Why Fixed Costs Matter for Proof-of-Work Based Cryptocurrencies[1]

Rod Garratt (UCSB) and Maarten van Oordt (Bank of Canada)

2nd Crypto Asset Lab Conference

27 October 2020

[1] *Views expressed do not necessarily reflect official positions of the Bank of Canada.*

FINANCE
The Coronavirus Economy: Bankruptcy attorneys are learning to hit 'mute'

FINANCE
Dow Jones edges higher despite continued unrest across U.S.

ENTERTAINMENT
Christian Slater on retelling the Betty Broderick story in the new season of 'Dirty John'

THE LEDGER • BITCOIN

Bitcoin Spinoff Hacked in Rare '51% Attack'

BY **JEFF JOHN ROBERTS**

May 29, 2018 7:48 AM PDT

51% attack on Bitcoin Gold

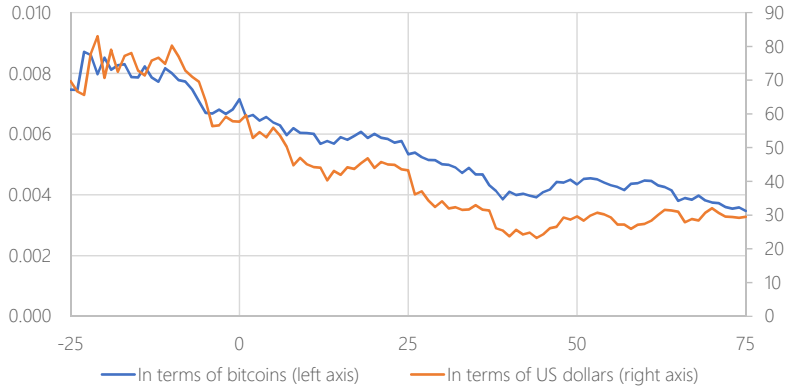
- Bitcoin Gold was born as a hard fork of the Bitcoin blockchain in October 2017
- Used a proof-of-work protocol that disabled the use of specialized equipment (eg ASICs) for mining operations
- Goal was to achieve higher level of resilience through decentralized mining structure

51% attack on Bitcoin Gold

- Bitcoin Gold was born as a hard fork of the Bitcoin blockchain in October 2017
- Used a proof-of-work protocol that disabled the use of specialized equipment (eg ASICs) for mining operations
- Goal was to achieve higher level of resilience through decentralized mining structure

- Several 51% attacks during May 16-19 double spent $18 million worth of Bitcoin Gold
- Loss of confidence in Bitcoin Gold and decline in exchange rate
- Only one-sixth of what it was at time of attack and number of transactions declined to less than one-third

Bitcoin Gold: Exchange Rate and the 51 % Attack in May '18



Note: The solid line shows the exchange rate of Bitcoin Gold during the 25 days before and 75 days following the double-spending attack in May 2018. The start of the double-spending of attacks on 15 May 2018 is indicated by $t = 0$ on the horizontal axis. Source: Binance (cryptocurrency exchange).

Key question

Why was Bitcoin Gold subject to a successful 51% attack, while Bitcoin itself has not been?

Key question

Why was Bitcoin Gold subject to a successful 51% attack, while Bitcoin itself has not been?

- Understanding the role of fixed costs in cryptocurrency mining is crucial to answer this question, and others

Literature

- Papers that formally model bitcoin mining and double-spending attacks consider a per-period flow cost of mining, but not the fixed cost involved with setting up mining operations
  - E.g., Kroll et al. (2013), Abadi and Brunnermeier (2018), Pagnotta and Buraschi (2018), Biais et al. (2019), Chiu and Koeppl (2019a,b), Cong et al. (2019), Easley et al. (2019), Huberman et al. (2019) and Auer (2019).

Literature

- Papers that formally model bitcoin mining and double-spending attacks consider a per-period flow cost of mining, but not the fixed cost involved with setting up mining operations
  - E.g., Kroll et al. (2013), Abadi and Brunnermeier (2018), Pagnotta and Buraschi (2018), Biais et al. (2019), Chiu and Koeppl (2019a,b), Cong et al. (2019), Easley et al. (2019), Huberman et al. (2019) and Auer (2019).

- Partial exceptions
  - Budish (2018) offers verbal discussion
  - Prat and Walter (2019) discuss entry by bitcoin miners in the presence of fixed costs, but they don't model implications for double-spending attacks. Their estimates suggest about two-thirds of the total cost of mining are fixed costs.

Our paper

- Incorporate fixed costs of setting up a mining operation

Our paper

- Incorporate fixed costs of setting up a mining operation
- Some theoretical results

Cost structure of mining	**Only variable**	**Variable and fixed**
Miners earn zero income in equilibrium	True	False
Miners lose when the exchange rate drops	False	True
Mining power exhibits downward rigidity	False	True
Costs of double-spending attacks	Low	High

Our paper

- Incorporate fixed costs of setting up a mining operation
- Some theoretical results

Cost structure of mining	**Only variable**	**Variable and fixed**
Miners earn zero income in equilibrium	True	False
Miners lose when the exchange rate drops	False	True
Mining power exhibits downward rigidity	False	True
Costs of double-spending attacks	Low	High

- Extension with cryptocurrency groups with transferable mining power
  - For tiny currencies with low exchange rate correlation, transferability can eliminate the protection that fixed costs provide

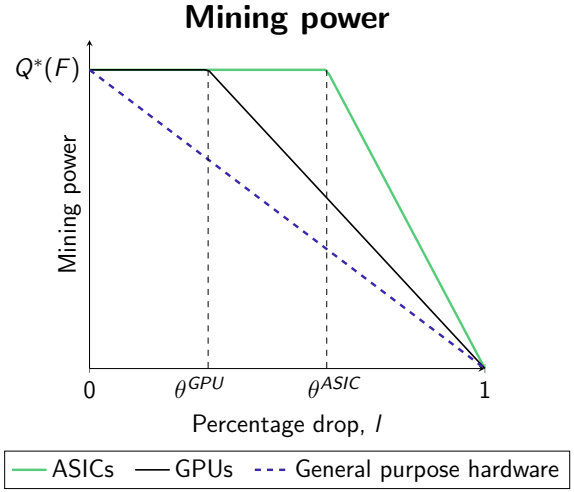
Our paper

- Incorporate fixed costs of setting up a mining operation
- Some theoretical results

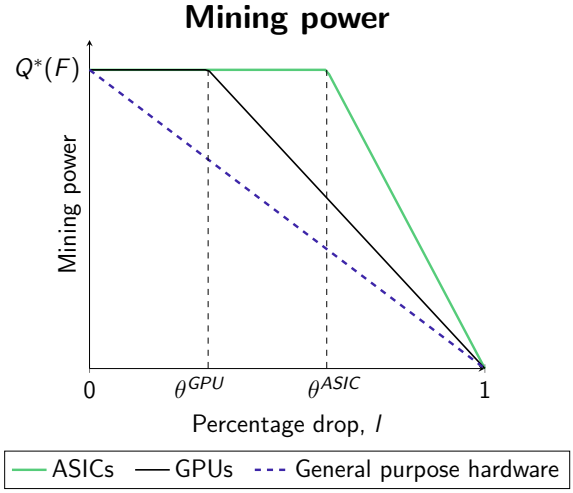
Cost structure of mining	**Only variable**	**Variable and fixed**
Miners earn zero income in equilibrium	True	False
Miners lose when the exchange rate drops	False	True
Mining power exhibits downward rigidity	False	True
Costs of double-spending attacks	Low	High

- Extension with cryptocurrency groups with transferable mining power
  - For tiny currencies with low exchange rate correlation, transferability can eliminate the protection that fixed costs provide
- Empirical results provide supportive evidence of our theoretical results

Theory: Impact of drop in exchange rate



Theory: Impact of drop in exchange rate



In equilibrium:

$$\theta = \frac{\text{Fixed cost} - \text{Alternative use value}}{\text{Total cost over entire life-time}}$$

Empirical relevance of fixed costs

Consider the regression model

$$\Delta q_{it} = \beta_0 + \beta_1 \Delta s_{it} + \beta_2 \Delta s_{it}^{MAX} + \mu_i D_{it} + \varepsilon_{it}, \tag{1}$$

where

- q_{it} and s_{it} are the log levels of the mining power and the exchange rate,
- $s_{it}^{MAX} = \max\{s_{i1}, ..., s_{it}\}$, and
- D_{it} is a dummy variable for "halvings" in block rewards.

Empirical relevance of fixed costs

Consider the regression model

$$\Delta q_{it} = \beta_0 + \beta_1 \Delta s_{it} + \beta_2 \Delta s_{it}^{MAX} + \mu_i D_{it} + \varepsilon_{it}, \tag{1}$$

where

- q_{it} and s_{it} are the log levels of the mining power and the exchange rate,
- $s_{it}^{MAX} = \max\{s_{i1}, ..., s_{it}\}$, and
- D_{it} is a dummy variable for "halvings" in block rewards.

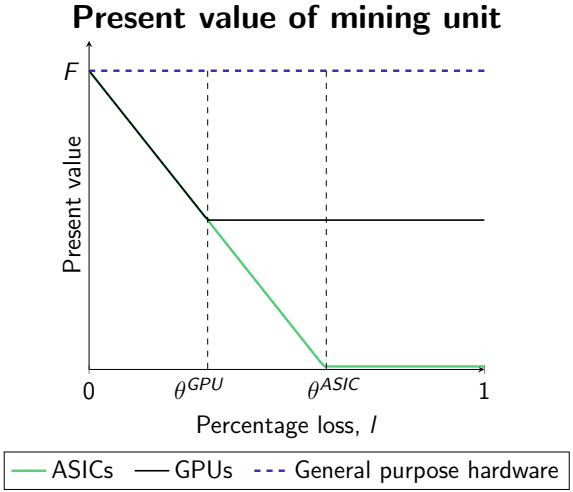
Coefficient β_2 is expected to be insignificant under the null hypothesis where fixed costs are irrelevant (so, no path dependence).

Empirical relevance of fixed costs

VARIABLES	Bitcoin	Ethereum	Litecoin	Monero	Dash	Panel
Change in log	0.085	0.226*	0.074	0.050	0.575***	0.169
exchange rate (Δs_{it})	(0.139)	(0.116)	(0.092)	(0.089)	(0.130)	(0.096)
Change in log	0.670***	0.269*	0.591***	0.676***	0.285	0.537***
peak level (Δs_{it}^{MAX})	(0.145)	(0.159)	(0.125)	(0.166)	(0.173)	(0.078)
Change in Bitcoin	-0.293***					-0.324***
block reward	(0.095)					(0.016)
Change in Ethereum		-0.251**				-0.609***
block rewards		(0.105)				(0.034)
Change in Litecoin			-0.440***			-0.177***
block rewards			(0.115)			(0.024)
Change in Dash					-0.754***	-0.399***
block rewards					(0.191)	(0.039)
Constant	0.384***	0.230***	0.331***	-0.030	0.542***	0.297***
	(0.055)	(0.056)	(0.055)	(0.055)	(0.116)	(0.013)
Observations	106	48	85	61	66	366
R-squared	0.483	0.641	0.577	0.421	0.468	0.478

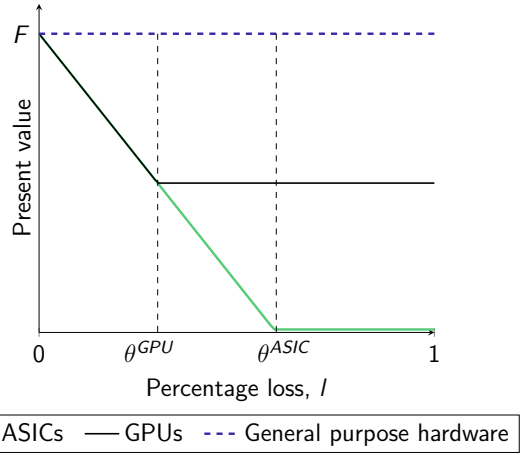
Note: The dependent variable is the quarterly change in log mining power (Δq_{it}). Estimated with least squares. Robust standard errors are reported in parentheses. Statistical significance at the 1%, 5% and 10% significance levels are indicated by ***, ** and *, respectively.

Theory: Impact of drop in exchange rate



Theory: Impact of drop in exchange rate

Present value of mining unit



Double-spending attacks

Two costs to attackers

(a) Coins mined during attack are sold against lower exchange rate

(b) Lower present value after attack (only with fixed costs)

Calibration: Double-spend necessary for profitable attack

Panel (a): Current rewards per block ($b \approx 6.67$)

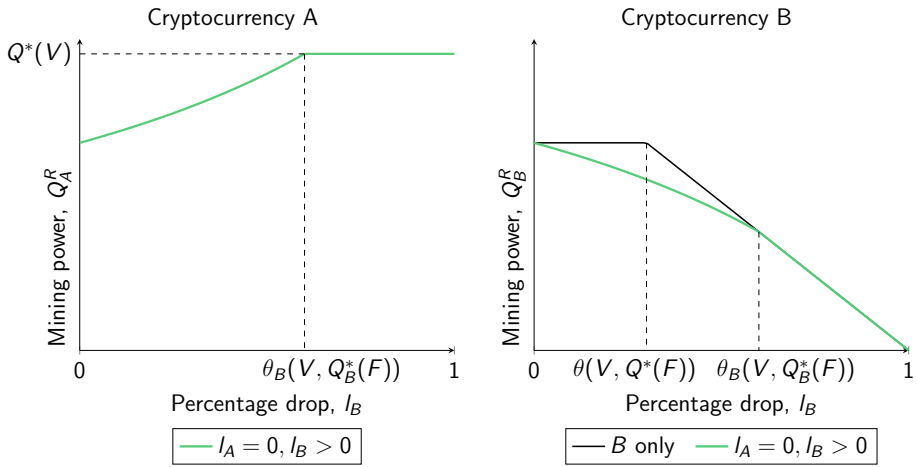
Drop in exchange rate:		15%	30%	60%
Alternative use value:	100%	60	146	510
	50%	124,794	151,608	265,569
	0%	157,759	303,070	530,628

Panel (b): Only transaction fees ($b \approx 0.42$)

Drop in exchange rate:		15%	30%	60%
Alternative use value:	100%	4	9	32
	50%	7,858	9,547	16,722
	0%	9,934	19,084	33,413

Note: The table reports the minimum number of coins that attackers should be able to double spend in order for an attack to be profitable. Parameter choices are: $t^* = 100$, $r = 0.20$ (annualized), $P/Q = 0.51$, $\varepsilon = 1,350$ (annualized), $F = 2,100$. The transaction fees of 0.42 per block are based on the average for bitcoin over the period 2019Q1-Q3.

Preview of transferable mining power



Concluding remarks

- Accounting for fixed costs and alternative use value is crucial to understanding mining behavior and double-spending attacks
- bASIC truth: ASIC mining, which involves fixed costs and a low alternative use value, reduces the profitability of double-spending attacks
- The investment in specialized hardware weakens doomsday predictions regarding the future viability of Bitcoin
- Cryptocurrencies may be less protected when they don't rely on specialized hardware or when they are tiny compared to peers that rely on the same hardware (extension)

Thank you!

Merci à tous!

References

J. Abadi and M. Brunnermeier. Blockchain Economics. *NBER Working Paper*, 25407, 2018.

R. Auer. Beyond the Doomsday Economics of "Proof-of-Work" in Cryptocurrencies. *BIS Working Paper*, 765, 2019.

B. Biais, C. Bisière, M. Bouvard, and C. Casamatta. The Blockchain Folk Theorem. *Review of Financial Studies*, 32(5): 1662–1715, 2019.

E. Budish. The Economic Limits of Bitcoin and the Blockchain. *NBER Working Paper*, 24717, 2018.

J. Chiu and T.V. Koeppl. Blockchain-based Settlement for Asset Trading. *Review of Financial Studies*, 32(5):1716–1753, 2019a.

J. Chiu and T.V. Koeppl. The Economics of Cryptocurrencies: Bitcoin and Beyond. *Bank of Canada Staff Working Paper*, 2019-40, 2019b.

L.W. Cong, Z. He, and N. Wang. Decentralized Mining in Centralized Pools. *Working Paper*, 2019.

D. Easley, M. O'Hara, and S. Basu. From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Journal of Financial Economics*, 2019.

G. Huberman, J. Leshno, and C.C. Moallemi. An Economic Analysis of the Bitcoin Payment System. *Columbia Business School Research Paper*, 17-92, 2019.

F. Kroll, I. Davey, and E. Felten. The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries. *Princeton Working Paper*, 2013.

E. Pagnotta and A. Buraschi. An Equilibrium Valuation of Bitcoin and Decentralized Network Assets. *Working Paper*, 2018.

J. Prat and B. Walter. An Equilibrium Model of the Market for Bitcoin Mining. *Working Paper*, 2019.

Form to Calculate Profitability of Attack

Cryptocurrency blockchain

Typical mining rewards per block, b (coins) 6.67

Normal block time (minutes) 10

Attack

Average duration of successful attack, t^* (block time) 100

Fraction of miners participating, P/Q 0.51

Projected drop in exchange rate, l (coins) 0.30

Mining equipment

Fixed cost of equipment, F (dollars) 2100

Alternative use value of equipment, V (dollars) 0

Annualized flow cost, ε (dollars) 1350

Annualized cost of capital, r 0.20

Profitable attack?

Only when attackers can double-spend more coins than: 303070.05