How costly is trust in the blockchain?

by Tyler Cowen *July 26, 2022 at 1:07 am in* **Economics**, **Web/Tech**

Eric B. Budish has <u>a new paper</u> on this topic:

> Satoshi Nakamoto invented a new form of trust. This paper presents a three equation argument that Nakamoto's new form of trust, while undeniably ingenious, is extremely expensive: the recurring, "flow" payments to the anonymous, decentralized compute power that maintains the trust must be large relative to the one-off, "stock" benefits of attacking the trust. This result also implies that the cost of securing the trust grows linearly with the potential value of attack — e.g., securing against a $1 billion attack is 1000 times more expensive than securing against a $1 million attack. A way out of this flow-stock argument is if both (i) the compute power used to maintain the trust is non-repurposable, and (ii) a successful attack would cause the economic value of the trust to collapse. However, vulnerability to economic collapse is itself a serious problem, and the model points to specific collapse scenarios. The analysis thus suggests a "pick your poison" economic critique of Bitcoin and its novel form of trust: it is either extremely expensive relative to its economic usefulness or vulnerable to sabotage and collapse.

I enjoyed these sentences:

> The intuition for why Nakamoto's method of creating trust is so expensive, relative to other methods of creating trust, is that Nakamoto's form of trust is *memoryless*. The Bitcoin system is only as secure at a moment in time as the amount of computing power being devoted to maintaining it at that particular moment in time.

Whether or not you agree with the arguments here, or maybe you think proof of stake will render them less relevant, it is nice to see academics (U. Chicago business school) making contributions to crypto debates.

And do you know what is excellent about this paper? At the end is an appendix "Discussion of Responses to this Paper's Argument." If you can't write one of those for your own paper, maybe nobody gives a damn!

Via the excellent Kevin Lewis.