Bitcoin

Securing the Network

Published: August 01, 2015

Author
Chris Burniske Analyst at ARK Invest

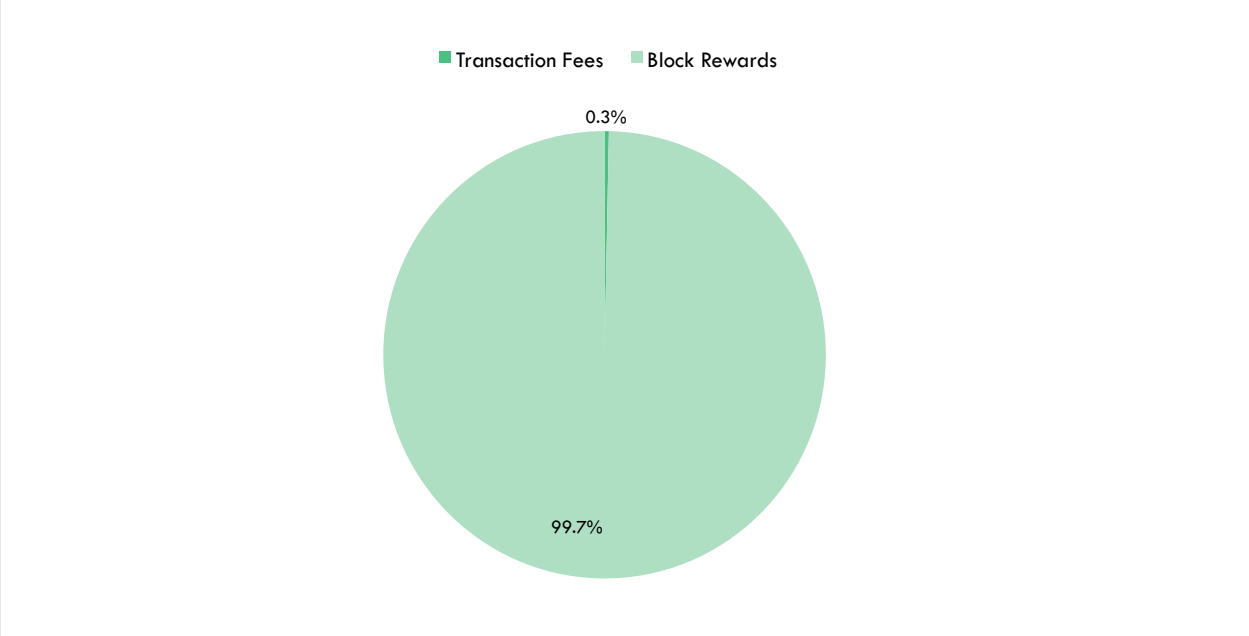
Bitcoin: Securing the Network

Bitcoin has the potential to be disruptive in a way not seen since the development of the Internet. While the Internet decentralized the dissemination of information, Bitcoin and its underlying "blockchain" are decentralizing the securitization of information. Due to its decentralized design, however, there is no single entity guaranteeing Bitcoin's long-term reliability. This white paper investigates how the Bitcoin network will be sustained, especially as its incentive structure changes in coming years, and the effect these changes will have on stakeholders. For those readers who are not already familiar with Bitcoin, ARK Invest has prepared an introductory white paper entitled "bitcoin: A Disruptive Currency," which provides an overview of bitcoin and the Bitcoin network.[1]

Bitcoin and its underlying blockchain solve a problem humanity has grappled with for centuries: without a reliable third party, how can one trust information sent by a stranger via an insecure channel? Thus far, the financial services sector has been unable to solve this problem, and therefore relied upon expensive middlemen. The Bitcoin blockchain, instead, encrypts information with mathematical functions that are computationally impossible to decipher, unless one is the sender or receiver of the information. Thus, bitcoin does not require a central repository or single administrator to process transactions.

A decentralized network of computers, called miners, provides the processing power that encrypts information and secures the blockchain. The blockchain secures bitcoin. Together, they form a digital ledger that is transparent to the world and records every transaction ever made. Currently, newly minted bitcoins, issued via block rewards, incentivize miners to provide the processing power that sustains the system. While the protocol allows for transaction fees, at this time these fees are a small fraction of miners' revenue, as shown below.[2]

FIGURE 1
Miner's Revenue in 2014



SOURCE: ARK Investment Management LLC, Quandl

1 In this paper, "Bitcoin" refers to the open source, decentralized technology platform upon which "bitcoin", the digital currency, depends.
2 ARK Investment Management LLC ("ARK Invest"), data sourced from: "Bitcoin Currency Data," Quandl, Accessed August 2015, http://arkinv.st/1GuyqO2.

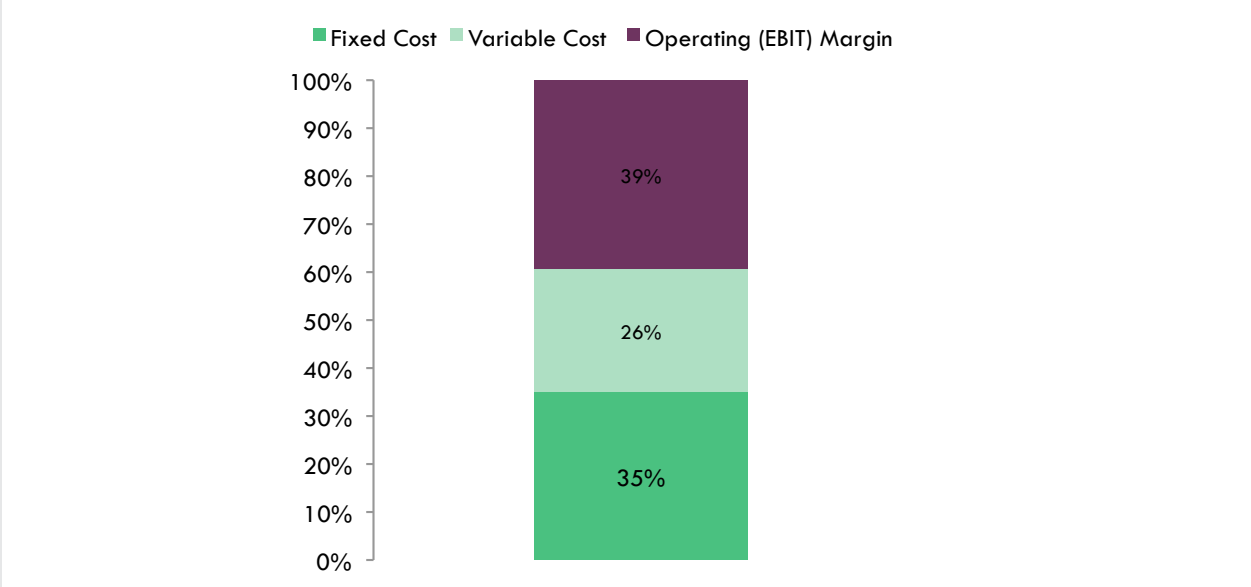
Over the coming decades, however, as block rewards decline, resulting in a lower rate of bitcoin supply inflation, the fee structure will change. In his original white paper, *Bitcoin: A Peer-to-Peer Electronic Cash System,* Satoshi Nakamoto suggested, "Once a predetermined number[3] of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free."[4] Herein lies a major problem: part of the currency's attraction as a medium of exchange is its low transaction fee structure. However, as the currency's monetary expansion diminishes in importance as an incentive to miners, transaction fees will have to take up the slack to maintain the ecosystem. In effect, what was once a hidden subsidy will become a direct cost on Bitcoin transactions.

At first glance this incentive problem might appear to be Bitcoin's fatal flaw. To keep the mining network at its status quo without block rewards, transaction fees that currently make up 0.3% of miners' revenue would have to make up 100%, suggesting a 330 fold increase in fees. Starting from the current average of 0.01%,[5] the transaction fee would soar to 3.3%. At that level, bitcoin transactions would be more expensive than credit cards.

However, that logic misses two variables, which ARK Invest believes will change the equation: mining margins and processing power. First, as the industry matures and block reward "subsidies" dissipate, mining will become less risky as capital intensity and revenue-variance both diminish. As a result, participating miners should accept lower margins. Second, since block rewards have been subsidizing their revenue, ARK Invest's research reveals miners have over-invested in infrastructure, and therefore security, relative to bitcoin's current market cap. As these block rewards halve in accordance with Bitcoin's algorithms, the infrastructure should scale down to an efficient size on the sole basis of transaction fees.

The current profit structure of the Bitcoin network is robust, as shown below.[6]

FIGURE 2
Mining Income Percent Breakdown



SOURCE: ARK Investment Management LLC, Quandl, Blockchain.info, Hashcoins
NOTE: As of August 1, 2015

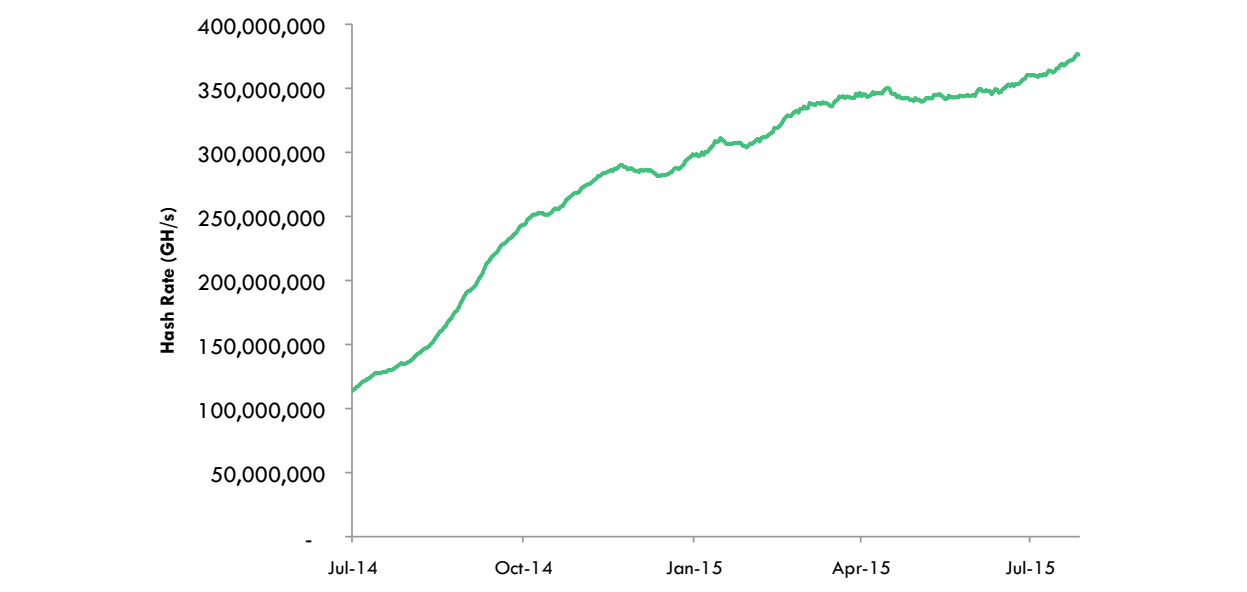
3 This predetermined number currently stands at 21 million coins, which will be reached by 2140.
4 "Bitcoin: A Peer-to-Peer Electronic Cash System," Satoshi Nakamoto, Pg. 4, 2008, http://arkinv.st/1GwV9ZS.
5 ARK Investment Management LLC, data sourced from: "Bitcoin Currency Data," Quandl, Accessed August 2015, http://arkinv.st/1GuyqO2.
6 ARK Investment Management LLC, data sourced from: "Bitcoin Currency Data," Quandl, Accessed August 2015, http://arkinv.st/1GuyqO2, and "HashCoins Shop," HashCoins, Accessed August 2015, http://arkinv.st/1Uiaqtz.

The average EBIT margin[7] for the electric utilities industry over the trailing twelve months ended Q2 2015 was 14.94%, a third that of the big bitcoin miners.[8] With time, as miners earn less income from block rewards, but also spend less on fixed costs and refreshing their installed based (due to the maturation of specialized ASIC[9] hardware), ARK Invest believes that bitcoin mining margins will converge with that of the electric utility industry.

When mining first started[10] people used CPUs to mine bitcoin, then switched to GPUs, before settling on specially designed ASIC chips. Starting from humble beginnings, an arms race[11] quickly emerged around building the fastest and lowest energy bitcoin mining ASIC chips. KnCMiner, one of the companies leading this arms race is deploying a chip at the 16 nm node,[12,13] which is at the leading technological edge of the semiconductor space. For some perspective, the CPU in Apple's (AAPL) iPhone 6 was fabricated at a larger, and therefore less advanced, 20 nm node.[14]

With more bargaining power, the biggest mining pools[15] have faster access to the latest releases of mining chips, elevating their margins due to performance and efficiency superiority. Meanwhile the average miner uses inferior equipment, leading to compressed margins. Margin pressure would explain why the growth in computing power of the Bitcoin network has been more moderate in 2015, as shown below.[16] Because the price-performance ratio for mining chips is still improving, a constant flow of investment would correlate with an increase in the network's hashing[17] power. A flattening of hashing power implies decreased investment and an atrophying of the capital put into the installed base.

FIGURE 3
Hash Rate



SOURCE: ARK Investment Management LLC, Blockchain.info
NOTE: As of August 1, 2015

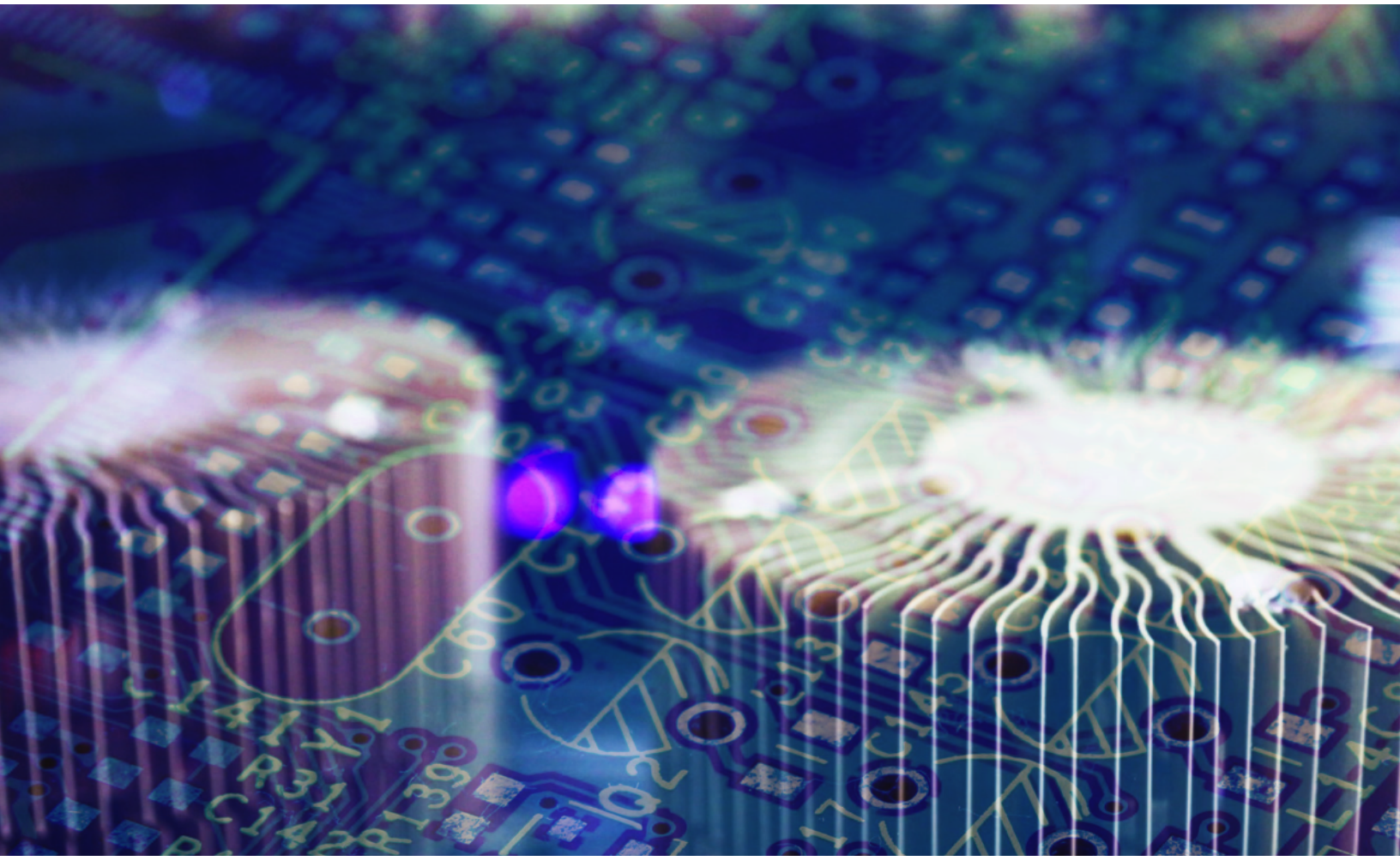
7 Earnings before Interest and Taxes.
8 "Electric Utilities Industry," CSI Market, Accessed August 2015, http://arkinv.st/1JPhzfM.
9 ASIC stands for Application-Specified Integrated Circuit, which is a microchip designed to perform a single purpose extremely fast at low energy.
10 "The History of Bitcoin Mining," CEX.IO, November 2014, http://arkinv.st/1GwVdc5.
11 "Inside the Race to Build the World's Fastest Bitcoin Miner," Wired Magazine, April 2013, http://arkinv.st/1GwVdZN.
12 "KnCMiner Deploys Next-Generation 16 nm Bitcoin ASIC," CoinDesk, June 2015, http://arkinv.st/1PMZ0li.
13 A node refers to the gate length of a transistor. The smaller the node, the smaller the transistors. Therefore, more transistors can be packed into the same space, achieving improved performance and energy efficiency in accordance with Moore's Law.
14 "Apple's A8 SoC Analyzed," Extreme Tech, September 2014, http://arkinv.st/1GwVf3H.
15 A mining pool is a group of miners that unite their computing power to share in the risk and benefit of mining.
16 ARK Investment Management LLC, data sourced from "Hash Rate," Blockchain.info, Accessed August 2015, http://arkinv.st/1fJlMnS.
17 Computing power is also referred to as "hash rate" or "hashing power." A gigahash (GH/s) is one billion hashes per second.

In line with Moore's Law, the ASIC arms race has given bitcoin mining equipment a two-year lifespan before it becomes uneconomical to run. Now that the ecosystem is at leading nodes and the semiconductor industry is struggling to keep pace with Moore's Law, equipment should remain relevant for longer, bringing down fixed costs substantially. In that case, infrastructure spending will shift from fixed to variable costs that are highly dependent on the price of electricity.

Taking into account the current machinery solving the blockchain's computational puzzle, the installed base of specially designed ASIC miners is worth between $200-400 million.[18] This base will get squeezed not only by maturing margins, but also by shrinking block rewards over the coming years, depressing miners' revenue relative to bitcoin's market cap.

As miners get squeezed, the security of the network could come into question. In a widely touted vulnerability, called a "51% attack," any miner with more than half of the network's computing power could spend the same bitcoin twice, not only to generate material one-time profits, but also to undermine the currency.

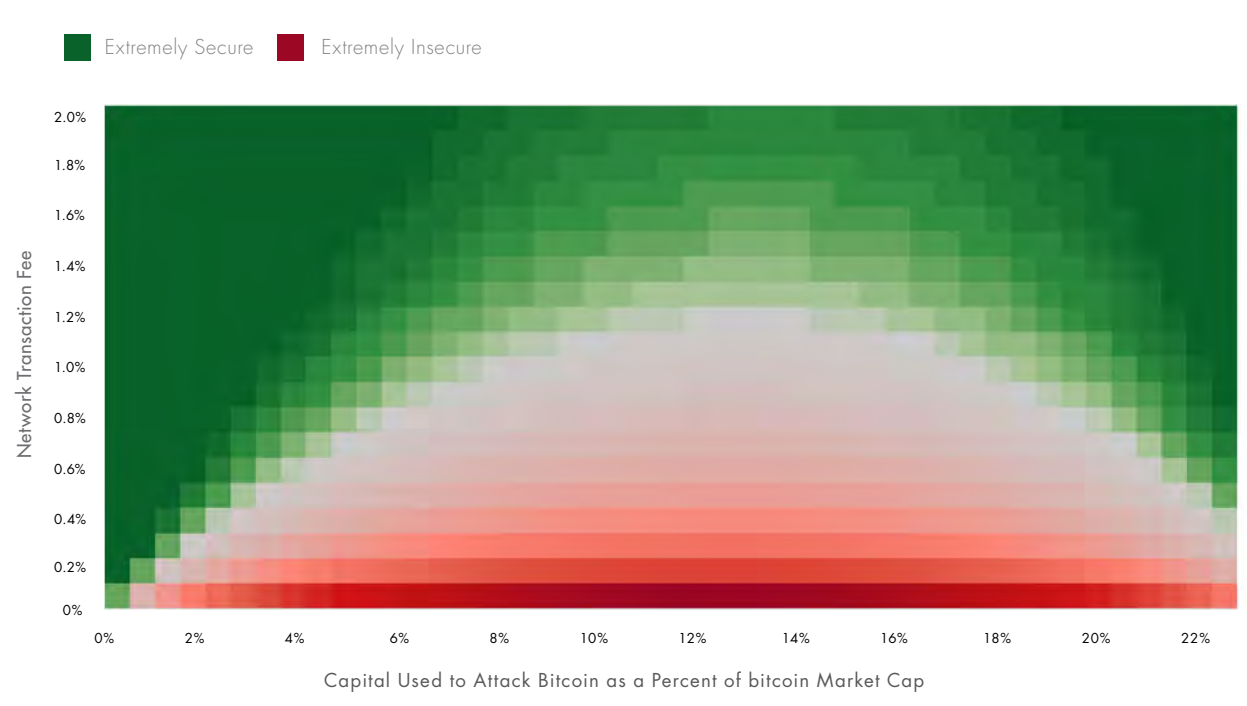
Practically speaking though, the odds of a malicious and successful 51% attack are low. An attacker would have to invest in mining infrastructure equal in size to the existing installed base as of August 2015, or $200-400 million, putting much at risk. Because the attack could destroy Bitcoin and the value of associated mining equipment, an attacker would have to count on hundreds of millions of dollars in revenue merely to break even.



18 ARK Investment Management LLC, deduced from hashing power and mining equipment prices. This estimate for the capital deployed in the mining ecosystem based on the hash rate is roughly consistent with what would be expected given the mining ecosystem's cash flow.

However, where there's a will there's often a way, begging the question of what would be the minimum installed base of mining infrastructure to make the bitcoin network impenetrable to attack. Many assumptions go into answering this question, but ARK Invest calculates that void of block rewards, transaction fees of 1.2% would incentivize a mining infrastructure sufficiently secure regardless of bitcoin's market cap.[19] A secure currency means it would be economically impossible to profit from an attack: the fixed and variable costs would outweigh the expected benefit from a double-spend. The graph below illustrates the topology of network transaction fees and capital outlays that would make an attack economically feasible. The red area depicts what transaction fees and capital outlays would be necessary for a nefarious miner to profit from a 51% attack, while the green area represents a secure network.

FIGURE 4
Bitcoin: Securing the Network

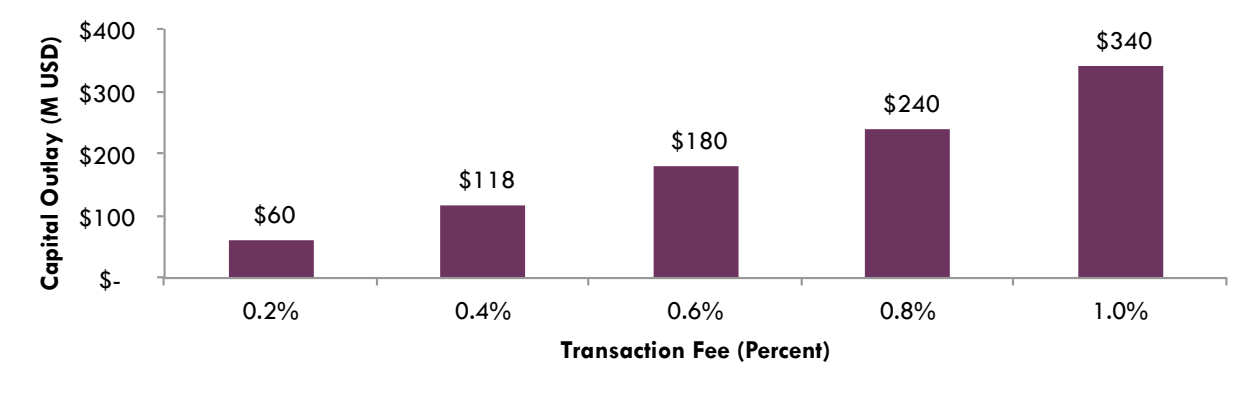


SOURCE: ARK Investment Management LLC

19 ARK Investment Management LLC. The math distills to: the cost of buying the mining equipment, the amount of money the attacker plans to double spend, the trading costs of entering money into and out of the currency, the operating expense of running the mining equipment while executing the double spend, the capital lost when the mining equipment depreciates to 0, all weighed against the revenue from double spending. There is a crossover point at which such a double spend can theoretically be profitably executed, but the amount of capital that has to be put at risk remains quite high relative to the potential reward, even at lower security levels. A major assumption is a double-spending miner has to limit itself to less than ten percent of daily bitcoin transaction volume to avoid arousing suspicions of the mining community and any counterparty who would stand to lose out due to the double spend. Ten percent fraudulent activity would only be made manifest at the end of attack, when the attacker releases its alternate chain.

When the Bitcoin ecosystem reaches maturity and block rewards become a negligible source of revenue, transaction fees alone will incentivize miners to continue building out and securing the network. If bitcoin were to be at a market cap of $4 billion at maturity, which was roughly its size on August 1, 2015, then transaction fees of 0.2%, 0.4%, 0.6%, 0.8% or 1.0% would leave the network vulnerable. However, these transaction fees would necessitate a capital outlay of $60, $118, $180, $240, and $340 million, respectively, for a miner to have even a chance of profiting from a malicious 51% attack. At transaction fees of 1.2% or greater, ARK Invest's research shows that the miners would be incentivized to build out a network that is secure from an economically profitable attack, regardless of bitcoin's market cap and the capital allocation of a nefarious miner.

FIGURE 5
Minimum Capital Outlay for Successful 51% Attack



SOURCE: ARK Investment Management LLC
NOTE: Assuming a Bitcoin market cap of $4 billion and no block rewards

It is important to note that a growing market cap of bitcoin will likely be due to increased bitcoin demand and transaction volume, therefore providing miners with more revenues from transaction fees. Therefore, the mining base will grow to an economically rational size, which in turn will increase the necessary capital outlay to successfully attack the network, an inherent protection built into the protocol. Hence, while a 1.2% transaction fee is a mathematical catch-all to incentivize mining infrastructure of sufficient size to secure bitcoin at any market cap, the precise "vulnerability threshold" transaction fee will depend on the size of bitcoin's market cap in the future. Even at its current market cap, bitcoin is well protected because not many individuals or organizations can raise and risk hundreds of millions of dollars.

An attack in any of the above scenarios would need to be sustained for weeks to prove profitable.[20] Weeks of odd activity would raise suspicion and trigger an aggressive response from the Bitcoin community to thwart the attack. The blockchain's agility as an open source software platform is its strength and will enable the network to evolve quickly if need be. If all else fails, given how much the mining ecosystem and economic majority could lose, they could roll-back the blockchain ledger to undo a successful attack. In other words, even if the transaction fee were to be below 1.2%, the risks of a failed attack are sufficiently high that a nefarious miner probably would choose a different way to invest hundreds of millions of dollars.

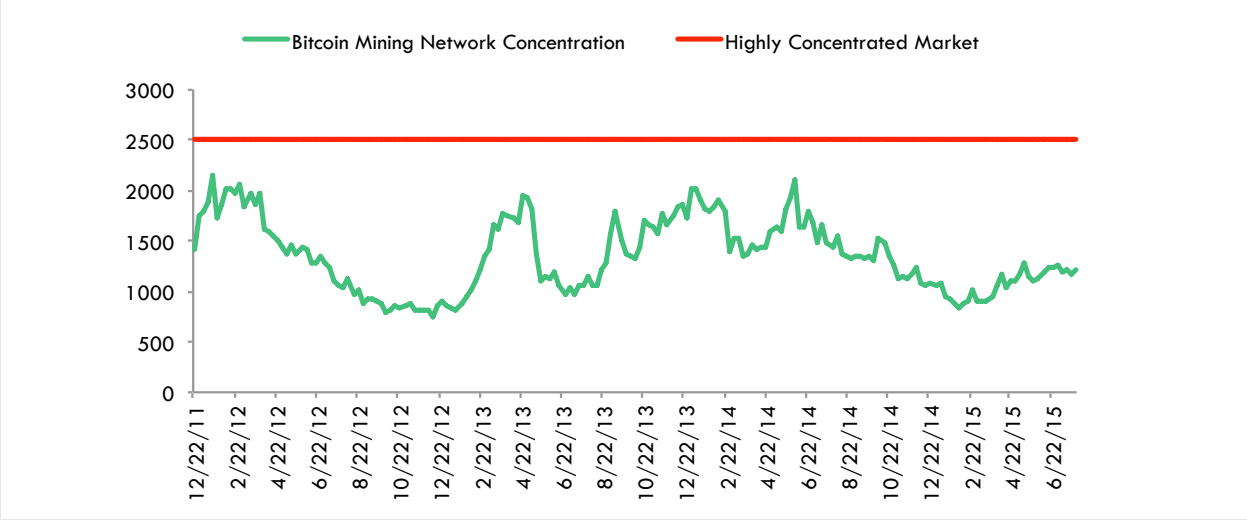
20 This is because average bitcoin transaction volume has been roughly $50 million per day from August 2014 to August 2015, and the assumption is a nefarious miner would need to double-spend at a low percent of transaction volume to have a chance at avoiding detection.

Most importantly, this thought experiment implies transaction fees need never rise above 1.2%, which is less than that of credit cards and debit cards. However, even in Bitcoin's mature revenue model, miners are unlikely to gravitate collectively towards the level of transaction fees at which the network would be secure. Instead, with the goal of securing the network from a 51% attack, fee requirements will have to be programmed into the open source protocol, elastic to the market cap of bitcoin.[21] As already mentioned, the bigger the network becomes, the smaller the transaction fee needs to be to incentivize sufficiently secure mining infrastructure.

Another risk to Bitcoin's security and sustainability is miner centralization. Over time, as mining has become more specialized, miners have pooled resources to reduce the volatility of their earnings, and the industry has become more centralized. Seemingly innocuous, the risks associated with centralization rise as a mining pool inches towards the 50% share threshold. A big enough pool can begin selectively preventing transactions from being incorporated into the blockchain, inhibiting competitor miners from participating in the mining process. It has been mathematically demonstrated that beginning at a 25% share threshold miners can engage in selfish mining that will carry them inevitably to 50+ percent.[22]

The Herfindahl-Hirschman Index (HHI), a measure widely used by antitrust regulators to evaluate relative concentration risk, can be applied to the bitcoin mining community. In conjunction with data scientist Andrew Geyl, ARK Invest has calculated the HHI of the Bitcoin network. After declining for much of 2014, it has been on the rise in 2015. Outsize concentration of the mining network's computing power in one miner or a pool of miners could result in an HHI in excess of 2,500, which is the threshold for what the US Department of Justice classifies as a highly concentrated market. In June 2014, a mining pool called Ghash.io provided over 51% of the mining network's computing power, which put the HHI over 2500.[23] In order to discourage mining centralization, the Bitcoin protocol may have to be modified. Otherwise, sustained HHI values of greater than 2,500 will cast significant doubt on bitcoin's security.

FIGURE 6
Weekly Herfindahl-Hirschman Index

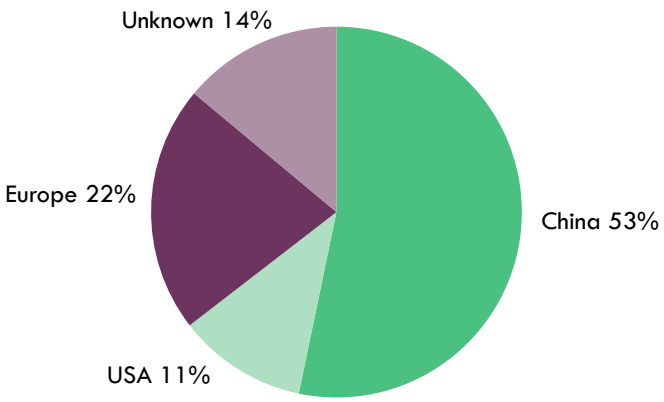


SOURCE: ARK Investment Management LLC, Andrew Geyl
NOTE: As of August 1, 2015

21 There is flexibility in the way these fees could be imposed. For example, a transaction fee schedule could be created for transactions of various size and type. Alternatively, blocks could be capped at a size that incentivizes miners to only confirm transactions that pay sufficient fees.
22 "Majority Is not Enough: Bitcoin Mining is Vulnerable," Cornell University, November 2013, http://arkinv.st/1GwVjAm.
23 This data point is not captured in the graph, which shows weekly HHI.

Because the variable costs of mining are heavily dependent on the costs of electricity, as mining expenses shift from fixed to variable costs, mining will concentrate in geographic areas with the lowest electricity costs. That said, geographic dispersion of miners will be important if bitcoin is to become a worldwide currency: a concentration of miners in one country could put the system at the whim of a single nation. TradeBlock, which serves financial institutions with execution and analytic tools to capitalize on the potential of blockchain technologies, provided ARK Invest with the following distribution of mining pool originations as of June 2015.[24]

FIGURE 7
Global Hashing Power Distribution Origin of Pool

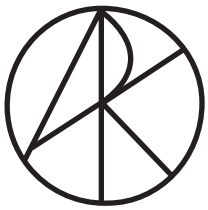


SOURCE: TradeBlock
NOTE: As of June, 2015

Ironically, despite the government's declaration that bitcoin is not a currency with real meaning, China has the largest percentage of mining originations. Because of the popularity of mining pools, Chinese miners could become a potentially dangerous powerhouse in the Bitcoin network.

While the Bitcoin community needs to remain vigilant, ARK Invest believes that its open source nature will be its greatest strength in rapidly eradicating vulnerabilities, adapting to potential threats, and developing policies that incentivize miners to keep the network sustainably secure.

24 The origin of mining pools does not guarantee where the individual mining activity is presently being carried out. That information is not discernible, but this serves as the best approximation.



This material is for informational purposes only and does not constitute, either explicitly or implicitly, any provision of services or products by ARK. Nothing contained herein constitutes investment, legal, tax or other advice and is not to be relied on in making an investment or other decision. Investors should determine for themselves whether a particular service or product is suitable for their investment needs or should seek such professional advice for their particular situation.

All statements made herein are strictly beliefs and points of view held by ARK. Certain of the statements contained herein may be statements of future expectations and other forward-looking statements that are based on ARK's current views and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in such statements. In addition to statements that are forward-looking by reason of context, the words "may, will, should, could, expects, plans, intends, anticipates, believes, estimates, predicts, potential, projected, or continue" and similar expressions identify forward-looking statements. ARK assumes no obligation to update any forward-looking information contained herein. Although ARK has taken reasonable care to ensure that the information contained herein is accurate, no representation or warranty (including liability towards third parties), expressed or implied, is made by ARK as to its accuracy, reliability or completeness.

Any reference to a particular company or security is not an endorsement by ARK of that company or security or a recommendation by ARK to buy, sell or hold such security. ARK and clients as well as its related persons may (but do not necessarily) have financial interests in securities or issuers referenced. Investors should determine for themselves whether a particular security is suitable for their investment needs or should seek such professional advice for their particular situation.

Any descriptions of, references to, or links to other publications, sites, products or services do not constitute an endorsement, authorization, sponsorship by or affiliation with ARK with respect to any such publication, site, product or service or its sponsor, unless expressly stated by ARK. Any such publication, site, product or service have not necessarily been reviewed by ARK and are provided or maintained by third parties over whom ARK exercises no control. ARK expressly disclaims any responsibility for the content, the accuracy of the information, and/or quality of products or services provided by or advertised by these third-party publications or sites.

ARK Invest
155 W. 19th, 5th Fl.
New York, NY 10011
info@ark-invest.com
www.ark-invest.com

JOIN THE CONVERSATION
@ARKwebx0
@ARKinvest