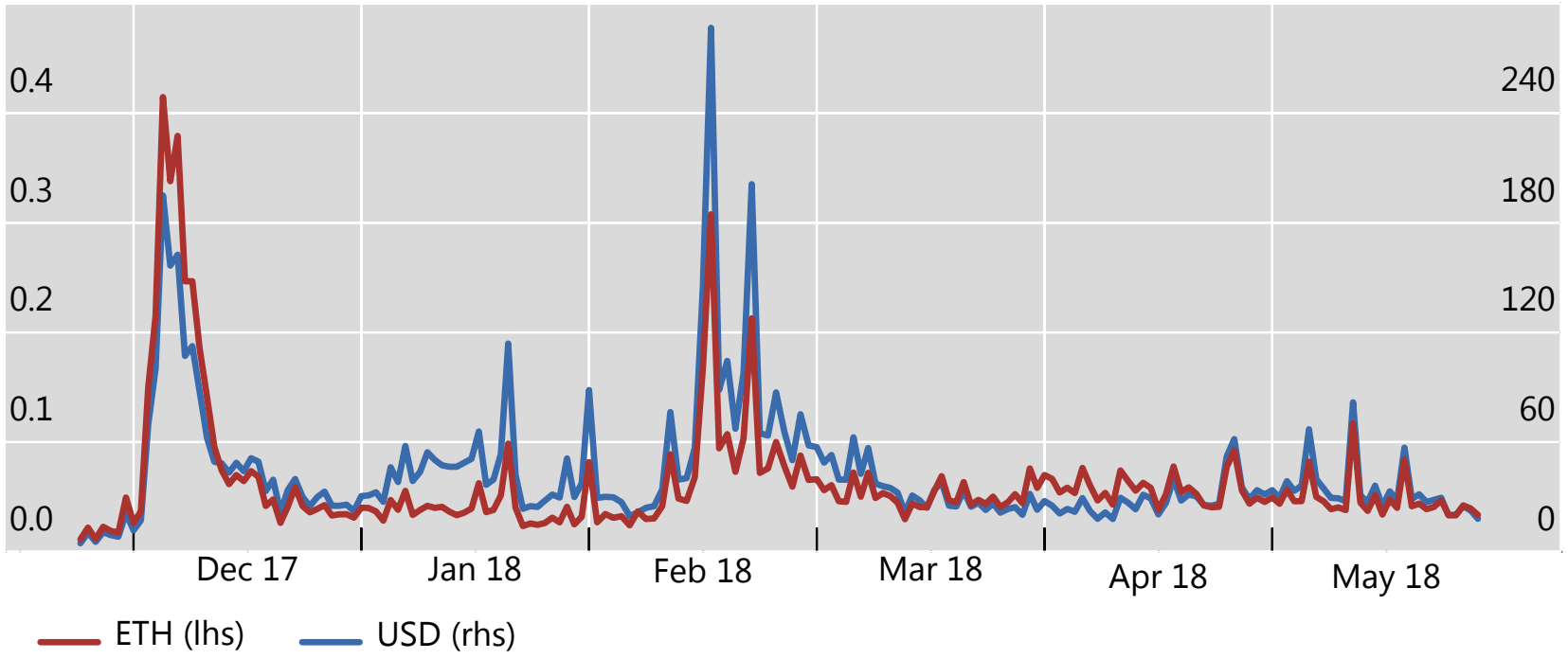


[1] Transaction fees per transaction are computed by dividing the total transaction fees in a given day by the number of daily confirmed Bitcoin transactions.

Crypto Kitties for sale



Crypto Kitties: average daily sale price



Samson Mow
@Excellion

"Guys, no one's using our 8 lane highway."
"We need 32 lanes."
"You're a genius."#Overheard #TransactionSuperhighway #Bcash

9:06 AM - May 8, 2018

1,595 397 people are talking about this

Summing up

- Economics of cryptocurrencies pose questions just as hard as for illicit activities and consumer protection
- Outsourcing trust to selfish book-keepers results in a congestion game, not a coordination game
  - The more the sorrier, instead of the more the merrier
- Outsourcing trust to selfish book-keepers cannot guarantee finality, the cornerstone of a payment system
  - Not simply about technical agreement, but about accountability