Ransomware Activity and Blockchain Congestion

by Konstantin Sokolov

Discussion by Emiliano S. Pagnotta

Imperial College London

2nd Toronto Fintech Conference, March 15, 2019

Outlook and Main Test

- Block space is limited and there is competition to add transactions to each block
- Ransomware attacks represent an **exogenous shock to settlement demand**
- Do these shocks affect other users? Is there crowding out of legit transactions?

Main Test

$$Y_t = \beta_1 Vuln_t + \beta_2 VIX_t + \beta_3 PriceBTC_t + \text{noise}_t$$

where Y can be

1. Total number of transactions
2. Transactions involving "regular" addresses: Top 100 addresses
3. Transactions involving "ad hoc" addresses: Rest

Main results

- R1: $\beta_1 > 0$ in the case of Total Transactions
- R2: $\beta_1 < 0$ in the case of Regular Transactions

Comments (1): Interpretation

1. Empirical results seem intuitive. But what is the precise economic question that we answer? The question should not be whether decentralized blockchains face an important scaling challenge

Comments (1): Interpretation

1. Empirical results seem intuitive. But what is the precise economic question that we answer? The question should not be whether decentralized blockchains face an important scaling challenge
2. R1: Would be the alternative hypothesis?
3. R2: "Endogenous" vs "exogenous" demand: perhaps more precise definitions?
    - E.g., liquidity shocks are less exogenous than attack shocks?
    - Voluntary vs attack-related demand seems more appropriate

- R2: Endogenous demand proxied by top 100 addresses (<5% total by transactions)
- Intuition: by-and-large these addresses belong to big exchanges. If so, we are capturing the effect of ransomware attack on demand for exchange services (a) Deposits: from BTC to fiat/altcoins (3) withdrawals
- Can we generalize conclusions to P2P transactions? (e.g., retail, remittances)

Comments (2): Specifications

- Previous analysis seems to equate number of transactions to congestion
  - Would like to see interaction between Vuln and observable controls related to congestion
- Good: paper also consider more direct measures of congestion as dependent variables: transfer fees and congestion time and effect of attacks is **positive**
- I would expand more on these
  - Percentage of full blocks
  - Mem pool size
- Alternatives to onchain settlement:
  - Paper considers exchange volume from Gemini
- Interesting to further explore more recent alternatives
  - offchain smart contracts (e.g., Lightning)
  - use of forked coins like BCH. Exploit SegWit adoption as experiment?