What we have today is not Bitcoin but BINO

By Tim Swanson

Yesterday I was told by a China-based WeChat user that I was “hating on a technology” and “expending energy trying to destroy it.” It being Bitcoin. This is untrue, I like some of the ideas in Bitcoin (the protocol) circa 2009 and work daily with startups to create value in this space. However, what currently is called “Bitcoin” is a shell, at most, of its former self for at least two reasons, both of which illustrate a couple miscalculations by Satoshi.

The first and most important reason: Bitcoin and specifically, SHA-based proof-of-work, was irreparably ‘broken’ in July of 2010 by a German nicknamed ArtForz. He was the first person to figure out how to scale mining onto not just GPUs, but GPUs working within a farm (dubbed the ‘ArtFarm’). Several months ago I wrote a lengthy explanation of how he did it and how his farm evolved. Between July 2010 and January 2011 his farm accounted for (at its peak) around 25-30% of all network hashrate and he generated well over 100,000 bitcoins.

In December 2010, this scaling issue was further compounded by another European, Marek Palatinus who hails from The Czech Republic. He created the first mining pool, called Slush’s pool, which while still around, was later supplanted by dozens of other pools including notably, DeepBit, BTC Guild and GHash.io.

What this centralization 18 months after its launch ultimately led to was the removal of the relative-anonymity of miners because in order to effectively remain competitive with hashrate for seigniorage rewards, miners increasingly needed larger amounts of capital. Or as I repeatedly explain in chapter 3: due to the Red Queen effect, larger amounts of capital are needed to be expended somewhere to provide security and transactional capabilities (in the short run it has largely been through capital expenditures).

These larger units of capital requirements incentivized miners to seek new methods of funding, including tapping venture and private equity markets. In order to raise and receive these funds, the miners had to “deanonymize” themselves to the community and to investors thus removing a core pillar of how the network was intended to operate.

Thus, the decentralization consensus apparatus that Bitcoin depended on to functionally *be* Bitcoin no longer exists. What we have today is simply Bitcoin in name only (or BINO as I have refer to it).

In fact, rereading the Bitcoin whitepaper, one sentence in the abstract highlights the brokenness of this protocol today:

> Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

Today there are several trusted parties that the community hopes and trusts do not double-spend (including GHash.io and Discus Fish). Operators of the top three mining pools can simply call one another one the phone and collude to achieve this double-spend functionality over and above the vaunted 51% barometer (we should celebrate and learn from how GHash.io managed to do something that was thought to be impossible or impractical). They actually do contact one another through a variety of methods such as formalizing peering agreements for block propagation and agreeing to certain plans at industry-only meetings. As they begin to hire the protocol developers (to solve a public goods problem) this will continue to erode the separation of powers that was intended for a decentralized process.

Why would they double-spend? Perhaps when block rewards halve and miners become increasingly reliant on transaction fees for income, when users accidentally send extra-large fees, they could be incentivized to attack the network (e.g., censure and DDOS pools from propagating blocks with a high fee tx). For instance, last summer, an unknown user accidentally paid 200 bitcoins as a transaction fee to ASICMiner, a large mining farm in China. It thus may make sense (to farms or pools) to double-spend transactions with thousands of coins. Though, in that instance, such transactions will wait for tens of confirms and would not be the end of the world.

As the above scenarios roll out, if Bitcoin is “anti-fragile” then vocal adopters should have nothing to worry about. Yet as copiously shown throughout the book, it is not anti-fragile – it does not automatically strengthen in the face of adversity, someone has to fix it when it breaks. Or in other words, the trustless part of the experiment failed to reach escape velocity let alone achieve lunar orbit.

The human element and fees

The second, arguably slightly less important, reason for why Bitcoin became BINO is through the interjection of trusted third parties such as insurance, customer service and mandates in the form of Know Your Customer (KYC) and Anti-Money Laundering (AML) laws implemented by exchanges and merchants over the past two years. Again, before condemning the New York State Department of Financial Services or admonishing processors, consider the enormous amount of bad actors within the community that were “trusted” and ended up stealing or scamming vast quantities of bitcoins out of users – and the community “thought leaders” did nothing to stop it. No investor-led letter writing campaign or “town hall” meeting was done in the face of Mt. Gox’s entire existence (i.e., where is Scamworld crypto style?).

Many members of the community tolerated trusted third parties due to a variety of incentives that will continue to remain (e.g., convenience, speed, customer support). It also bears mentioning that holders do not need or are not required to use the payment processors to use bitcoin. Rather, they are providing optional services at the cost of privacy and trust.

Yet, if you artificially insert and add a trusted third part into the blockchain you remove its core advantage and it became the very thing it was trying not to be (and more expensive to do so).

Or as I mentioned in chapter 4 of *Great Chain of Numbers*, General Turdgison's memorable quote regarding "Plan R" which (un)intentionally was used to bypass authorization protocols and the chain-of-command to unilaterally drop nuclear bombs against the Soviets sums up this conundrum: "the human element appears to have failed here, but we'd hate to condemn an entire program based on a single slip up."

With that said, the transactional aspect of the network is still not primarily used for its strengths because of these edged case incentives. It was intended to distribute and decentralize trust and provide pseudonymity while processing these transactions. To do that you need numerous, geographically disparate, relatively-anonymous miners which is now a footnoted era. While Tor may be able to add that in the future, Tor's design creates additional lag time delaying the propagation of blocks which may increase orphan rates (see Jonathan Levin's research and Gavin Andresen's recent post).

As noted above, motivations to include KYC/AML percolated because of the enormous amount of thefts and scams that continue to propagate in the community, some of which involve the shoehorned use of bitcoin in retail payments. Again, Bitcoin was not created to reduce transaction *fees* in the retail payments sector but rather reduce overall aggregate transaction *costs* of compliance and mediation.

The very first paragraph of the white paper notes this:

> Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non- reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

Fast forward nearly six years later and this space is now peppered with trusted third parties (e.g., Coinbase, BitPay, Xapo, Circle) that offer insurance and customer support on the edges. They do this in part because holders are increasingly looking for more convenient, user-friendly solutions and because of the high level of scams and fraud that do not disappear just because a new network was made. To be balanced, these processors above do not directly provide a service comparable to the blockchain (or Visa) – to receive a payment holders only need to send to an address but in practice merchants do not normally do that because in this case they lose the possibility of automatic conversion into fiat. Consequently, because these are off-chain, users are essentially trading Coinbasecoins and Xapocoins (that is not inherently a bad thing).

Consumers want mediation and the ability to be repaid in the event fraud occurs. Thus each of these centralized organizations have cost structures, burn rates and profitability targets that have eventually have to be paid for, which could ultimately increase the transaction costs of their customer base. Currently, in addition to raising venture capital, these companies all rely on selling coins to liquidity brokers and exchanges and use the profits from the spread to fund operations (incidentally they also each operate as "dark pools" because it is unknown how they execute orders).

Continuing is the next paragraph from the introduction in the whitepaper:

> What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers.

In practice, the network internally appears secure yet it is the edges again where the fraud still occurs. While multisig escrow services are finally being implemented, in the interim it will unlikely remove all trust and counterparty risk for every situation on the other end of the network (e.g., merchants shipping broken fedoras and used alpaca socks).

How does privacy intersect with fraud? Towards the end of the paper, in section 10, Satoshi describes how privacy is attained:

> The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

Again, because between 15-30% of all mined coins have been stolen, seized, or destroyed (see chapter 12), insurance and customer support services have been added to the edge-based transactional process. Providing this requires funds and often depend upon users to deanonymize themselves.

Furthermore, nowhere in the paper does he claim that the transaction fees will be cheap or are cheap as some advocates claim. In fact, later in the incentives section for mining he notes:

> The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

One reason it is reasonable to guess that Satoshi was probably not in academia is because he had very few references or footnotes (or mathematical proofs). If he was planning to argue that "cheap" transaction fees were its competitive advantage, he would have said so here in that paragraph and would have referenced some alternative source to compare it with (e.g., Visa). Instead he does not and in fact later explained in the early FAQ that "When Bitcoins start having real exchange value, the competition for coin creation will drive the price of electricity needed for generating a coin close to the value of the coin." Or in economic terms, the marginal value of a coin equals the marginal cost of creating and securing it (MV=MC).

Again, bitcoin transactions are not cheap or even cheaper than incumbents specifically because decentralized networks require costly overhead; thousands of hashing systems are expending energy (technically exergy) that could otherwise be done in a cheaper, faster and more efficient centralized manner. To avoid using trusted third parties real costs are absorbed by the labor force of the network.

Decisions

The cartoon caricature of Bitcoin that some adopters vocally supporting is not Bitcoin; it is largely fan fiction. Bitcoin was not intended to be an asset or commodity – that is *not* something that Satoshi promoted in its early days. The money-like informational commodity aspect that enshrines bitcoin (the token) is an artifact, a byproduct of its deflationary, inelastic money supply. In fact, the title of the whitepaper is a *"Peer-to-Peer" Electronic Cash System* and the very first sentence of the abstract states that Bitcoin is, "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."

Satoshi wanted it to be used as money, by 2014, as shown by blockchain analysis most holders do not because it has poor modern attributes of money which was discussed at length in chapter 9, 10 and 11.

How to re-decentralize the mining process when economies of scale favor centralization?

Insurance, customer service, trusted third parties and KYC/AML are here to stay. That is the reality for users in the OECD and other jurisdictions. Furthermore, mining operations are not immune to capital expenditures needs that create a perpetual cycle of continual fund raising to tape out a new chip; and investors want to know who is manufacturing and potentially using those products.

Another China-based WeChat user also asked yesterday that if bitcoins are legally deemed property at the US federal level and the network were to sustain a double-spend attack by a VC-funded mining pool, would the SEC or other agency invoke legal punishment?

This is unknown but what is clear is that it is unlikely that any agency, governmental or not, could act fast enough to not only prevent it, but to somehow roll back the transactions that were conducted in a double-spend attack (this is called replevin). Maybe they could, but that would defeat the purpose of a blockchain, to be immutable. Irrevocability and irreversibility were the cornerstones of the project; the first section of the whitepaper alone uses the term "reverse" five times (Ryan Straus wrote an excellent piece last year that ties into *nemo dat*).

And again, it is not a matter of mining pools needing permission to participate or build blocks on a public network (e.g., see the permissionless meme). For instance, if a mining farm or pool in Finland or Ukraine (such as BitFury and GHash.io) built upon and created a longer chain than the chain recognized by Coinbase and thereby pulled off a double-spend of some kind, how could other institutions react in time before a cascading systemic issue rolled across the network (e.g., especially those relying on disproportional security rewards)? It was designed to route against such interference by being decentralized. If it can be coopted in that manner then again, it loses that checkmark feature (an issue recently encountered by NXT due to a hack at BTER).

What does this mean? Satoshi made three assumptions that did not pan out:

> 1) In November 2008, he assumed that botnets would be beneficial, but this simply accelerated centralization and squeezed out legitimate miners. Farms and pools exacerbated this.
>
> 2) Initially he assumed human institutions on the edges (trusted third parties) could and would not be able to do what they are able to do (intervention). Yet he clearly saw this problem in December 2010 in his last several public forum posts regarding Wikileaks (he did not want Wikileaks to accept bitcoins because he did not want to attract attention from the government).
>
> 3) Due to how the static block rewards were set up, he probably subscribed to a theory of economics that suggests deflation and inelasticity is good and would not impact the function of bitcoin as money. This is an empirical, measurable flop as it is not being used as money but rather instead as an asset or commodity. This was tackled in chapter 9 (remember, excessive reserves does not necessarily lead to large levels of inflation).

Knowing this false-starts, there are two directions adopters can take:

1) Continue trying to use and promote BINO for something it is continually handicapped at doing (e.g., being decentralized)

2) Work with what we have and build businesses around consumer behavior

As described in chapter 13, the first option comprises a number of individuals who build services such as mixing and coin washing in an attempt to provide some form of anonymity. Yet, mixers are an extra transaction cost and transaction fee to users that again, are negative sum. In addition, many consumers that use bitcoins for non-illicit retail payments and remittances do not use mixers (because of the hassle, speed and fees). Consequently, some of the holders that use mixers are those who need to, those with ill-gotten gains. Effectively developers of these tools are unwittingly creating getaway cars for thieves.

The second option is for those who realize the state of what BINO is and accept it, move on and build businesses that integrate with how the environment has evolved with (including trusted third parties and compliance) and around how consumers use the remaining parts of Bitcoin (as a ‘commodity’).

While it looks as if proof-of-work based on popular hash functions (SHA256, scrypt) will be forever ‘exploitable’ via economies of scale once the “market cap” (monetary base) of a coin reaches a certain fiat level that covers NRE, perhaps 2.0 projects like Hyperledger, Pebble, Tezos and Nimblecoin or spin-offs like Viacoin using tree-chains can provide similar functionality that Bitcoin intended to have. Or maybe PeerNova, Tadge Dryja (proof of idle) and Blockstream will prove this trend untrue.

Skeptical analysis and usage of data may make it seem that I am anti-Bitcoin or hate it, however, as shown above and in my books, this is not true. Unfortunately some advocates who are unfamiliar with what Bitcoin actually was, conflate the modern BINO doppelganger with pre-ArtForz Bitcoin. By ignoring the past and not confronting how the challenges crept up, advocates could continue fulfilling George Santayana’s dictum. Instead, explaining how and why we have reached this point, the industry can move forward, incorporating the lessons learned into productive enterprises and endeavors.