ACADIAN

PERSPECTIVES

VIEWPOINTS FROM THE ACADIAN TEAM

PHILIP OWRUTSKY, PH.D., CFA
VICE PRESIDENT, INVESTMENT STRATEGIST, CLIENT ADVISORY

CRYPTOS' ACHILLES HEEL: THE RISE OF THE "51% ATTACK"

JANUARY 2019

- **As of January 8th, Ethereum Classic is experiencing a "51% attack," whereby malicious agents have stolen over $1.1 million by assuming control of enough computing power to falsify the currency's transaction history. During 2018, several other cryptocurrencies were subject to similar attacks that netted fraudsters over $20 million.**
- **We believe that these attacks threaten the very core of an entire class of cryptocurrencies, those based on the "proof-of-work" paradigm, which includes Bitcoin.**
- **Paradoxically, the threat to this class of currencies has been exacerbated by their very success; namely, their integration into mainstream financial institutional frameworks.**

Bitcoin and other cryptocurrencies that are based on what is known as a "proof-of-work" paradigm[1] represent a valuable technological advancement. Their underlying methodology allows for the maintenance of a provably correct public ledger of transactions without the need for a central, trusted party to maintain it. That ledger's veracity, and, thus, these cryptocurrencies' credibility, depends on an inviolable condition: that no individual or syndicate can control a majority of the computing power associated with the platform. If that were possible, then an actor could commit fraudulent transactions by falsifying the ledger in what is called a "51% attack."

As of this writing, such an attack is underway against the Ethereum Classic cryptocurrency. This isn't the first currency to fall victim. In 2018, malicious agents successfully attacked several other cryptocurrencies in this manner, pocketing over $20 million in the process (Table 1). By securing majority computing power associated with a currency, the perpetrators have been able to "double-spend" coins by undoing their side of anonymous transactions, retaining both their coins and their counterparties'. (Please see appendix for details.)

TABLE 1: KNOWN 51% ATTACKS DURING 2018-19, TOTALING OVER $20MM IN DAMAGES

Date	Coin	Exploit	Market Cap ($)	Amount ($)
May-18	Bitcoin Gold	51%	206 M	18+ M
April-Dec 2018	Verge (x4)	51% (using code bug)	90 M	2.8+ M
Jan-19	Ethereum Classic	51%	535 M	1.1 M
Jun-18	Zencash	51%	25 M	550k
May-18	Monacoin	51%	28 M	90k
Jun-18	Litecoin	51%	1.5 B	Unknown/small

Sources: "Bitcoin Spinoff Hacked in Rare '51% Attack', Jeff Roberts, Fortune, May 29, 2018."Third Time's a Charm: Verge Suffers 51% Attack Yet Again", Tony Spilotro, BlockExplorer News, May 29, 2018. "Ethereum Classic 51% Attack – The Reality of Proof-of-Work", Gareth Jenkinson, Cointelegraph, Jan 10, 2019. "Zencash Target of 51% Attack; Loses More than $500k in Double Spend Transactions", Matthew Hrones, Bitcoinist, Jun 3, 2018. "LiteCoin Cash (LCC) Latest Victim of a 51% Attack", Mark Hartley, Crypto Coin Spy, Jun 8, 2018. For illustrative purposes only.

[1] Proof-of-work blockchains rely on a distributed network of transaction verifiers called "miners" to ensure the veracity of their public ledger – commonly called the blockchain.

TABLE 2: ESTIMATED COST PER HOUR OF A 51% ATTACK

Coin	Symbol	Market Cap ($)	Algorithm	Hash Rate	Attack Cost/hr ($)	NiceHash-able
Bitcoin	BTC	60.99 B	SHA-256	33,918 PH/s	213,766	0%
Ethereum	ETH	9.49 B	Ethash	157 TH/s	68,447	5%
Bitcoin Cash	BCH	1.81 B	SHA-256	1,178 PH/s	7,425	2%
Litecoin	LTC	1.50 B	Scrypt	160 TH/s	15,586	9%
Monero	XMR	739.05 M	CryptoNightV8	391 MH/s	4,679	8%
Dash	DASH	570.63 M	X11	2 PH/s	2,914	71%
Ethereum Classic	ETC	416.88 M	Ethash	9 TH/s	3,884	87%
Zcash	ZEC	309.74 M	Equihash	2 GH/s	12,982	9%
Bitcoin Gold	BTG	207.84 M	Zhash	2 MH/s	675	4%
Bytecoin	BCN	109.03 M	CryptoNight	494 MH/s	335	57%

A hash rate is roughly a measure of the computational power across all miners on a platform. The "NiceHash-able" percent represents the portion of hashing power available to rent from NiceHash relative to the amount required to execute an attack. For Bitcoin, an insignificant portion is available to rent. However, for the recently attacked Ethereum Classic, most of the required power is available by a simple rental.

Source: Crypto51. As of Dec.12, 2018. For illustrative purposes only.

Paradoxically, the success of cryptocurrencies, specifically their integration into traditional financial institutional frameworks, has elevated both the potential damage and profits from an attack. Crypto-exchanges are natural counterparties for transactions large enough to make an attack profitable. Not surprisingly, exchanges have been consistently targeted by attacks, generating millions of dollars in losses often in a matter of minutes. Unfortunately, an attack on an exchange may introduce systemic risk through trading suspensions, account freezes, and partial payouts to account holders that affect participants other than the direct victims of the fraud and even holders of other currencies. Crypto futures may further increase the incentive to commit attacks, allowing malicious agents to establish short positions before undermining a currency.

For many cryptocurrencies, it may take alarmingly little investment to temporarily control enough computing power to mount an attack. In some cases, substantial mining power is rentable through online marketplaces.[2] One website now tracks the cost of executing a 51% attack based on this rentable capacity (Table 2). Collective mining activity also increases currencies' vulnerability. Many miners contribute their resources to pools in order to share in a more consistent revenue stream. Such pools represent a significant share of the computational power on the Bitcoin network, for example (Figure 1). Control over a large pool, either by a malicious owner or by somebody who gains access to their account, may represent a material head start toward acquiring majority control. Even if the pooled resources simply are taken off-line,[3] the resulting computational vacuum might be enough to enable a 51% attack. The concentration of Bitcoin mining in China also highlights the risk of state-sponsored attacks as a general concern.

Currently, though, we believe that Bitcoin is safe from a 51% attack, because its mining community is too large and heavily reliant on specialized hardware; it would be infeasibly expensive even for a consortium to take control of majority computing power. But even Bitcoin's security shouldn't be taken for granted. The recent plunge in its price depressed the payoff from mining to below the cost of electricity in many regions, resulting in a 35% decline in the platform's computational power.[4] That materially lowered the barrier to an attack. If Bitcoin's price were to drop below $3,000, then mining in China, which we estimate to account for at least 75% of current mining (Figure 1), would start to become unprofitable.[5] If the Bitcoin platform were to further lose such a significant portion of its mining power, then it too would become susceptible to a 51% attack.

We see the threat to proof-of-work cryptocurrencies from 51% attacks as existential. The consequences of a specific fraud extend beyond its immediate victims. Market participants may lose confidence in currencies and exchanges, not only those specifically targeted. While smaller platforms are particularly vulnerable, Bitcoin's increasing vulnerability to attack as its price slides underscores the need for more robust protocols if cryptocurrencies are to survive.

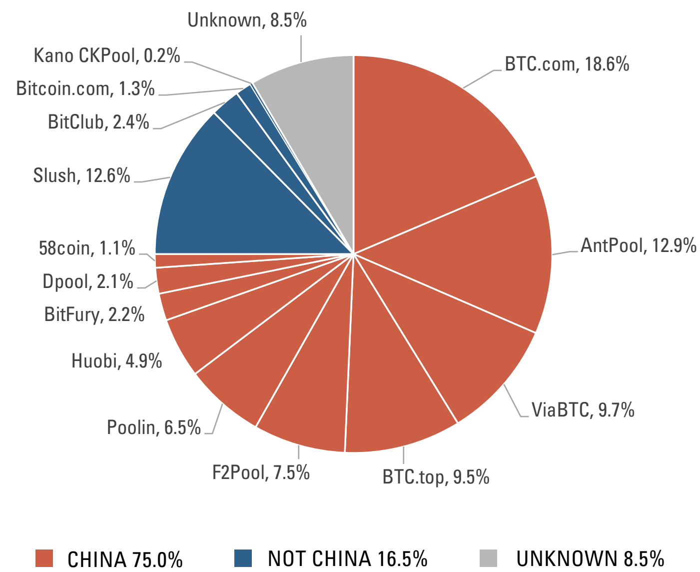
2 NiceHash is a marketplace specifically for buying and selling mining computing power.

3 Such an event might be accidental (e.g., a power outage) or deliberate (e.g., a distributed denial of service).

4 Source: data.bitcoinity.org

5 Source: Elite Fixtures

FIGURE 1: DISTRIBUTION OF BITCOIN MINING BY GEOGRAPHY AND MINING POOL



Share of mining performed by major mining pool and region. Note that the top 3 pools control over 40% of the mining network. China has the largest concentration of miners due to generally lower costs of electricity. China mining share calculated based on the affiliation of the corporation or individual that owns (or ownership share of) the pool.

Source: Coin Dance and Acadian calculations. As of Dec.12, 2018. For illustrative purposes only.

APPENDIX: ANATOMY OF A "51% ATTACK"

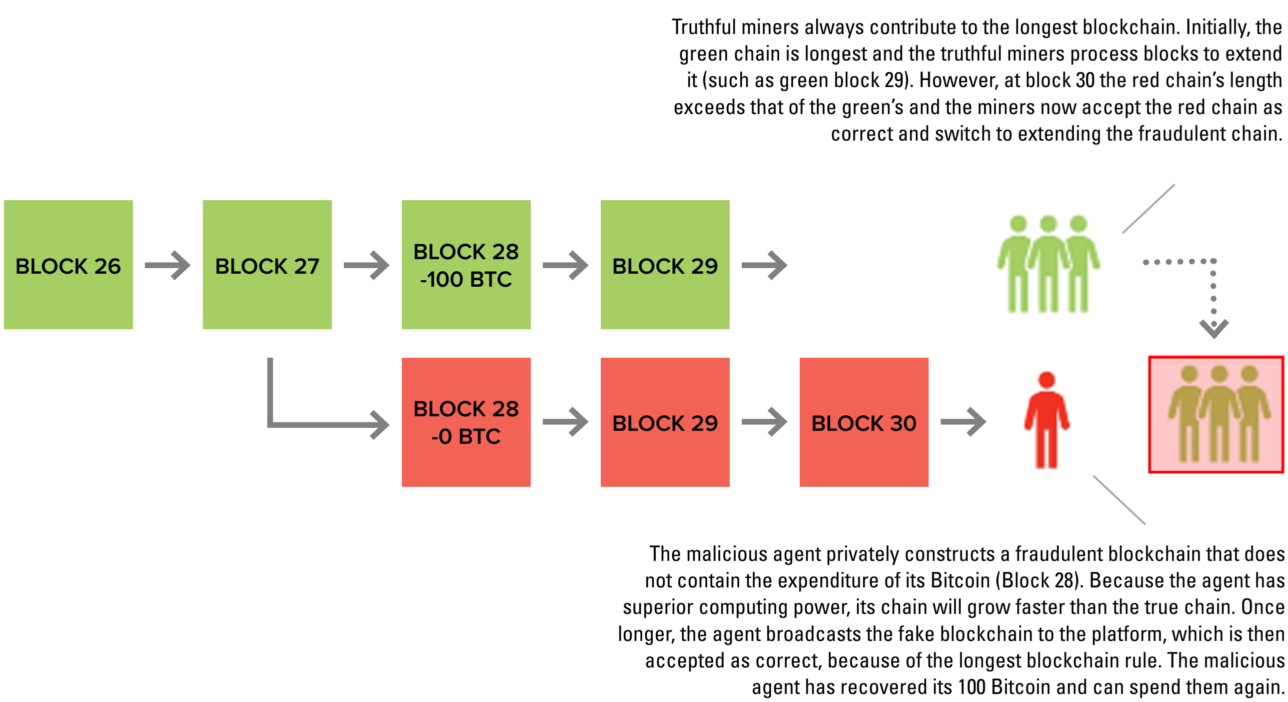
Most cryptocurrencies, e.g., Bitcoin, track coin ownership on a public blockchain, which serves as a ledger of all transactions to date. As part of the cryptocurrency's definition, all participants accept the longest blockchain as correct ("The Blockchain"). Under normal circumstances, this rule safeguards the veracity of The Blockchain because of the computational expense of validating transactions, i.e., adding blocks to the chain: in order to add a block, somebody (a "miner") must solve an extremely resource intensive, transaction- and history-dependent cryptographic problem (but that is trivial to subsequently verify). Miners are paid for being the first to solve the problems, incentivizing competition and a large mining community.

Ordinarily, the difficulty of these cryptographic problems operates in conjunction with the longest-blockchain rule to prevent counterfeit chains. The idea being that it should be infeasible for a malicious individual to generate a fraudulent blockchain, i.e., to falsify the ledger. If, however, an individual or a consortium gains control of more than 50% of the computing power on a platform, then the agent can do just that, enabling it to "double-spend" coins.

As the term suggests, double-spending indicates the ability of a coin holder to (fraudulently) spend the same coin twice. A malicious agent would do so by effectively annihilating the record of its side of a transaction, all the while retaining the good or service (often a different cryptocurrency) that the counterparty transferred (Figure 2). The fraudster needs majoritarian computing power, which enables it to add blocks to a falsified version of the blockchain faster than the entire network can add blocks to the real one. Once the length of the fake blockchain surpasses the length of the correct blockchain, it will be accepted as The Blockchain. Crucially, this counterfeit blockchain does not contain the transaction in which the malicious agent spent currency (such as Bitcoin), allowing it to spend the same coins again.

Please contact the author for further details.

FIGURE 2: MECHANICS OF A 51% ATTACK



Depiction of a 51% attack through which a malicious agent with majoritarian computing power is able to double-spend coins by creating a fraudulent blockchain.

Source: Acadian. For illustrative purposes only.

BIOGRAPHY

PHILIP OWRUTSKY, PH.D., CFA

VICE PRESIDENT, INVESTMENT STRATEGIST, CLIENT ADVISORY

Philip joined Acadian in 2016 and is an investment strategist on the Client Advisory Team, aligned closely with Acadian's Global Client Group and Investment Teams. Prior to joining Acadian, Philip was an associate trader at Potamus Trading and was previously a vice president at State Street Bank where, working within enterprise risk management, he was responsible for developing and maintaining regulatory and economic capital models for the securities lending and stable value wrap business units. Philip also worked in a consultant role for various hedge funds while doing his post-graduate academic work. Philip holds a Ph.D. in applied mathematics from Harvard University; an M.S. in engineering sciences and an M.A. in statistics also from Harvard; as well as a B.A. in mathematics and a B.S. in engineering physics from Cornell University. He is a CFA charterholder and a member of CFA Society Boston.

GENERAL LEGAL DISCLAIMER

Acadian provides this material as a general overview of the firm, our processes and our investment capabilities. It has been provided for informational purposes only. It does not constitute or form part of any offer to issue or sell, or any solicitation of any offer to subscribe or to purchase, shares, units or other interests in investments that may be referred to herein and must not be construed as investment or financial product advice. Acadian has not considered any reader's financial situation, objective or needs in providing the relevant information.

The value of investments may fall as well as rise and you may not get back your original investment. Past performance is not necessarily a guide to future performance or returns. Acadian has taken all reasonable care to ensure that the information contained in this material is accurate at the time of its distribution, no representation or warranty, express or implied, is made as to the accuracy, reliability or completeness of such information.

This material contains privileged and confidential information and is intended only for the recipient/s. Any distribution, reproduction or other use of this presentation by recipients is strictly prohibited. If you are not the intended recipient and this presentation has been sent or passed on to you in error, please contact us immediately. Confidentiality and privilege are not lost by this presentation having been sent or passed on to you in error.

Acadian's quantitative investment process is supported by extensive proprietary computer code. Acadian's researchers, software developers, and IT teams follow a structured design, development, testing, change control, and review processes during the development of its systems and the implementation within our investment process. These controls and their effectiveness are subject to regular internal reviews, at least annual independent review by our SOC1 auditor. However, despite these extensive controls it is possible that errors may occur in coding and within the investment process, as is the case with any complex software or data-driven model, and no guarantee or warranty can be provided that any quantitative investment model is completely free of errors. Any such errors could have a negative impact on investment results. We have in place control systems and processes which are intended to identify in a timely manner any such errors which would have a material impact on the investment process.

Acadian Asset Management LLC has wholly owned affiliates located in London, Singapore, Sydney, and Tokyo. Pursuant to the terms of service level agreements with each affiliate, employees of Acadian Asset Management LLC may provide certain services on behalf of each affiliate and employees of each affiliate may provide certain administrative services, including marketing and client service, on behalf of Acadian Asset Management LLC.

Acadian Asset Management LLC is registered as an investment adviser with the U.S. Securities and Exchange Commission. Registration of an investment adviser does not imply any level of skill or training.

Acadian Asset Management (Japan) is a Financial Instrument Operator (Discretionary Investment Management Business). Register Number Director-General Kanto Local Financial Bureau (Kinsho) Number 2814. Member of Japan Investment Advisers Association.

Acadian Asset Management (Singapore) Pte Ltd, (Registration Number: 199902125D) is licensed by the Monetary Authority of Singapore.

Acadian Asset Management (Australia) Limited (ABN 41 114 200 127) is the holder of Australian financial services license number 291872 ("AFSL"). Under the terms of its AFSL, Acadian Asset Management (Australia) Limited is limited to providing the financial services under its license to wholesale clients only. This marketing material is not to be provided to retail clients.

Acadian Asset Management (UK) Limited is authorized and regulated by the Financial Conduct Authority ('the FCA') and is a limited liability company incorporated in England and Wales with company number 05644066. Acadian Asset Management (UK) Limited will only make this material available to Professional Clients and Eligible Counterparties as defined by the FCA under the Markets in Financial Instruments Directive.

ACADIAN

BOSTON LONDON SINGAPORE TOKYO SYDNEY

ACADIAN-ASSET.COM