Discussion of “The Economics of Cryptocurrencies - Bitcoin and Beyond” by Chiu and Koeppl

Discussant: Egemen Eren (BIS)

Economics of Payments IX

Basel, November 2018

“A bubble, a Ponzi scheme, and an environmental disaster”

https://www.ft.com/video/5716595f-4cde-43af-856c-cc2363eb0718?playlist-name=editors-picks&playlist-offset=2

Chiu and Koeppl on bitcoin

Disaster for welfare

“We estimate that the current Bitcoin scheme generates a large welfare loss of 1.4% of consumption.”

Can a better cryptocurrency be designed?

My message to young people: stop trying to create money!

“Central banks are trusted, and that trust is something they have built up over decades and for which there is no substitute right now. Trust is a valuable commodity. It is easily destroyed, but winning it takes time. Money has become established. Young people should use their many talents and skills for innovation, not reinventing money. It's a fallacy to think money can be created from nothing.” A. Carstens

https://www.bis.org/speeches/sp180704a.htm

Chiu and Koeppl

- There is nothing inherently wrong with cryptocurrencies.
- The current design is the problem.

- It is possible that the welfare loss can be lowered substantially to 0.08%.
- Optimal design:
  - Reduce mining
  - Rely on money growth (seigniorage) instead of transaction fees.

- Cryptocurrencies can potentially challenge retail payment systems provided scaling limitations can be addressed.

(Short) Summary of the paper

- Means of payment = Solving the double spending problem
- Focus on a single cryptocurrency.
- Competition to update (costly mining) and delayed settlement.
- Competitive mining, most results rely on $M \to \infty$

<u>Results:</u>

- With PoW, settlement cannot be both immediate and final.
- Optimal design: no transaction fees, only rely on money growth (seigniorage).
  - Intuition: Inflation tax shared by all, transaction fees only by buyers. Inflation allows distortions to be smoothed out across all buyers upfront. Hence, it is better.
- Cryptocurrencies better with retail than large value, DS incentives are larger in large value.

The model is good, what to make of it?

- Internally consistent model with interesting ideas.
- How realistic? What do we make of the results?

- All assumptions of all models are wrong.
- If you are making statements like welfare losses can drop to 0.08%, CCs can rival retail payments etc., this can be taken out of context.
- Be clear on what the assumptions are and how they are wrong.
- How can they change your conclusions?

Means of payment = solving double spending?

- How well can a cryptocurrency serve as a means of payment?
- They focus on the double spending problem.
- Being a means of payment is much more than solving the double spending problem:
  - In the model, miners are risk neutral and miner rewards deterministic. This is far from the data.
  - Are incentives of miners and end-users aligned? The more the merrier or the more the sorrier? (Shin (2018))
  - Many forks – not related to DS, what to make of this? Network externalities? Miners' and end-users' platform choices? Multiple CCs?
  - Why are there transaction fees at the first place? Block size?
  - How about dishonest sellers?
  - Price volatility.
  - Higher level point: cash solves the DS problem, declining as means of payment.

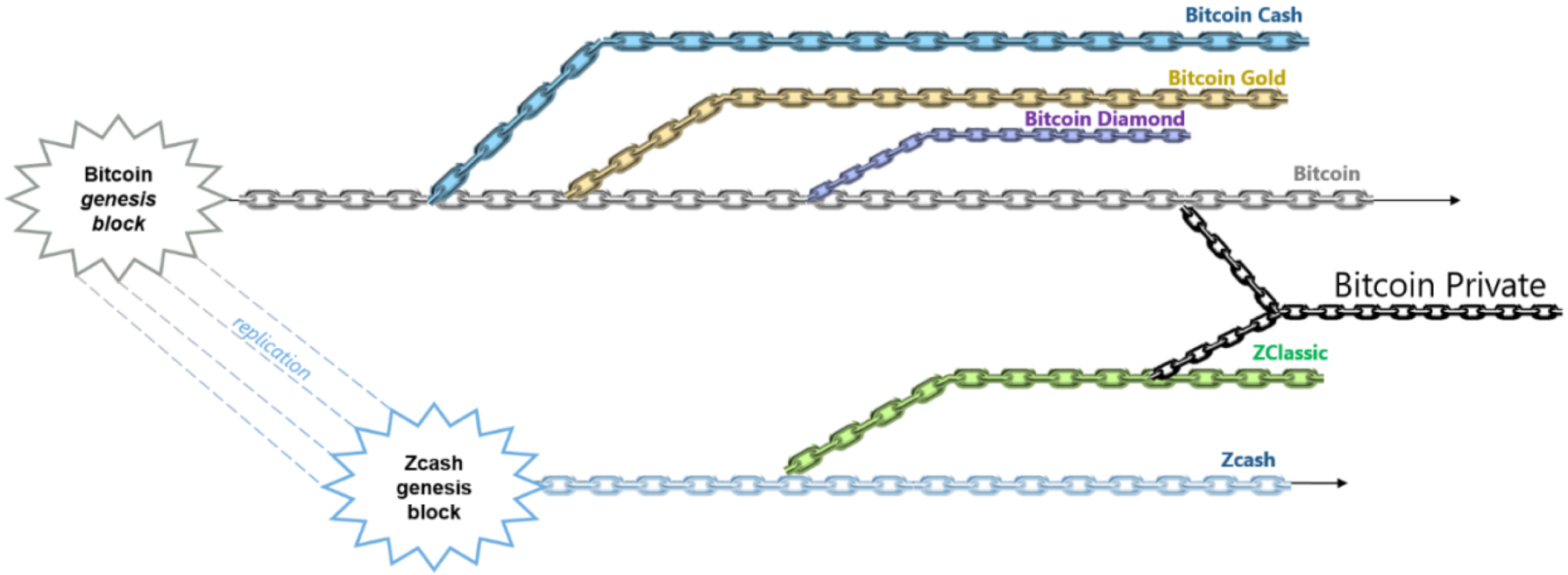
Is double spending the main issue?

- The model is based on a one-shot double spending attack.
- In reality, there are many forces that disincentivize DS attacks.

- First, competing cryptocurrencies and repeated game. Once the integrity of the CC under question, what is earned by DS could be worthless.
- Once a miner solves a block, others verify. Fraudulent blocks could be undone by other miners, provided they have enough CPU power.
  - If they don’t, then it is a problem for the CC at the first place.

A bigger problem: Forks and new CCs

Cryptocurrencies' family tree, selected cryptocurrencies — Diagram 1



Note: Blockchain blocks are represented as chain links. There are two initial blockchains: the original *Bitcoin* blockchain and the *Zcash* blockchain. The *Zcash* blockchain is a replication of the *Bitcoin* blockchain at its original block (genesis block). *Bitcoin Cash*, *Bitcoin Gold* and *Bitcoin Diamond* are *Bitcoin* forks, currently traded as independent cryptocurrencies. *ZClassic* is a cryptocurrency forked from *Zcash*. *Bitcoin Private* is a cryptocurrency forked from *ZClassic* and merged with a fork from *Bitcoin*.

A bigger problem: Forks and new CCs

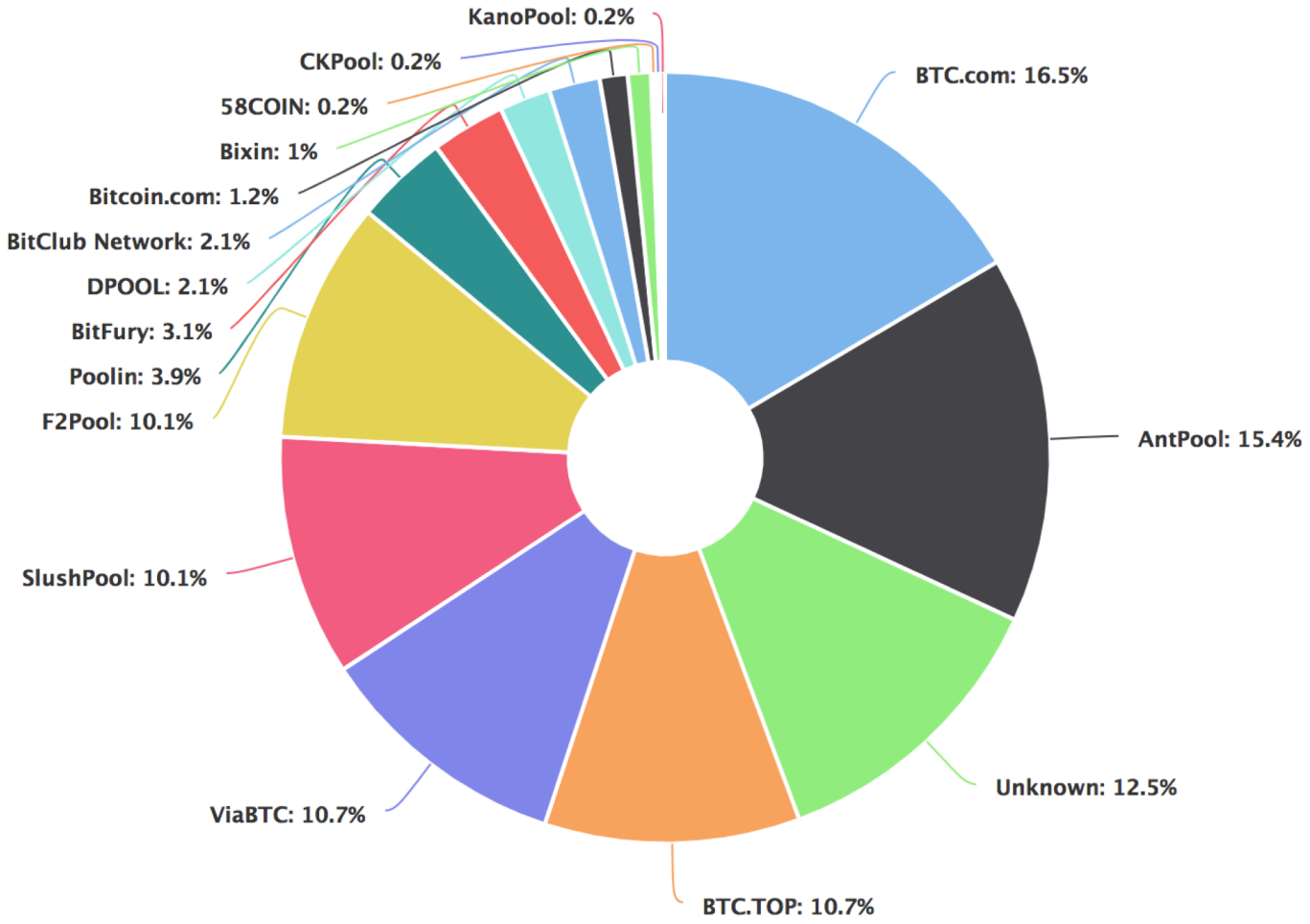
- The paper makes the point that once the scalability issues are solved CCs that solve the DS problem can be means payment.
- Even when scalability is solved, forks (or creation of new CCs) are inherent to CCs. Here to stay.
- If everyone coordinates on a different CC, all your savings could be worthless. Again, competing CCs is very important.

- The game between miners themselves, and miners and end-users is more complicated than modeled in this paper.

Are miners modeled correctly? Is what's missing crucial?

- Miners are risk neutral: In reality, risk averse hence the mining pools.
- Price is deterministic: In reality, fluctuates & huge speculative component.
- Most of the results are for M goes to infinity. They also suggest that this is a good assumption. It is not. Mining is extremely concentrated.
- M is not exogenous. M is an important endogenous variable to be solved for. e.g. Miners choose which CCs to mine.
- Costs are heterogenous across miners: Concentration? Dynamics?
- Competing cryptocurrencies and miners' incentives.

Mining pools: Hash rate distribution. M is not infinity.



Source: www.blockchain.com

Fees and block sizes: coordination vs congestion

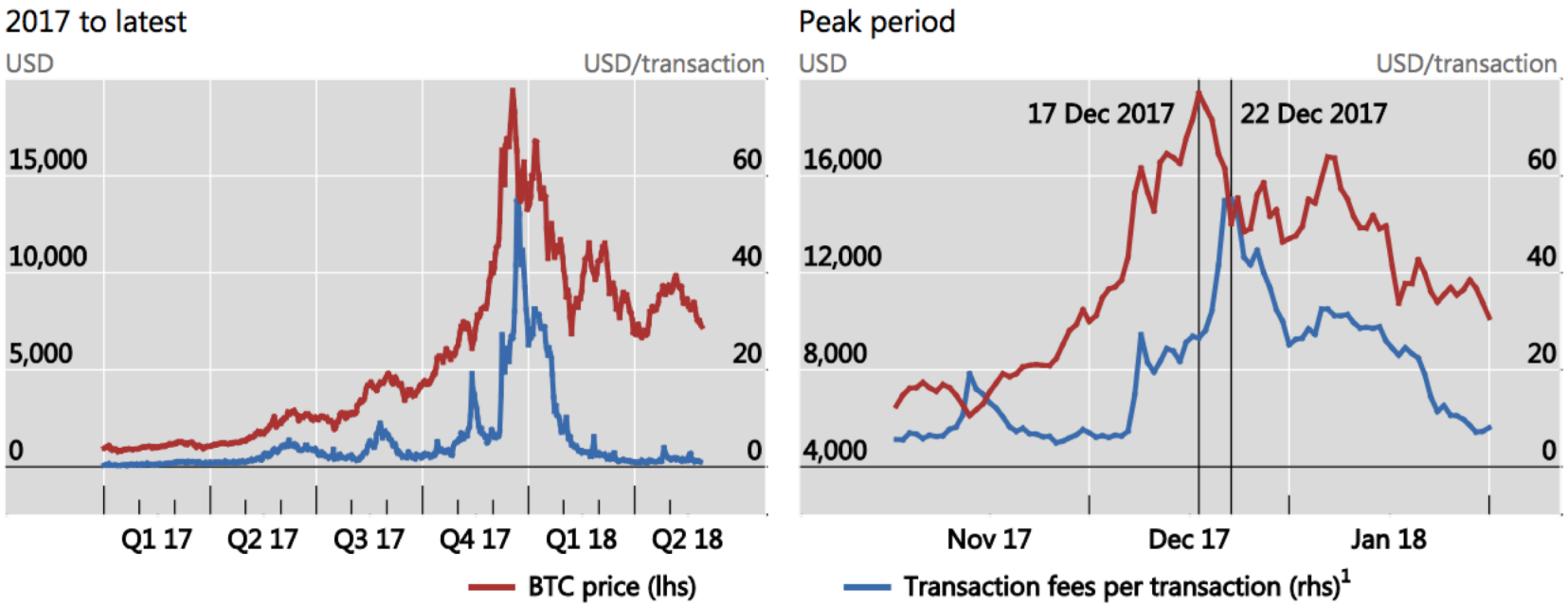
- In the paper, distinction between transactions & blocks not clear/realistic.
- Why are there transaction fees at the first place? Block size
- End-users compete to include transactions. Optimal block size?
- Once blocks are important, then limits to block size become an issue.
- This generates a game between miners and end-users.
- You want your transaction to be included, you are competing with others.

Transactions fees: to get ahead of the line

Bitcoin price and transaction fees[1]

In US dollars

Graph 1



[1] Total transaction fees in a given day divided by the number of daily confirmed Bitcoin transactions.

Source: www.bitinfocharts.com.

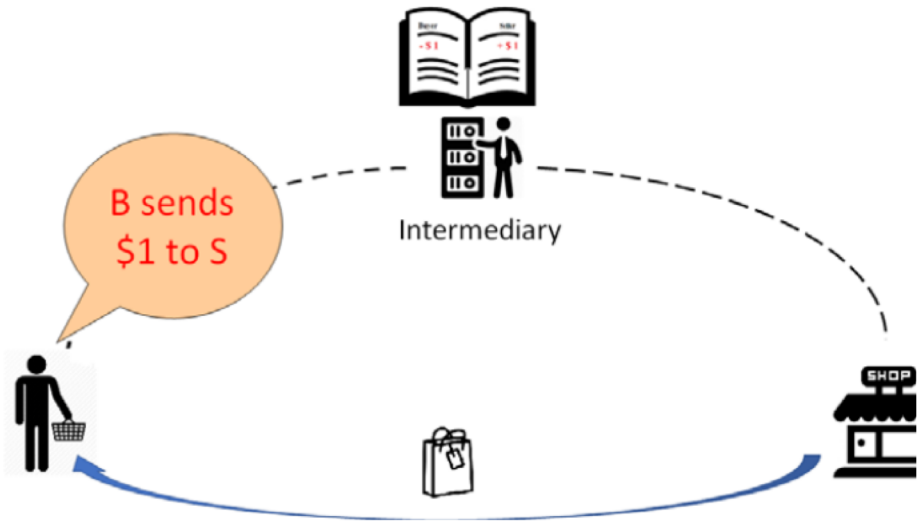
https://www.bis.org/speeches/sp180624b.pdf

Block size is an important design problem

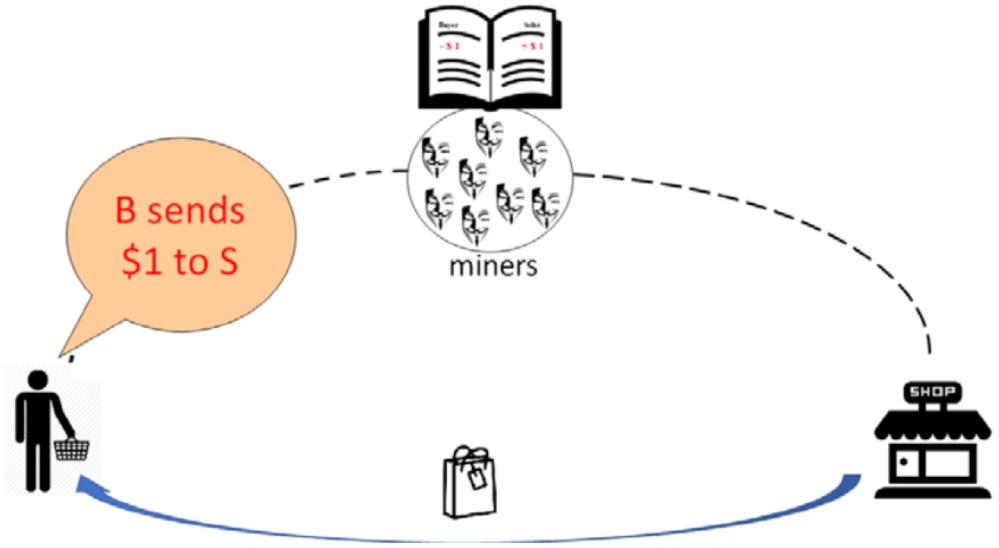
Source: Shin (2018)

The “double keeping” problem?

Digital tokens with a trusted third party (e.g. PayPal)



Digital tokens without a trusted third party (e.g. Bitcoin)



The flip side of the double spending problem

- Enforcement:
  - Buyer pays, it is assumed that the seller is honest.
- Current system is good because in case of fraud, you only have to convince the intermediary. Intermediary has the right incentives because of its franchise value.
- Bitcoin or decentralized cryptocurrencies: No solution to the “double keeping problem:” Seller keeping the money and goods.
- Footnote 14: a case in point. Only spot trades, and not DS-proof.

Conclusion

- I congratulate the authors to be among the first economists to address issues related to cryptocurrencies.
- Many extensions are possible (and some needed).
- My suggestions to the authors:
  - Motivate: why should we care about DS compared to other issues?
  - Take miners seriously. They are risk averse. There are mining pools. There is concentration. Heterogeneity in costs. Random component in prices.
  - Take end-users seriously. Transactions come in blocks (for a reason). They compete with each other to enter into a block.
  - Things like lightning networks claim that they solved the scalability problem. How does that compare to your optimal design?
  - Either extend the model or add a section listing caveats to your conclusions.