The Stateless Currency and the State:

An Examination of the Feasibility of a State Attack on Bitcoin

COS 598b

Professor Arvind Narayanan

May 13, 2014

By Andrew Kim, Daryl Sng, Soyeon Yu [1]

[1] We extend our appreciation to Edward Felten, Jerry Brito and Michael Taylor for their time and willingness to discuss key aspects of this paper with us.

This paper explores the feasibility of a state-led attack on Bitcoin and other similar electronic currencies, or cryptocurrencies. After a brief overview of how Bitcoin works, this paper discusses the unique characteristic of the state and its ability to attack Bitcoin exogenously (as a regulator and a governing authority) and endogenously (as a participant in the Bitcoin system). We then discuss the different kinds of endogenous computing power-based attacks a state could deploy. Our research demonstrates just how feasible such attacks would be for a state to execute. Lastly, we discuss the implications of the surprising feasibility of a state attack on Bitcoin.

Bitcoin and the Mixed Blessing of Decentralization

Explanations of how Bitcoin works of varying levels of technical detail are widely available. For the purposes of this paper, we briefly review the basics of what Bitcoin is and how it works. From there, we consider how the system's unique decentralized nature affords certain benefits, but is also the root of some of its fundamental vulnerabilities.

Bitcoin Basics

Bitcoin is a form of electronic currency that leverages cryptographic technology to function in a decentralized, peer-to-peer manner. Invented in 2008 by

the anonymous entity Satoshi Nakamoto[2], Bitcoin rose to prominence because of its innovative approach to (ostensibly) resolving what is known as the double-spending problem independent of a trusted third party authority.[3] When one spends cash, it is simply spent; that is, when a specific physical bill is used to purchase one good, it cannot also be used in a separate purchase at the same time. Electronic currency, however, is not tied to a specific physical object. Rather, it is stored in the form of data, which can be easily replicated. As such, double-spending electronic data essentially requires nothing more than making a copy of that data and sending it to two separate vendors. To be sure, one could "double-spend" cash by creating counterfeit copies, but the double-spending problem with electronic currency is all the more salient because copying data requires almost no additional effort. Furthermore, copied data, unlike counterfeit bills, is literally indistinguishable from the "original."

As Jerry Brito points out, the traditional solution to this problem of double-spending with electronic currencies was to trust a central third party, e.g. a bank or credit card company, to maintain the authoritative record of all legitimate transactions.[4] Bitcoin, however, eliminated the need for such a third party by distributing the burden of maintaining that authoritative record of transactions across a decentralized network of "miners."[5] Mining in Bitcoin, as the original

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System"
[3] Jerry Brito and Andrea Castillo, "Bitcoin: A Primer for Policymakers," 4.
[4] Jerry Brito and Andrea Castillo, "Bitcoin: A Primer for Policymakers," 4.
[5] Satoshi Nakamoto's original paper "Bitcoin: A Peer-to-Peer Electronic Cash System" outlines the technical details of how Bitcoin uses cryptography; for our purposes, we will focus more on the implications of Bitcoin's distributed, decentralized infrastructure than on the technical innovations beneath the system. Joshua A. Kroll, Ian C. Davey, and Edward W. Felten also provide a helpful explanation of how Bitcoin works in "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries."

meaning of the verb implies, is the process of minting new Bitcoins into existence. Less intuitively, however, mining is also precisely the process by which legitimate transactions, grouped into "blocks," are added to the authoritative record, or what is called the "block chain." Successfully adding a block, then, involves grouping the latest transactions with the existing block chain and inputting that data into a cryptographic puzzle (i.e. a hash function). The first miner to find a solution to that puzzle, i.e. the version of that puzzle that contains the data of the latest transactions, is then recognized by her peers to have created a legitimate block. The legitimacy of this block grows as miners include it as part of the block chain in their attempt to add subsequent blocks containing the next batch of transactions.

The cryptographic puzzle is designed to adjust its difficulty such that new blocks are created, on average, every 10 minutes. Miners are incentivized to engage in mining (and therefore legitimizing new transactions by adding them to the block chain) by being awarded a fixed amount of Bitcoins with each successfully added block. Originally, that reward was 50 BTC per block. It has now halved to 25 BTC and will continue to halve every 21000 blocks.[6] This will continue until 2140, when the total supply of Bitcoin is projected to reach its maximum supply of 21 million BTC, and the mining reward will be reduced to 0.[7] As the system approaches this point, it is thought that miners will charge higher transaction fees to make up for the diminishing rewards.[8]

---

[6] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries," 5

[7] Bitcoin Wiki, "Controlled Supply," https://en.bitcoin.it/wiki/Controlled_supply.

[8] Ken Tindell, "Geeks Love the Bitcoin Phenomenon Like They Loved the Internet in 1995," *Business Insider*, April 5, 2013, http://www.businessinsider.com /how-bitcoins-are-mined-and-used-2013-4.

The Problem with Decentralization

Because mining takes the form of computational problem solving, mining power is proportional to computational power, and, therefore, computational power is proportional to one's ability to influence which blocks get added to the block chain. Unlike an electronic currency scheme that employs a central authority to decide which transactions are legitimate and which are not, Bitcoin distributes that authority in the form of computing power. Therefore, where centralized schemes require trust in the central authority, Bitcoin requires trust in the idea that the majority of mining power will be aimed at adding legitimate blocks to the block chain.

There is no guarantee, however, that mining power will be directed toward those ends. Miners can disagree on which version of the block chain to codify as legitimate, and thus branches can form. As Kroll, Davey, and Felten note: "miners vote for a branch by devoting their mining effort to extending it, and the Bitcoin rules say that the longest branch should be treated as the only valid one."[9] Consequently, it is not necessarily some objectively '*legitimate*' branch of the block chain that wins out, but rather the one with more mining power behind it.

The role of trust, therefore, is not done away with in Bitcoin but merely repackaged. Even though a centralized electronic currency carries the inherent risk

[9] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries," 5

of a self-interested arbiter, a decentralized scheme like Bitcoin carries the inherent risk of a malicious actor (or group of actors) amassing sufficient mining power. There is no predetermined central authority in Bitcoin, but the possibility of one emerging is ever present. Moreover, because the power to change Bitcoin rules of operation and infrastructure is also decentralized, it is inherently less nimble than a centralized system, wherein the central authority could unilaterally change the parameters of the system to adjust to attacks.

Types of Bitcoin Users

A diverse range of entities currently compose Bitcoin's user base, and each type has its own nuanced reasons for partaking in and supporting the survival and promotion of Bitcoin. Such entities include individuals who distrust existing government and financial institutions, particularly in the aftermath of the 2008 financial crisis. Another community is comprised of individuals who are concerned with privacy and are attracted to Bitcoin's pseudonymous[10] features. There is a spectrum of investors and venture capitalists, who on one extreme see Bitcoin purely through a speculative, opportunistic lens and on the other end foresee Bitcoin becoming a resilient and widely adopted currency of the future. And finally, there are hobbyists, who are simply drawn to Bitcoin's novelty. Across these different user groups, commitment to the survival of Bitcoin in the face of an

[10] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating User Privacy in Bitcoin. In Proceedings of Financial Cryptography, 2013.

attack will also vary. Defining the exact make-up and interests of these Bitcoin user communities remains an area for further research.[11]

Types of Attackers

Before we expanding on *how* attacks can be conducted on Bitcoin, we will first discuss *who* would want to and why.

Private Attackers

The adversary envisioned in the existing literature typically assumes a private entity—either an individual miner or pool of miners—motivated by economic gain or some unspecified ideological cause.[12] Because any attack that undermines faith in Bitcoin would devalue Bitcoin—and therefore undermine the economic incentive of the attack in the first place—the economic gain from an attack must be realized outside of Bitcoin. For example, an economically motivated attacker might have a major short position in Bitcoin, in which case she would benefit from a Bitcoin devaluation. This type of attack has been modelled by Kroll, Davey, and Felten in what they call the "Goldfinger Attack."[13]

[11] Lui Smyth conducted an initial demographic survey of 1,000 Bitcoin users, suggesting that the average Bitcoin user is "male (95.2%), 32.1 years old, libertarian / anarcho-capitalist (44.3%), non-religious (61.8%), with a full time job (44.7%), and is in a relationship (55.6%)": http://simulacrum.cc/2013/03/04/the-demographics-of-bitcoin-part-1-updated/

[12] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries," 6-10.

[13] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries," 13.

Other motivations of a private entity might include destroying Bitcoin for ideological reasons, but it is difficult to imagine what kind of private entity would be sufficiently dedicated, resourced, and secure to successfully amass the computing power necessary to execute a truly destabilizing attack. For a private entity, Bitcoin mining hardware is expensive, and given that it would be fairly easy to identify anyone amassing the hardware necessary for an attack capability, she would likely be stopped before irreparable damage were done. The economic incentives modelled in the Goldfinger Attack seem most compelling, but even then, the limitations of a private individual seem to render such an attack unlikely.

State Attackers

The interests and capabilities of a state, however, differ from those of a private entity. A state is less likely to attack Bitcoin for a one-off economic profit—in fact, doing so would likely trigger reactions from other states (such as restricted trade relations and even economic sanctions) that ultimately damage its economy. Rather, a state might consider attacking Bitcoin in order to counter perceived threats to its national security. For example, should Bitcoin proliferate to the point that it eclipses a state's own national currency or lead to a threatening increase in what the state considers illicit activity, a state may perceive Bitcoin as weakening its control over its own domestic affairs. Already, states impose a wide range of limitations on financial transactions: the United States controls money laundering,

financing of nuclear proliferation and terrorist financing; China has capital controls in place to regulate flows of capital in and out of its capital account and prevent the renminbi from being fully convertible. Conversely, states might co-opt Bitcoin manipulation as an offensive tool, particularly if one among two belligerent states is more reliant on Bitcoin than the other. The threat of attacking Bitcoin, therefore, could conceivably become another means of coercing states whose economies become disproportionately reliant on the cryptocurrency.

State reactions to Bitcoin have thus far been apprehensive and incomplete, and among legal and regulatory commentators, there is a sense that further government action is on the way.[14] So far, the U.S. government seems to be avoiding regulation of the Bitcoin infrastructure itself while attempting to regulate the entities that use it.[15] Indeed, even in the aftermath of the infamous Silkroad crackdown, the U.S. government focused its prosecution on the Silkroad platform as opposed to Bitcoin itself.[16] While the IRS's designation of Bitcoin as property have caused anxiety in some quarters[17], the announcement has been generally welcomed for introducing some regulatory clarity and further validating the notion "that Bitcoin is becoming recognized as an innovative technology."[18]

---

[14] Peter J. Henning, "More Bitcoin Regulations Is Inevitable," *The New York Times,* 3 February 2014. http://dealbook.nytimes.com/2014/02/03/more-bitcoin-regulation-is-inevitable/

[15] Edward Felten, conversation on 29 April 2014.

[16] Nicolas Christin, Raine Bohme, and Sarah Meiklejohn, "Economics and Bitcoin Panel," *Bitcoin and Cryptocurrency Research Conference* at Princeton University, 27 March 2014, min. 58:00

[17] Alex Hern, "Bitcoin is legally property, says US IRS. Does that kill it as a currency?" *The Guardian,* 31 March 2014. http://www.theguardian.com/technology/2014/mar/31/bitcoin-legally-property-irs-currency

[18] John D. McKinnon and Ryan Tracy, "IRS Says Bitcoin is Property, Not Currency," *The Wallstreet Journal,* 25 March 2014. http://online.wsj.com/news/articles/SB10001424052702303949704579461502538024502

Beyond the United States, there are several countries where the regulatory environment is somewhat more hostile. According to BitLegal, an interactive map that classifies the Bitcoin regulatory environment by country as either permissive, contentious, or hostile, two countries (Iceland and Vietnam) have been labeled as hostile, while seven others (China, India, Kazakhstan, Jordan, Mexico, Russia, and Thailand) have been labeled contentious.[19]

While the recent string of restrictive Bitcoin policies in some states by no means implies an impending state-led attack, it is worth noting that states have indeed manipulated—and destroyed—other countries' currencies in the past for national security reasons, most commonly through circulation of counterfeit currencies. (This is distinct from state-sponsored counterfeiting done to acquire the 'funds' to finance its operations, since the counterfeiting state in such instances wants people to retain their trust in the currency.) For example, the U.S. poured vast amounts of counterfeit dinars into Iraq following the first Gulf War in order to cripple the Iraqi economy and destabilize the Saddam Hussein government[20], while the German government attempted to destabilize the British economy in World War II through its 'Operation Bernhard' counterfeiting operation. [21] To be sure, Bitcoin is not directly associated with any single state. However, in an era when states are no longer the only type of actor in the international system, it is not inconceivable for a state (or group of states) to become actively hostile toward a decentralized

[19] Map and index on Bitlegal.net.
[20] Youssef M. Ibrahim, "Fake-Money Flood Is Aimed At Crippling Iraq's Economy" , *New York Times*, 27 May 1992. http://www.nytimes.com/1992/05/27/world/fake-money-flood-is-aimed-at-crippling-iraq-s-economy.html
[21] Lawrence Malkin, *Krueger's Men: The Secret Nazi Counterfeit Plot and the Prisoners of Block 19* (New York: Little, Brown and Company, 2006)

electronic currency like Bitcoin with features attractive to the brokers of illicit activity and perhaps even terrorist networks or separatist movements.

Types of Attacks

Unlike private adversaries, a state can attack Bitcoin *exogenously*—that is, by changing the regulatory environment Bitcoin exists in without engaging as a participant of the Bitcoin system. This form of attack would be fairly straightforward and come in the form of regulation and/or legislation, such as some extreme version of China's existing rule that bars financial institutions from processing transactions in Bitcoin. [22] More interesting, however, is how a state might attack Bitcoin *endogenously*, that is, as a participant. In this section, we focus on these endogenous attacks, focusing on three forms of attacks that a state could execute by amassing sufficient mining/computing power: the 51% attack, the feather-fork attack, and the selfish miner attack.

The 51% Attack

Any would-be attacker that controls more than 50% of the overall network's computing power can, for the time that she is in control, exclude and modify the ordering of transactions. This attack, known as the 51% attack, allows the attacker

[22] "China Bans Financial Companies From Bitcoin Transactions", *Bloomberg News*, 5 December 2013. http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html

to: i) reverse transactions that she sends while controlling a majority share of the computing power, allowing her to double-spend transactions that previously had already been seen in the block chain; ii) prevent any transactions from being confirmed; and/or iii) prevent other miners from mining any valid blocks.[23] In effect, the attacker could effectively stop all payments and shut down the network. (With less than half of the computing power, a would-be adversary could mount the same kind of attack, but with less than a 100% rate of success. For example, an attacker with only 40% of the network's total mining power can prevent a 6-deep transaction from being confirmed with a 50% success rate.) A successful 51% attack has taken place before on Feathercoin, another cryptocurrency.[24]

The 51% attack could cause a loss of faith in a cryptocurrency. The recent concentration of Bitcoin's mining power in a few mining pools resulted in fears of an inadvertent situation where a single pool controls more than half of all computing power, and corresponding actions to guard against a loss of faith in the Bitcoin network. For example, in early 2014, after the mining pool ghash.io reached 42% of the total Bitcoin computing power, a number of miners voluntarily dropped out of the pool and Ghash.io issued a press statement to reassure the Bitcoin community that it would avoid reaching the 51% threshold[25].

[23] It is also worth noting the limits of a 51% attack. Even with a successfully mounted attack, the attacker cannot create coins out of thin air or change the number of coins generated per block, nor can she send coins that she does not possess, prevent transactions from being sent at all, or reverse other people's transactions.
[24] Danny Bradbury, "Feathercoin hit by massive attack", *Coindesk*, 10 June 2013 http://www.coindesk.com/feathercoin-hit-by-massive-attack/. For a study of the technical details of the 51% attack on Feathercoin, see MaxMiner, *Feathercoin's 51% Attack - Double Spending case study*, June 2013 http://maxminer.files.wordpress.com/2013/06/ftc_51attack.pdf
[25] According to the press release, "Ghash.io will take all necessary precautions to prevent reaching 51% of all hashing power, in order to maintain stability of the bitcoin network." In https://ghash.io/ghashio_press_release.pdf

One of the arguments against the possibility of a 51% attack on Bitcoin is that there is little profit in doing so: taking control of the network would only net a small profit in the window before the attack is obvious, and if sustained, the resulting lack of trust in the network would cause the value of Bitcoins to fall, thereby negating the economic incentives to mount such an attack. Another argument is that a 51% attack would be easy to detect and therefore easy to defend against, through the quick rewriting of Bitcoin rules to exclude such attacks. Gavin Andresen, Chief Scientist at the Bitcoin Foundation, has stated that "if a 51% attacker stopped including all broadcast transactions in blocks 'we' would quickly figure out a rule or rules to reject their blocks"[26]. In response to a query in 2014 about the possibility of a sovereign 51% attack, Andreas Antonopoulos, Chief Security Officer of Blockchain, answered that the community could simply change the mining algorithm on the fly to render the attackers' investment a waste.[27]

A third line of argument stems from the belief that a single malevolent actor cannot outpace the production of the entire ASIC industry, or from the libertarian view that governments cannot out-innovate the free market. Finally, another argument is that a state would not have any reason to do so, or that a state would choose its traditional powers of regulation.

In the following section, we take on the arguments above, and postulate that the Bitcoin community has not paid enough attention to the potential for a state

[26] Gavin Andresen, "Taking Down Bitcoin" thread, bitcointa.lk, 29 April 2012. https://bitcointa.lk/threads/taking-down-bitcoin.51231/page-2#post-822208
[27]Ryan Selkis, "Spreading FUD Week: A Sovereign 51% Attack", The Two-Bit Idiot http://two-bit-idiot.tumblr.com/post/79998098398/spreading-fud-week-a-sovereign-51-attack

to sponsor a 51% attack on Bitcoin. The Bitcoin wiki simply states that "Since this attack doesn't permit all that much power over the network, it is expected that no one will attempt it" and that "even someone trying to destroy the system will probably find other attacks more attractive"[28]. Andresen has written in an online forum discussion that "there are much higher priority things on my TODO list; I don't think a 51% attack is likely."[29] As our calculations below show, a 51% attack is, at present, relatively cheap for a state to mount, and might not be able to be defended against by the Bitcoin community. This would have lasting effects not just on faith in Bitcoin but on cryptocurrencies in general.

Feather-Fork Attack

Another form of computing-power based attack is the feather-fork attack, discovered by Miller[30], which allows an attacker to influence the network using much less than 50% of the total computing power. Under a feather-fork attack, an attacker that controls fraction α of mining power (where $\alpha < 100\%$ of total hashpower) could attempt to blacklist transactions from a particular address, by announcing that he would treat blocks that include forbidden transactions as non-existent and try to mine against it while treating other blocks as valid. The attacker would succeed in mining against the block with probability α^2, while the forbidden block would survive with probability $1-\alpha^2$. The attacker has in effect increased the

[28] Bitcoin wiki, "Weaknesses". https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power
[29] Op. cit., Andresen.
[30] Andrew Miller, "Feather-forks: enforcing a blacklist with sub-50% hash power" thread, BitcoinTalk, 17 October 2013. https://bitcointalk.org/index.php?topic=312668.msg3353004#msg3353004

transaction fee for including a blacklisted transaction by $\alpha^2 U$, where U is the average block reward (currently 25BTC). As α increases, the transaction fee for including blacklisted transactions in a block increases.

In this situation, the failure of an attack is costly and reduces revenue, since it results in wasted mining. Therefore, for the attacker's threat to be credible, it needs to demonstrate, first, that it is capable of doing the attack (such as by successfully carrying out the attack once), and that it is willing and able to commit itself to the attack, at cost to itself. Once the attacker establishes itself as a credible threat, there is an incentive for other miners to go along with the attack and reject certain blacklisted transactions. Alternatively, those involved in blacklisted transactions could be forced to increase their transaction fees. Combined with the imperfect anonymity of Bitcoin (since Bitcoin requires public keys), a feather-fork attack could allow governments to blacklist certain categories of transactions (e.g. a state could shun transfers to particular businesses, or could say "transactions above X value have to be registered with the government").

Selfish Mining Attack

Lastly, as outlined by Ittay Eyal and Emin Gun Sirer, an attacker could launch a selfish mining attack, in which a prospective attacker keeps its discovered blocks private and then intentionally forks the block chain. In this case, the attacker would mine on its private branch as the honest miners continued on the public chain. The

attacker would develop a longer lead as it secretly developed more blocks. The attacker would then reveal these new blocks when the public branch approached the length of the pool's private branch. Both the attacker and the honest miners would end up wasting energy, but the honest miners would waste proportionately more while the attacker gained rewards that exceeded its share of the mining power. As such, the attacker gains a competitive advantage and rational miners would be incentivized to join its version of the block chain. This attack would thus undermine the decentralized nature of the system by leading to a further consolidation of mining power in the attacker's favor.[31] While Felten has argued that a coalition of selfish miners is likely to fall apart, he leaves open the question of whether a single selfish miner with a significant share of computing power could launch this attack.[32]

The Feasibility of a State Attack

The feather-fork and selfish mining attacks are significant because they demonstrate how Bitcoin could be threatened by a malicious attacker with less than 51% mining capacity. In other words, they lower the bar for computing power necessary to pose a threat to the integrity of Bitcoin. The caveat with these attacks, however, is that they only pose a certain percentage of risk. An attacker with 51% of total Bitcoin mining capacity, however, would unambiguously pose an existential

[31] Ittay Eyal and Emin Gun Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," arXiv:1311.0243, 15 November 2013

[32] Edward Felten, "Bitcoin isn't so broken after all", *Freedom to Tinker*, 7 November 2013. https://freedom-to-tinker.com/blog/felten/bitcoin-isnt-so-broken-after-all/

threat to the system. Therefore, to set the highest bar for demonstrating feasibility, in this section we examine the feasibility of a state actor obtaining 51% mining capacity.

Costs of Obtaining a 51% Attack Capability

What would it cost to acquire a 51% attack capability? The following presents a preliminary calculation based on extrapolating from the current costs of computing power. The hash rate as of May 1, 2014, was 58,067,925 GH/s. The present best-available double SHA256 ASIC mining hardware includes the CoinTerra TerraMiner IV and the Avalon3-2U, details of which are given in the table below:

	Hash rate (GH/s)	Power consumption (W; 1 W = 1 J/s)	Cost
CoinTerra TerraMiner IV	1600	2100	$3499
Avalon3-2U	800	822	4.59 BTC (~$2000)

To mount a 51% attack, a state could simply introduce mining power to the Bitcoin network slightly above the current total computing power. (We assume that states will not want to take over current mining capacity.) Doubling the current hash rate instantly would require 58,067,925 / 1600 or roughly 36,500 CoinTerra TerraMiner IV chips at a cost of US$128 million; or 73,000 Avalon3-2U machines at a cost of 333,165 BTC, approximately US$145 million. (This assumes there are

no economies of scale from making or volume discounts from buying such a large volume of chips.)[33]

Energy costs are known to be an important component of Bitcoin mining costs. The estimated energy to run 36,500 CoinTerra TerraMiner IV machines would be 2100W*36500, or 76,650 kW, while the estimated energy to run 73,000 Avalon3-2U machines would be 822W*73000, or 60,000 kW. At present, the cheapest electricity costs in the U.S. are in Arkansas, at about 7.40 cents per kilowatt-hour[34], while electricity costs in China are roughly about 7.50-11 cents per kilowatt-hour.[35] The energy cost from running the required set up in a low-cost electricity state in the US would thus be about $136,000 a day using CoinTerra machines or $106,000 a day using Avalon3-2U machines, and not much more in China.

The calculations above are in line with other estimates of around US$100 million, calculated by similar methods of extrapolating the costs of mining. Other methodologies give higher estimates. The equilibrium method, which bases its cost estimate on a calculation of 51% of the present value of all future revenues derived from Bitcoin mining, estimates the value of launching a 51% attack at $878.8 million, as of May 10, 2014.[36] Bitcoin entrepreneurs the Winklevoss twins claimed at a New York Department of Financial Services hearing on 'Bitlicenses' in January 2014 that they had completed a study, which showed that it would cost

[33] The costs of renting computing power (e.g. mining Bitcoin using Amazon EC2) would largely be similar.
[34] Price as of February 2014, taken from Energy Information Administration, *Electric Power Monthly with Data for February 2014*, p. 123. http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=pmt_5_6_a
[35] "Tiered power bill debated", *Shenzhen Daily,* 17 May 2012. http://english.sz.gov.cn/ln/201205/t20120517_1914423.htm
[36] Coinometrics, "Equilibrium 51% Attack Cost ", http://www.coinometrics.com/bitcoin/brix. Accessed 5 May 2014.

$700 million to acquire the capacity to conduct a successful 51% attack[37], though they did not disclose the methodology behind their calculations. Yifu Guo, founder of Avalon, has claimed that the "51% attack can be achieved for much, much less than these projections"[38] derived from the equilibrium method, likely because he was extrapolating from the cost of Bitcoin hardware.

Putting State Capacity in Context

Regardless of whether one chooses the extrapolation method or the equilibrium method for calculating the costs, it is clear that the cost of acquiring the computing power necessary for a 51% attack would lie in the range of hundreds of millions of US dollars. While this might be large for an individual, the cost of acquiring this amount of computing power is relatively trivial for a state, particularly when compared to the sums that states are willing to devote to national security. For example, China's official 2012 defense budget was 808.28 billion yuan, or approximately US$130 billion. The cost of a single F-35A fighter aircraft to the U.S. is estimated at US$153.1 million with the total program cost for the F-35 airplane of US$1.0165 trillion, while the cost of an MQ-9 Reaper Unmanned Aerial Vehicle (i.e. a drone) is US$18.2 million with a total program cost of US$11.8

[37] Op. cit., Selkis
[38]Yifu Guo, in "A Real-time Tracker of Bitcoin's 51% Attack Cost and then Ranked Compared to Military Spending Across all Countries" thread, Reddit r/Bitcoin, 23 August 2013. http://www.reddit.com/r/Bitcoin/comments/1ky4om/a_realtime_tracker_of_bitcoins_51_attack_cost_and/cbudce5

billion. [39] Even non-superpowers would find a sub-billion dollar sum affordable: for example, both Jordan and Sri Lanka spent US$1.45 billion on defense in 2012, making them only the 64th and 65th largest defense spenders in the world.[40]

If a state decides to acquire the computing power needed to mount a 51% attack, its main roadblocks are likely not going to be cost, but rather supply. It is true that the existing supply of mining hardware is finite and might not be sufficient to double the computing power, although Guo has stated that "Avalon essentially controls more theoretical computing power than the entire network's hash rate."[41] Moreover, a large-scale purchase of mining hardware from existing ASIC manufacturers could be detectable, which could cause ASIC manufacturers to be suspicious and reject the sale if they foresaw they would be used to destroy the market. Alternatively, they could make it easier to achieve consensus on amending Bitcoin's block-acceptance rules to reject a potential state attacker. That said, states could mitigate detection somewhat by creating false online actors to mimic groups of users banding together for large-scale 'group buys.'

At this point in time, the major ASIC manufacturers are all relatively small firms: Avalon, Butterfly Labs, and CoinTerra. The current customized silicon ASICs were developed without the support of any major company, research university,

[39] All figures from "Fiscal Year (FY) 2014 President's Budget Submission, Aircraft Procurement, Volume 1." U.S. Air Force, February 2013. p. 231. http://www.saffm.hq.af.mil/shared/media/document/AFD-130408-079.pdf
[40] Stockholm International Peace Institute, Database on military expenditure from 1988-2012. http://portal.sipri.org/publications/pages/expenditures/download-database
[41] Alec Liu, "Engineering the Bitcoin Gold Rush: An Interview with Yifu Guo, Creator of the First Purpose-Built Miner", *Vice Motherboard*, 26 March 2013. http://motherboard.vice.com/blog/engineering-the-bitcoin-gold-rush-an-interview-with-yifu-guo-creator-of-the-first-asic-based-miner

or venture capitalist.[42] This suggests that there is scope for a state to enlist major chip manufacturers to produce the required computing power, similar to how the US federal government already contracts with Intel Federal to produce high-performance supercomputers.[43] Since an ASIC is simply a dedicated chipset for Bitcoin mining and does not require particularly unusual raw materials, it would appear that as long as a state could afford the US$150 million, the ability to produce the ASICs in the required time frame would not be limited: US$150 million is a trivial proportion of the annual revenue of chip-making firms such as Intel and AMD. Alternatively, a state could even produce its own ASICs using state-owned enterprises (e.g. mobile chip manufacturer Spreadtrum is already owned by Chinese state-owned enterprise Tsinghua Holdings). Without the restriction of intellectual property protections, a state would likely have the ability to reverse-engineer the latest ASIC designs.

So a state willing to turn its state-owned enterprises (including state-owned defense contractors) towards ASIC production or engage private sector contractors to produce the required quantity of ASICs is likely to be able to produce its desired number of ASICs in a short amount of time; if it does so using state-owned enterprises, it may even be able to keep its production secret. In extremis, if a state believes the national security threat is severe enough, it could even expropriate current ASIC production capacity within its sovereign borders; this would be

[42] Michael Bedford Taylor, "Bitcoin and The Age of Bespoke Silicon", p. 10. http://cseweb.ucsd.edu/~mbtaylor/papers/bitcoin_taylor_cases_2013.pdf
[43] Intel Federal LLC, "Intel Federal LLC to Propel Supercomputing Advancements for the U.S. Government", 13 July 2012. http://newsroom.intel.com/community/intel_newsroom/blog/2012/07/13/intel-federal-llc-to-propel-supercomputing-advancements-for-the-us-government

possible in countries that have significant chip manufacturing capacity, such as China and the United States.

The Consequences of State Attack Feasibility

Having demonstrated in preceding sections that launching a 51% attack is well within the means of a state, here we discuss in greater detail what such an attack would look like and also address common points made to downplay the threat of computing power attacks.

A State's Attack Options

One line of thinking with regards to a sovereign attack on Bitcoin is that patterns of behavior in the block chain are detectable, and that the rest of the Bitcoin community can thus react to the attack in a way that makes the attack unprofitable or that otherwise defangs the attack e.g. ignoring those blocks added by attackers. Andresen has suggested that a 51% attack could be neutralized by extending the 'bitcoin priority' notion to influence the chain-fork-selection code.[44] It is true that any sudden influx of new computing power without previous known miners would provoke suspicion and may cause some demand to change the rules. However, introducing new chain-acceptance rules requires building consensus, and

[44] Gavin Andresen, "Neutralizing a 51% attack", *GavinTech* , 1 May 2012 http://gavintech.blogspot.com/2012/05/neutralizing-51-attack.html

the process of consensus may take more time than it requires for a state that has been secretly hoarding computing power to introduce the computing power into the network for a one-time attack. Since it is nearly impossible to disentangle the changes made during a successful attack, a state may only need to accumulate the computing power necessary by stealth and only 'plug in' the power and execute the attack successfully once to reduce faith in the reliability of Bitcoin transactions and establish itself as a credible adversary.

Moreover, it is unclear if it would be even possible to write a chain-acceptance rule that would discourage an attacker—whose goal is simply to reduce confidence in the reliability of Bitcoin transactions—without discouraging legitimate transactions at the same time. Andresen's first (offhand) stab at such a rule—"ignore a longer chain orphaning the current best chain if the Σ[priorities of transactions included in new chain] is much less than Σ[priorities of transactions in the part of the current best chain that would be orphaned]"[45]—is easy enough to circumvent through a form of the selfish miner attack: an attacker who has 51% of the capacity would create a hidden chain that includes 99% of all transactions i.e. most but not all transactions (either excluding random transactions or dropping transactions it would like to blacklist). If after two weeks the attacker releases this hidden and now longest chain, the rule would still allow the chain to be accepted, but with 1% of all transactions randomly or selectively rolled back. If miners and transactions build on this new chain immediately, manually rolling back to the older chain would be messy at best and probably impossible.

[45] Gavin Andresen, "Neutralizing a 51% attack", GavinTech , 1 May 2012

Alternately, a state may only need to prove that it can amass the computing power to take over 51% of the network, without necessarily launching the attack or even accumulating the power, to credibly threaten Bitcoin. A state could announce the threat of a feather-fork attack and essentially claim: "we have no intention of destroying Bitcoin, but these particular transactions bother us and we are willing to destroy Bitcoin if the system continues to accept them." If the state shows itself to be only interested in eliminating certain kinds of transactions (as is already done by the United States with financial transactions involving nuclear proliferation and terrorist financing), miners might choose to cooperate with the state and reject certain categories of transactions that the state has declared *non grata* (particularly if they support the state's view that these transactions should be rejected), rather than undergo the difficult process of finding a consensus on new chain-acceptance rules, which carries the risk of potentially creating second-order effects from large-scale rule changes.

Implications for Other Cryptocurrencies

One alternative if a state successfully mounted a 51% attack on Bitcoin would be for users to shift to another cryptocurrency. In fact, since the rise in Bitcoin's popularity, numerous alternative cryptocurrencies such as Zerocoin have emerged, with many claiming greater resilience and enhanced features. [46] Even

[46] Miers, I.; Garman, C.; Green, M.; Rubin, A.D., "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," Security and Privacy (SP), 2013 IEEE Symposium on , vol., no., pp.397,411, 19-22 May 2013, Jerry Brito, email conversation on 7 May 2014, and Marc Hochstein, "Why Bitcoin Matters for Bankers" in *American Banker Magazine*, March 2014, Volume 124, Issue 2, p. 18

if Bitcoin can be destroyed, the underlying technology cannot. A successful state attack on Bitcoin, therefore, would not preclude another alternative cryptocurrency from simply filling the void.[47]

However, it remains unclear why that other cryptocurrency would be less vulnerable to computing power attacks than Bitcoin. Even if such alternative cryptocurrencies use merge mining techniques to essentially inherit Bitcoin's mining power (currently the highest among the cryptocurrencies) and keep the hash rates high, the costs of destroying a cryptocurrency through a computing-power attack will likely remain attainable for a state at the present moment. The destruction of investor, merchant, and consumer confidence in Bitcoin as a secure platform might thus not only shake the public's faith in Bitcoin but, more generally, in cryptocurrencies as a whole.

To illustrate this point, suppose the Bitcoin community moved to adopt an extension protocol, such as Zerocoin, that allows for fully anonymous (rather than merely pseudonymous) currency transactions[48], to prevent attacks that target specific transactions. Despite this added layer of protection, the attacker might then decide to mount a 51% attack on transactions throughout the entire network if it considers the collateral damage minimal.

Feasibility into the Foreseeable Future

[47] Jerry Brito, email conversation on 7 May 2014
[48] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin". http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

The previous section's calculations of the cost of mounting a computing-power based attack are, of course, not static: it depends on the rate of growth of the hash rate relative to the cost of the equipment. While the hash rate is likely to keep increasing exponentially, particularly if Bitcoin mining increases, the efficiency of the mining technology is also likely to increase concomitantly. A similar extrapolation-based calculation in 2011, when GPUs were the prevailing mining technology and the hash rate was 24,000 GH/s, suggested that the total cost of mounting a 51% attack then would have been US$16.35 million[49]. This suggests an interesting dynamic in the relationship between Bitcoin's hash rate and its security from sovereign attackers. At lower hash rates (i.e. lower general use of Bitcoin), it is likely to be easier to destroy faith in Bitcoin and other cryptocurrencies through technological means. However, the incentives of a sovereign attacker to perform such an attack are likely to be less (which can be said to be a form of security by obscurity).

We thus calculate the likely growth rate in the Bitcoin hash rate. Taylor suggests that there are four growth vectors for the hash rate, the first two economic and latter two technological[50]:

i. If Bitcoins become more valuable, then hash rate will increase correspondingly because there is a larger pool of money

[49] User 'nmat', "How much would it cost to execute a 51% attack?" thread, Bitcoin Stack Exchange, 16 Sep 2011. http://bitcoin.stackexchange.com/questions/1093/how-much-would-it-cost-to-execute-a-51-attack/1094#1094

[50] We are indebted to Professor Michael B. Taylor at the UCSD Center for Dark Silicon for contributing his insights on the development of Bitcoin technology and the growth of the Bitcoin hash rate, as elaborated on in this and the following two paragraphs.

ii. People moving their farms to cheaper sources of energy
iii. Moore's Law (which will continue to apply to the evolution of chips at least from 22 nm to 7 nm)
iv. Better designs for Bitcoin miner ASICs e.g. leveraging dark silicon

Taylor notes that the exponential growth of the Bitcoin hash rate in the recent past was mostly driven by Moore's Law, better Bitcoin designs, and rising Bitcoin prices in decreasing order of magnitude. However, this "massive technology ramp" is starting to slow. Taylor estimates that there is an 80% chance that no new technology will supplant ASICs, since the likely industry-wide spending of half a billion dollars per year is not enough to ramp an entirely new non-ASIC technology. (Bitcoin mining chips do have some unique properties and low complexity compared to general purpose chips that could lead to novel innovations.)

With Bitcoin falling or stabilizing, Taylor's view is that the future will be a competition over hash energy efficiency, with technology playing a much smaller role. Taylor thus predicts that the Bitcoin hash rate will grow over the next decade due to a burst of movement to cheap-energy locations (leading to up to 20x growth in hash rate), accompanied with much slower but steady improvements in the application of Moore's Law (3x growth) and better Bitcoin designs (4x growth). This would suggest a total hash rate growth of 240x over the next decade, or about $14 * 10^9$ GH/s.

However, the hash rate growth would also be accompanied by a continual fall in the cost per GH/s, as has historically been the case with both Bitcoin mining technology specifically[51] and computing power in general. The impact of technological advances, therefore, on the hash rate would likely be cancelled out by the reductions in cost to the consumer, leaving energy efficiency as the main factor increasing the future costs of mounting a computing-power based attack. Using Taylor's 20x estimate, a computing-power based attack could cost 20 * 150 million = US$3 billion in 10 years. While this is non-trivial, it still remains within the reach of many governments, and certainly within the reach of global powers such as the United States and China.

Conclusion

Although Bitcoin's attraction has come from being a technical currency that tries to minimize the role of trust and authority through a decentralized architecture, Bitcoin's security and viability is not derived purely from technological sources. Its viability cannot rest on technical robustness alone, so long as manipulation of the currency remains prone to malicious actors. Bitcoin, therefore, implicitly relies on the state's approval for its functioning.

Additionally, the proponents of Bitcoin must be aware of the fact that the state, from which it requires recognition and perhaps even protection, can itself

[51] Op. cit., Taylor, p. 5.

threaten the currency as an attacker. Indeed, no hypothetical attacker would be as formidable as a state, given its vast resources and capability to conduct not only the endogenous attacks at greater scale but also exogenous attacks via regulation, legislation, and arbitrary force.

Though the ongoing debate on Bitcoin governance and the tension between its esoteric libertarian roots and mainstream ambitions is beyond the scope of this paper, the reality of Bitcoin's vulnerability to state attacks should be included in this debate. Bitcoin may be designed as a decentralized, peer-to-peer network internally, but the entirety of the Bitcoin system itself exists in a larger system, which is very much filled with centralized authorities accustomed to asserting at least some degree of control over any sufficiently pervasive medium of social interaction.

Some may downplay the significance of the vulnerabilities outlined in this paper, but Bitcoin's proponents have grand ambitions for the cryptocurrency. While few states may presently view Bitcoin as a threat, state perceptions of Bitcoin are likely to evolve as those ambitions materialize. Just as those who doubt Bitcoin's future relevance would be wise to consider the consequences of the cryptocurrency's success, so should Bitcoin's proponents grapple seriously with the full range of the system's inherent vulnerabilities.

Works Cited

Gavin Andresen, “Neutralizing a 51% attack”, GavinTech , 1 May 2012. http://gavintech.blogspot.com/2012/05/neutralizing-51-attack.html.

Gavin Andresen, “Taking Down Bitcoin” thread, bitcointa.lk, 29 April 2012. https://bitcointa.lk/threads/taking-down-bitcoin.51231/page-2#post-822208

E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating User Privacy in Bitcoin. In Proceedings of Financial Cryptography, 2013.

Danny Bradbury, “Feathercoin hit by massive attack”, Coindesk, 10 June 2013. http://www.coindesk.com/feathercoin-hit-by-massive-attack/.

Jerry Brito and Andrea Castillo, “Bitcoin: A Primer for Policymakers,” Mercatus Center at George Mason University, 2013.

Nicolas Christin, Raine Bohme, and Sarah Meiklejohn, “Economics and Bitcoin Panel,” Bitcoin and Cryptocurrency Research Conference at Princeton University, 27 March 2014.

Ittay Eyal and Emin Gun Sirer, “Majority is not Enough: Bitcoin Mining is Vulnerable,” arXiv:1311.0243, 15 November 2013.

Yifu Guo, in “A Real-time Tracker of Bitcoin's 51% Attack Cost and then Ranked Compared to Military Spending Across all Countries” thread, Reddit r/Bitcoin, 23 August 2013. http://www.reddit.com/r/Bitcoin/comments/1ky4om/a_realtime_tracker_of_bitcoins_51_attack_cost_and/cbudce5.

Peter J. Henning, “More Bitcoin Regulations Is Inevitable,” The New York Times, 3 February 2014. http://dealbook.nytimes.com/2014/02/03/more-bitcoin-regulation-is-inevitable/.

Alex Hern, “Bitcoin is legally property, says US IRS. Does that kill it as a currency?” The Guardian, 31 March 2014. http://www.theguardian.com/technology/2014/mar/31/bitcoin-legally-property-irs-currency.

Marc Hochstein, “Why Bitcoin Matters for Bankers” in American Banker Magazine, March 2014, Volume 124, Issue 2, p. 18.

Youssef M. Ibrahim, “Fake-Money Flood Is Aimed At Crippling Iraq's Economy” , New York Times, 27 May 1992. http://www.nytimes.com/1992/05/27/world/fake-money-flood-is-aimed-at-crippling-iraq-s-economy.html.

Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, “The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries,” in The Twelfth Workshop on the Economics of Information Security (WEIS 2013), Washington, DC, 11-12 June 2013, pp. 5-10, 13

Lawrence Malkin, Krueger's Men: The Secret Nazi Counterfeit Plot and the Prisoners of Block 19 (New York: Little, Brown and Company, 2006).

I. Miers, C. Garman, M. Green, A.D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," Security and Privacy (SP), 2013 IEEE Symposium on , vol., no., pp.397,411, 19-22 May 2013.

Alec Liu, "Engineering the Bitcoin Gold Rush: An Interview with Yifu Guo, Creator of the First Purpose-Built Miner", Vice Motherboard, 26 March 2013. http://motherboard.vice.com/blog/engineering-the-bitcoin-gold-rush-an-interview-with-yifu-guo-creator-of-the-first-asic-based-miner.

John D. McKinnon and Ryan Tracy, "IRS Says Bitcoin is Property, Not Currency," The Wallstreet Journal, 25 March 2014. http://online.wsj.com/news/articles/SB10001424052702303949704579461502538024502

Andrew Miller, "Feather-forks: enforcing a blacklist with sub-50% hash power" thread, BitcoinTalk, 17 October 2013. https://bitcointalk.org/index.php?topic=312668.msg3353004#msg3353004.

Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (2008).

Ryan Selkis, "Spreading FUD Week: A Sovereign 51% Attack", The Two-Bit Idiot http://two-bit-idiot.tumblr.com/post/79998098398/spreading-fud-week-a-sovereign-51-attack.

Lui Smyth, "The Demographics of Bitcoin (Part 1 Updated)," 4 March 2013.

Michael Bedford Taylor, "Bitcoin and The Age of Bespoke Silicon", p. 5, 10. http://cseweb.ucsd.edu/~mbtaylor/papers/bitcoin_taylor_cases_2013.pdf

Ken Tindell, "Geeks Love the Bitcoin Phenomenon Like They Loved the Internet in 1995," Business Insider, April 5, 2013, http://www.businessinsider.com / how-bitcoins-are-mined-and-used-2013-4.

Bitcoin Wiki, "Controlled Supply," https://en.bitcoin.it/wiki/Controlled_supply

Bitcoin Wiki, "Weaknesses"- https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power.

"China Bans Financial Companies From Bitcoin Transactions", Bloomberg News, 5 December 2013. http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html.

Coinometrics, "Equilibrium 51% Attack Cost," http://www.coinometrics.com/bitcoin/brix.

"Energy Information Administration, Electric Power Monthly with Data for February 2014," p. 123. http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=pmt_5_6_a.

"Fiscal Year (FY) 2014 President's Budget Submission, Aircraft Procurement, Volume 1." U.S. Air Force, February 2013. p. 231. http://www.saffm.hq.af.mil/shared/media/document/AFD-130408-079.pdf

Ghash.io Press Release - https://ghash.io/ghashio_press_release.pdf.

Intel Federal LLC, "Intel Federal LLC to Propel Supercomputing Advancements for the U.S. Government", 13 July 2012. http://newrsroom.intel.com/community/intel_newsroom/blog/2012/07/13/intel-federal-llc-to-propel-supercomputing-advancements-for-the-us-government.

Map and Index of Regulatory Landscape of Virtual Currency – bitlegal.net

MaxMiner, Feathercoin's 51% Attack - Double Spending case study, June 2013 http://maxminer.files.wordpress.com/2013/06/ftc_51attack.pdf.

Stockholm International Peace Institute, Database on military expenditure from 1988-2012. http://portal.sipri.org/publircations/pages/expenditures/download-database.

User 'nmat', "How much would it cost to execute a 51% attack?" thread, Bitcoin Stack Exchange, 16 Sep 2011. http://bitcoin.stackexchange.com/questions/1093/how-much-would-it-cost-to-execute-a-51-attack/1094#1094.