20 JULY 2018 / INSIGHTS

Crypto War Games: Imagining Decentralized Hostile Takeovers

Introduction

A recent uptick in literature surrounding the merging, acquisition, or takeover of crypto networks has sparked my interest. I had a brief stint working in corporate development / internal M&A so this subject is interesting to ponder when it comes to new network ownership models, tokenized economies, forking, and defensive tactics for projects.

What Does Hostile M&A Look

Like in Crypto?

A brief summary of traditional acquiring may be helpful for some. In this reading we will focus on stock-based acquisitions and not asset sales as stock acquisitions are the most aligned with crypto network takeovers. It will also help to talk specifically about public companies buying other public companies as their shares are traded in the public market, just like crypto networks. When Buyer Inc. wants to purchase Seller Inc. they approach the management & board of the company and come to an agreement, with the approval of shareholders, as to what the purchase price will be. Most of the time, save for some very rare occasions like a hostile takeover threat & other synergistic / long term growth ideas, the agreed price will need to be above the current price of the stock. This is pretty self-explanatory since shareholders usually don't enjoy selling their stock at a lower price than they need to.

Alternatively, Buyer Inc. can go ahead and initiate a hostile takeover attempt. If Seller Inc. rejects the original tender, Buyer Inc. can go directly to the public shareholders and begin a campaign to gain backers for a proxy fight in order to start replacing the board. Additionally, Buyer Inc. could go out and start purchasing a large chunk of outstanding stock in order to use it as a negotiating tactic. I encourage everyone to read about some of the more well-known hostile takeovers throughout history.

Looking at the above, crypto networks obviously operate a little differently. Crypto governance is still finding its place within the ecosystem and each blockchain operates a bit differently when it comes to voting, rule implementation, etc. With that in mind, there are a few different attack vectors for a takeover of a crypto-network, that is the ability to change development of the underlying protocol / project or 51% attack the mining network.

Mining Network Takeover

Let's first start with the 51% attack of the mining network of Bitcoin since it is a widely discussed topic and has a bit more research behind it. There are a few sources out there that estimate the **upfront** costs for a 51% attack range from ~$1.5 billion all the way up to ~$7 billion . Costs here vary widely and there is no verifiable number due to the unknown hardware pricing, availability, and cost of real estate to house the hardware. The more interesting factor is the ongoing cost of a 51% attack.

Joseph Bonneau's paper (referenced above) does a fantastic job outlining the four different methods for taking over a mining network as seen below:

		duration of control	
		temporary	**permanent**
source	**new**	Rent	Build
	existing	Bribe	Buy out

Table 1. Four basic strategies for gaining capacity in a Nakamoto consensus protocol.

Strategies for Renting, Building, Bribing, or Buying mining power

First off, Bonneau's paper was written when Bitcoin's hashrate was hovering around 10,000,000 TH/s which was the last 3 months of 2017. Bitcoin's current (July 12th, 2018) hashrate stands at roughly 3.5x that figure. With that in mind, assuming hardware prices have remained mostly level - which I think is a fair assumption as most GPU, memory, and ASIC prices have come back down to earth after their metoric rise at the start of the year - we can use the hashrate increase as a proxy for the required hardware cost. Additionally, ongoing energy costs have not drastically changed as far as I can see.

Assuming the above is fair, let's update Bonneau's numbers to today:

1. **Rental Attack on Bitcoin:** Amazon's EC2 Nvidia K80 chipset does not have an agreed upon hashrate from the experiments people have been running. One of the more seemingly reputable and recent experiments

stated ~275 MH/s/GPU on Amazon's EC2 K80 chipset for mining BTC. Let's move forward with that figure before I bore you anymore and drive myself any crazier trying to find a more agreed upon number. That would equate to ~127 million GPU's (35 billion MH/s divided by 275 MH/s) in order to have complete Bitcoin mining power. 51% of that would be ~65 million. Bonneau estimates about $1 / hour for each chip but I would hope Amazon would be charitable and give us a 20% discount on this large of an order so that would be $52 million / hour just to rent the hashing power needed. I am not able to find any details outlining Amazon's EC2 capacity but over 50 million GPUs might not be even possible. Considering one of these chips cost $1,900 at retail levels, it would be fair to say commercial prices are somewhere around $1,250 which would mean Amazon would have needed to / has invested $65 billion just for our order alone. Highly unbelievable considering Amazon's total fixed assets are only $48.8 billion and total assets are $131 billion.. TLDR: You probably can't rent the hashing power needed to 51% attack the Bitcoin network. You might be able to triangulate AWS, GCE, and Azure and get close but I don't think the hardware is even out there at this point.

2. **Building Attack**: We will be borrowing some ideas from the above attack vector but in a building attack, the attacker goes out and actually purchases the mining hardware (most likely ASIC chips, namely the Antminer S9i) and spins up a mining operation. With proper cooling, the S9i can cap out at around 13 TH/s which means the Bitcoin hashrate equates to roughly 2.7 million S9is. Assuming the same idea of needing 51% of the hashing power in order to "takeover" the chain through transaction verification restraints, this would equate to 1.35 million Antminer S9i's. S9i's retail, directly from Bitmain, for ~$700 ignoring shipping, tax, and customs costs. Let's assume that assuming the added costs of those factors are offset by a bulk purchase agreement so the $700 price point remains true, which also makes for easy math. Therefore, the upfront investment would be ~$961 million just to buy the hardware, this

ignores the land, cooling, real estate, internet connectivity, & infrastructure to support over a million miners. Lastly, there is the ongoing cost of running this many mining rigs. Gregory Trubetskoy still has one of the best walkthroughs for finding the cost of one Bitcoin and I will use the same process to find the hourly cost for the S9i. Assuming ~$0.05 KW/h energy prices - which I think is a fair average for industrial Chinese energy - and the S9i's power draw of 1,320W, the hourly cost is $0.066 / hour / per S9i. Therefore, the aggregate hourly cost would be $89,100. With all of the above in mind, a one hour "building attack" would be somewhere around $1 billion once you factor in the miscellaneous costs mentioned above.

3. **Bribing Attack**: A bribing attack is more abstract in nature. Miners, in theory, should verify the highest fee transactions in order to maximize their per block (average is around 1,500 right now) fee reward. Bonneau describes a process through which the attacker could pay a fee premium on a new branch of the chain in order to incentivize miners to come over to the new branch and abandon the main chain. My understanding of this process, which is admittedly limited, leads me to think that is just the act of a fork born from disagreement of protocol development i.e. BCH's disagreement of blocksize and the ensuing fork which caused some BTC miners to switch their hashing power over to the BCH chain. I would like to present a different idea through which high transaction "spoof" transactions could cause the legitimate transactions to never get verified out of the mempool and therefore cause many of the users to abandon the BTC network due to failing transactions. Right now, the Bitcoin network is averaging ~190,000 transactions per day. One really odd phenomenon is every 7 days, transaction volume falls by about 40,000 transactions as seen on the above chart. That investigation is for another time I suppose. Secondly, total transaction fees are hovering around $150,000 / per day recently. That would equate to an average of $0.79 / transaction in fees. It is important to note that Bitcoin is not a percentage based payment network like PayPal or trading networks. More specifically, I can send 1

BTC or 10,000 BTC for the same fee and they should arrive at roughly the same time. An attacker, in theory, could pump the mempool with extremely high fee transactions and therefore "crowd out" legitimate transactions. The difficulty here is building in what the actual transaction fees must be in order to make at least a majority of the miners verify those transactions only. Additionally, estimating how the market would react and bid up the initial mempool attack is nearly impossible to find without precedents. Admittedly, this model is a bit beyond the timeline and scope of this writing. More to come on that front at a later date. One closing thought here is regarding the idea of a combination of a bribing attack and one of the first two strategies where a party could attack the transactional network from two sides by using their hash power to mine their own spoofed transactions.

4. **Buyout Attack**: The buyout style of attack is a nice segway into the next section where I discuss the other attack vector: direct token takeover for centralized protocols. Bonneau has an especially noteworthy point:

> *For proof-of-work systems, the cost should be about half of the net present value of all future mining rewards. It appears that proof-of-stake systems are much more secure here, as the attacker must buy half of all value of the system, whereas with proof-of-work the attacker must only buy half of the future mining rewards (which should be less than the entire market cap).*

Before diving into this buyout strategy, my colleague, Matt Thompson, pointed out that Bitmain / Jihan Wu controls close to, if not more than, 51% of the mining power out there through both their affiliated mining pools or indirectly through Bitmain's hardware. Matt also noted that Jihan was integral within the BCH fork so there are some obvious incentives for him wanting to hurt Bitcoin in anyway possible in order to cause some / all of the market to shift over to his Bitcoin Cash fork.

For the time being, let's assume a different party wanted to execute a buyout attack on Bitcoin. As Bonneau notes above, miners will only continue to operate, or start a new operation, if the present value of the future expected mining rewards outweighs the current or upfront costs. The same is true within a buyout of any of these firms. Bonneau also adds:

> *If an attacker can credibly commit to buying out half of all capacity and using it to destroy the system, current owners will have a strong incentive to sell to avoid being left in the 49% which does not sell and ends up holding worthless capacity*

This is an especially interesting point, that will also be touched on in the next section surrounding direct token buyouts, in that there is a "critical mass" a buyer can reach in order to scare the remaining sellers to sell at a discount in order to avoid being left in the 49% camp. On the other hand, if the mining market was able to learn about this roll-up before it reached a meaningful market share, the remaining miners could pledge to not sell in order to defend the market against the 51% attack. This gets into a bit of game theory since one sizeable seller could sell out for a premium to defend themselves and destroy the entire strategy. PoS systems are especially susceptible to this type of attack since the staking assets will become worthless post-attack where as PoW hardware still, arguably, has value post-attack.

Direct Token Takeovers

The second attack vector for parties wanting to take over a crypto network would be direct token acquisition. Depending on governance models (which I encourage everyone to learn a bit about here, here, here, and here) token holders, or users, have a say on development and code adoption throughout the network. Most notably, Decred's hybrid governance system is a hot topic today through which users have pseudo-veto power over the mining network.

The initial response I got from many people when I brought up this idea was, "any takeover victim can just fork the asset." For many cases, this may very well turn out to be true. A real world example could be the ETC fork post DAO where the ETC community didn't believe in the rollback of the chain that Vitalik and team enacted. More abstractly, if Buyer Inc. wanted to take over Seller Inc. and their chain / cryptoasset and the community didn't believe in the mission or strategy of Buyer Inc., they could fork the asset away from the acquired chain.

Unlike in traditional equity markets, where, most of the time, shareholders are happy to sell their shares at an acquisition premium somewhere above the current market rate. There might be some push back if the shareholders believe that their stock will be worth more within their investment horizon time period and will vote to reject the acquisition. It is also important to note that most public companies only float about 9.5% of their total equity. The rest is held by the company within stock option plans, restricted stock, or treasury.

Utility token holders, on the other hand, may reject an acquisition offer because the purchaser may wipe out the product through which their token derives utility value. In the current state, unfortunately, many token purchasers (especially those that participate in ICOs) are buying these tokens from a speculative investment perspective rather than a usage one.

M&A would differ greatly depending on whether the buyer was a financial buyer (PE, activist investor, family office, etc.) or strategic (competitor, up / down stream company, etc.). Financial buyers would need to convince current token holders that a fork would not be beneficial and could utilize airdrops or market selling action on the forked asset to combat this action. On the other hand, strategic buyers would need to tell a compelling enough story about the combined chains, projects, assets, and product in order to convince Seller Inc. token holders to sell their asset or fork into Buyer Inc's asset.

Hostility from both buyer types could come from the selling of the forked asset

and then using those proceeds to partially fund the buying of the takeover token.

Looking Forward

M&A within the industry has already taken place on the centralized / corporate level with Coinbase's purchase of Paradex and a number of broker dealer firms along with Circle's acquisition of Poloniex. To my knowledge, a protocol level takeover is yet to be seen.

I am looking forward to writing more on "poison pills" takeover targets could implement along with other defense mechanisms. It will also be interesting to watch how the market prices, trades, and reacts to these token-based acquisitions when they do come.

— Coinigy Insights —

insights

Stacking Up Coin and Equity Offerings

1 post →

Wallet Tracking for XVG, ADA, QTUM, ZEN, CPC, LSK, IOTA, NANO, and XEM Now Available on the Coinigy Platform

Wallet tracking for the following coins/tokens is now available on the Coinigy platform: Verge (XVG) Cardano (ADA) Qtum (QTUM) ZenCash (ZEN) Capricoin (CPC) Lisk (LSK) IOTA (IOTA) Nano (NANO) NEM (XEM) In

1 MIN READ