For Good Measure

Between a Block and a Hard Place

DAN GEER AND DAN CONWAY

Dan Geer is the CISO for In-Q-Tel and a security researcher with a quantitative bent. He has a long history with the USENIX Association, including officer positions, program committees, etc.
dan@geer.org

Daniel G. Conway serves on the faculty at the University of South Florida, where he teaches blockchain technology, analytics, and data science. He has previously also served at Notre Dame, Indiana, Iowa, and Northwestern. He can be reached at dconway@usf.edu.

That Rumbling Sound

If you have been living under a rock the past five years, you will still have detected increasing vibrations in your rock, perhaps even out and out warming, depending on the damping effect of your rock's material. If your rock is made of ideal material, then the repeated message in those vibrations has been clear. Otherwise, we will disintermediate the Fourier transform for you:

Bitcoin. Ethereum. Blockchain.

In this column, we examine the risk footprint of Bitcoin and other cryptocurrencies—not general risk, but risk in the computer security sense.

Debuting shortly after the fall of the iconic Lehman Brothers, and driven by global anti-establishment sentiment, the top 100 virtual currencies have now amassed a market value exceeding $500B, 35% greater than that of JP Morgan Chase (~$366B). Bitcoin itself is up over 100,000% in those five years past. All the numbers in this column were true as of the hour we turned the column in; you will, yourself, want to update them because all are volatile, to say the least. Go to http://geer.tinho.net/fgm/fgm.geer.1803.references.html for the full set.

While some of this movement might be reasonably classified as hysteria (the CryptoKitties game clogging up the Ethereum network, with the highest priced "cat" selling for $117,712; Bitcoin mining in the trunk of a Tesla; and a FuckCoin raising $30K in 30 minutes), dismissing the entire movement seems too easy—but how much is dismissing it like whistling past the graveyard?

Until this year, China had been the most active trader in Bitcoin, but then the government made it all but illegal. Japan is currently the most active trader, accounting for 43% of transactions, followed by the US at 29%, European countries at 8%, South Korea at 4%, and China at 1.6%. Both this year and last, and interestingly parallel, according to the World Intellectual Property Organization, technology patents are running at three million per year, and the four countries that account for 78% of BTC trading account for 78% of those three million patents: China 36%, US 18%, Japan 16%, and South Korea 8%.

But to the point, on Sunday, December 10, the Chicago Board of Exchange launched Bitcoin futures. The day CBoE "GXBT" was announced, 100,000 new accounts were created on Coinbase, which now claims over 10,000,000 users. India has approximately 30,000 users active at any moment.

What Do the Numbers Say?

Estimates of the number of detectible Bitcoin miners range from 5,000 to 100,000. The wide uncertainty range can be interpreted as the existence of discomfort regarding their discovery. The other 1355 cryptocurrencies, of course, have their own mining interests, and these are just the public blockchains. It is reasonable to believe that private, permissioned blockchains, such as those built on Multichain, will dwarf public blockchains in scale and variety going forward.

In round numbers, the current hash rate is 12M hashes per second to power 450,000 transactions per day, with transactions totaling $2B/day, an average transaction of $4,444. This compares to 704,000,000 credit card transactions per day totaling $54.8B, an average transaction of $77. The Federal Reserve ACH (Automated Clearing House) reports $86.7B/day in clearance, an average transaction of $1,680. To steal a line from the musical *A Chorus Line*, Bitcoin is "Too young to take over, too old to ignore; I'm almost ready, but…what…for?"

The growth rate for Bitcoin has been exponential, not linear, yet, according to Cisco estimates, overall peer-to-peer network traffic is not expected to grow at all through 2021, the smallest change of all network sub-segments, versus the leading subsegment, gaming, at 62% growth.

The annual electricity consumption of Bitcoin's proof-of-work has been variously estimated, but we'll go with 8.27 terawatt-hours per year. That is "less than an eighth of what U.S. data centers use, and only about 0.21 percent of total U.S. consumption… Global production of cash and coins consumes an estimated 11 terawatt-hours per year. Gold mining burns the equivalent of 132 terawatt-hours. And that doesn't include armored trucks, bank vaults, security systems, and such." So, one can plausibly argue that Bitcoin is a "green" technology [1].

Attack Surface

All new technology introduces new failure modes, that much is certain, but what is the proportionality constant here? Is it nodes, hashes, wallets, latency, or what? Bitcoin uses a peer-to-peer distributed ledger technology; integrating that ledger with the incentive structure to participate in the network, the attack surface then consists of several facets and edges, everything from the characteristics of peer-to-peer networking to that of wallet (private key) management.

Remember, peer-to-peer networks do not have a single point of failure based on IP addresses, but also understand that the mining operation is not uniformly distributed among miners. For example, 56% of Bitcoin mining is done using technology from AntPool in Beijing. As a different measure of concentration, if one were to disrupt the top-five mining pools, then one might be able to remove 70.4% of the competition. As yet another, "The top 100 Bitcoin addresses control 17.3 percent of all the issued currency. With Ethereum, a rival to Bitcoin, the top 100 addresses control 40 percent of the supply, and with coins such as Gnosis, Qtum, and Storj, top holders control more than 90 percent. Many large owners are part of the teams running these projects" [2].

In the meantime, the bounty for breaking into and modifying the "immutable" record of Bitcoin is the market cap itself: $500+B. As you probably know, that immutable record is based on elliptical curve encryption, i.e., discrete logarithm problems widely considered to be Computationally Hard and hash functions. So far, only 109-bit curves are known to have been broken, though there is some interest in understanding the random numbers used to pick initial private keys.

Bitcoin's incentive nature differs from that of BitTorrent—BitTorrent has a throttle system to restrict bandwidth to those freeloading. Bitcoin has no such self-repair facility. In fact, it is believed that 3.79 million bitcoins have been permanently lost (out of the 21 million that are the maximum number of bitcoins there will ever be), meaning the corresponding private keys required to access the bitcoins on the ledger have been lost, thus leaving those 3.79 million ledger entries orphaned. That makes the ultimate bitcoin pool size 18% smaller, and the single bitcoin 18% more valuable just for that reason alone. With a fixed upper bound on the number of bitcoins, you profit from causing other people to lose their private keys, and all without having to receive stolen property.

It's not as if those who exploit security flaws are too busy elsewhere to have noticed all this; Poloniex, a large marketplace, is warning customers not to use the app available through Google's store as they haven't created an app—it's malware.

Is Immutability a Good Thing?

EOS is a blockchain operating system that will be released in July 2018. Its ICO currently has a market cap of $4.6B. This puts it above Wendy's, Cracker Barrel, and MorningStar. That will add another layer to our security concerns.

In so many words, purported money is not the only thing that a blockchain can make immutable; by putting smart contract programs (code) on a blockchain, the code becomes immutable, and, with Ethereum and its Turing-complete language Solidity, we can trick the blockchain into executing updates by carefully using the equivalent of pointers. (Paging the Language Theoretic Security Group…)

Immutability, like anything else, is not without tradeoffs. As a case in point, Bitcoin is transparent as far as a history of what wallets have what amount of currency. Mapping those wallet addresses to IP addresses or user identities is likely not a great challenge today. In other words, blockchain immutability carries the same freight as biometric identifiers—there's no invalidating the information once revealed. (Monero is more challenging and that is so on purpose, but remember the first rule of any serious investigation: "Follow the money." What if you can't?)

All of this is perhaps too speculative, too dynamic, too ephemeral for a column on "security metrics," but our central point is that the faster the value-at-risk rises, the more certain it becomes that the structural advantage that offense has over defense will out. How these numbers change in the next year should offer some insight as to where perceived value is being pursued.

In any case, should you decide that being under your rock is not such a bad place after all, you still may want to consider investing in FortitudeCoin, which will give you priority to the survivalist community Fortitude Ranch, and thus purchase priority accommodations should your rock prove inadequate. We recommend you first make a sizable investment in our ICO "DanCoin," a fork off of FreeLunchCoin, before pursuing this path.

References

[1] Elaine O-u, "No, Bitcoin Won't Boil the Oceans," *Bloomberg View*, December 7, 2017: https://www.bloomberg.com/view/articles/2017-12-07/bitcoin-is-greener-than-its-critics-think.

[2] Olga Kharif, "The Bitcoin Whales: 1,000 People Who Own 40 Percent of the Market," *Bloomberg Businessweek*, December 8, 2017: https://www.bloomberg.com/news/articles/2017-12-08/the-bitcoin-whales-1-000-people-who-own-40-percent-of-the-market.