2016 IEEE 1st International Workshops on Foundations and Applications of Self-* Systems

Bitcoin and the Myth of Decentralization:

Socio-technical proposals for restoring network integrity

Ariel Ekblaw, Chelsea Barabas, Jonathan Harvey-Buschel, Andrew Lippman
Media Lab
Massachusetts Institute of Technology
Cambridge, MA, 02139, USA

Abstract—**Since 2009, the Bitcoin open-source software project has established a commanding presence in the digital currency space as a self-organizing, distributed system. The project stems from a long history of efforts to harness decentralization and progressive cryptography for social good, as espoused by the ethos of the Cypherpunks mailing list on which Bitcoin was first released. However, certain design choices in Bitcoin's core protocol have led to consolidation of the peer-to-peer nodes, rather than greater diversification, thus threatening system integrity. In this position paper, we explore the socio-technical limits that challenge Bitcoin's ability to remain fully decentralized and "self-contained" as an algorithmically governed system. The need to integrate into existing human systems and infrastructures complicates the project's original vision. We propose hardware, software and electricity management modifications to the broader Bitcoin ecosystem, recognizing the need for socio-inspired design strategies to revive network integrity. We then use Bitcoin as an example to discuss the fundamental limitations of "pure decentralization" and algorithmic self-governance.**

Keywords—adaptive algorithms; cryptographic protocols; distributed information systems; multi-agent systems

I. Introduction

At the beginning of 2009, an individual (or group) working under the pseudonym Satoshi Nakamoto released an open source cryptocurrency project by the name of Bitcoin [1]. The promise of Bitcoin lay in its ability to bypass the centralized controls that banks and governments have historically held over the creation and transaction of money. Proponents of Bitcoin emphasize the power of replacing "trust" in social and political institutions with confidence in code that algorithmically regulates the way individuals exchange value over a decentralized network. This emphasis on decentralized, trustless payment networks marks a new chapter in the long conversation about the social nature of money.

Historically, the infrastructural underpinnings of money were upheld by a handful of public and regulated private financial institutions—social organizations like the Federal Reserve and Central Bank, which work alongside private commercial banks and credit card companies to maintain the payments rails we use today [2]. These institutions hold immense power, both in terms of their ability to establish the value of money through the minting of new bills, as well as their ability to control and censor the flow of value between individuals. Credit card companies and banks are well-positioned to extract rents for the use of their payments rails in the form of fees and, increasingly, the transactional data produced over digital payment networks. As Rachel O'Dwyer argues, "Instead of public authority, the proprietary relations of computers and communications networks are significant, as control of the 'rail' or infrastructure and control of value production and accumulation go hand in hand" [3].

Bitcoin was created as an alternative to closed networks for value creation and exchange, one that hypothetically offloads trust in fallible social institutions into algorithmic governance via code. It is on this open-access and transparently networked terrain that Bitcoin proponents have staked their claim. At the heart of the Bitcoin code lies a consensus protocol designed to decentralize the essential processes of verifying transactions and updating the canonical ledger of account. Bitcoin consensus is based on an open and permissionless protocol, which proportionally distributes the monetary incentives that accompany the process of sustaining or "mining" Bitcoin [1]. Part of this protocol, a computational scheme known as "Proof-of-Work," enables the Bitcoin network to maintain its peer-to-peer character, yet becomes the primary driver towards centralization. Proof-of-work is extremely expensive due to the computational costs associated with the unique, mining "puzzles" (cryptographic hash manipulations) used to secure and later validate the network. In order to maximize profits, miners have developed increasingly sophisticated operations that achieve efficient economies of scale. As the Bitcoin network has grown over time, it has evolved from a highly decentralized network of small scale actors into an increasingly centralized landscape of industrialized, professional mining operations. As one of the world's most successful self-organizing networks to date, the Bitcoin trajectory questions whether a certain degree of centralization proves inevitable in peer-to-peer networks.

To understand this phenomenon we must understand how Bitcoin operates, not as a purely self-contained system of algorithmic governance, but as an adaptive, software infrastructure that is shaped by its integration with other key infrastructures, such as hardware manufacturing markets, software management policies, and global electricity prices. In this paper, we explore the limits that challenge Bitcoin's ability to remain fully decentralized, by demonstrating how the need to integrate into existing human systems and infrastructures complicates the original vision for the Bitcoin network. With the realities of the current Bitcoin network thus considered, we propose socio-technical solutions outside

978-1-5090-3651-6/16 $31.00 © 2016 IEEE
DOI 10.1109/FAS-W.2016.18

IEEE computer society

of the core protocol, in areas of hardware, software and smart electricity management.

We analyze each proposal on four dimensions: how critical the proposal would prove for maintaining or reclaiming decentralization; how feasible the proposal proves for technical development and deployment; how realistic the proposal proves for adoption, given the governance constraints of Bitcoin's open-source software community; and how the proposal integrates with economic, market-driven forces.

II. Background on Bitcoin

Bitcoin, as it was originally defined, is a peer-to-peer electronic cash system that relies on multi-entry accounting to maintain validity [1]. The protocol provides explicit incentives for contributing the resources necessary for securing the Bitcoin network. Transaction validators, or "miners," are rewarded with newly minted bitcoin (the "block reward") for successfully updating the ledger. Miners assemble transactions into a data structure known as a block and then hash these blocks to produce valid "Proof-of-Work" (PoW). The protocol includes a self-adapting algorithm to adjust the difficulty of creating a block, such that new valid transactions are appended to the ledger approximately every ten minutes (regardless of how much computational power has recently joined the network). This creates a minimum delay on how quickly Bitcoin transactions can be processed.

Both network difficulty and block reward are known, and as a result one can directly calculate the financial incentive for producing blocks at any given time. Given that one must generate PoW to produce blocks, the value of a block, irrespective of the transactions it contains, is directly related to both the cost of electricity used to produce a valid PoW and the cost of the hardware used to process and broadcast the block.

The collective hashing power of all miners is known as the network "hashrate." Each new block includes the hash of the former, thus forming an immutable "blockchain." The PoW required of miners ensures content integrity. Generating a valid PoW requires computing an immense number of cryptographic hashes, and the probability of success is independent and identically distributed. This means that the probability of success is proportional only to the number of hashes performed, and therefore that success will reflect hardware hashing efficiency.

The Bitcoin protocol specifies the use and broadcast of digitally signed transactions, using identities derived from public/private keypairs known as addresses. These addresses are pseudonymous and transactions record transfer of ownership from one address to another set of addresses. Valid transactions are broadcast to peers and propagate across the network, thanks to the miners [1]. Notably, anyone can join the network as a miner (Bitcoin is an open, permissionless system) and anyone can generate a public/private keypair identity to transact in the system. This provides for robust anti-censorship potential (and the associated threat of money laundering) in contrast to the closed networks maintained by traditional financial institutions. No central authority controls the monetary supply (miners and the difficulty algorithm determine the pace of minting), and no proprietary entity stands at any advantage for extracting "rents" on the payment rail. It is with this vision for an open-access, unregulated, and decentralized currency that the Bitcoin project was borne.

In a twist of fate, the features that give Bitcoin its self-adaptive and self-organizing character also bring the network to today's state of increasing consolidation. The adaptive difficulty-adjustment algorithm is based on network hashrate, so any increase in the hashrate of one miner lowers expected profits for all other miners. This makes Bitcoin mining a low-margin and highly competitive industry, which has led to present-day mining centralization. Bitcoin self-organizes by allowing new nodes to join the mining network at any time and stay on indefinitely, without any checks for growing monopolies and dominating players. This creates a significant first-mover advantage and allows specialization in the hands of a few, thus disincentivizing smaller, more distributed players from contributing. In the following section, we explore the evolution of these trends and how they are reflected in the hardware and software ecosystems of the Bitcoin network.

III. Inherent Limitations in Bitcoin Proof-of-Work

Despite Bitcoin's founding principles and desire for a truly decentralized, self-contained system, both market incentives and computing properties have driven the protocol to a more centralized topology. Resources for heavy computation tend to require an economy of scale that favors concentrated hardware and cheap electricity. Mining power is increasingly concentrated in a few, large hardware centers and controlled by an intimate coterie of miners whose distribution around the globe is shaped by factors external to bitcoin's core protocol [4]. For example, these outfits have historically clustered around locations with an abundance of cheap electricity, which lowers the operating costs of mining [5]. These increasingly professionalized mining operations out-compete any amateur, or even a small collective of cooperative miners (known as a "pool") hoping to mine on the network.

The original Bitcoin white paper identifies the CPU as the standard processor used for Proof-of-Work, but over time, more customized Bitcoin mining implementations have been developed for GPUs, Field-Programmable Gate Arrays (FPGAs), and finally Application-Specific Integrated Circuits (ASICs), which now comprise the supermajority of network hashrate. Small, plug and play hashing hardware (like the Avalon Nano ASIC [6]) is no longer available, and sources of publicly-available hardware are currently limited to a handful of companies.

Researchers have argued that this development is inevitable, because Bitcoin provides strong incentives for miners to push mining hardware towards the limits of energy efficiency with respect to computation [7]. These incentives also reward vertically integrated mining companies that keep all hardware and IP in-house, which leaves the Bitcoin community with few options for purchasing hardware for individual use. As seen in the Fig. 1 graphical representation of Slush's pool from February 2016, the largest total contributions (and raw hashrate) often come from the smallest number of participants [8].

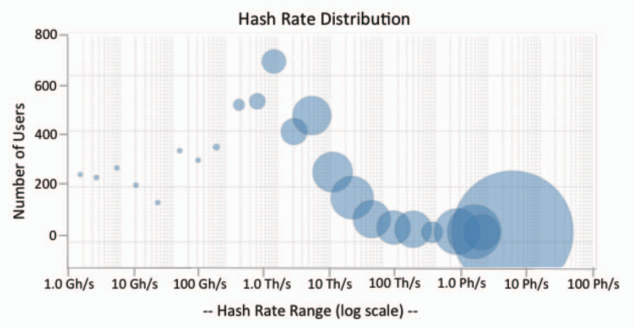

Figure 1. A February 2016 snapshot of the Slush Pool shows that a relatively small group of participants control the vast majority of the hashrate. Each circle represents a group of users with similar hashrate. The area of a circle represents total, summed hashrate of all users in the group [8].

In addition to the concentration of raw processing power, the management policies for pools incentivize centralization. In the early days of the Bitcoin network, participants would "solo mine," or mine on live network transactions and direct profits to their own personal address. As the popularity of Bitcoin and number of miners has increased, the expected return on individual mining has gone down. This has led to hashrate increasingly being aggregated by pools, which distribute work and rewards to a collective of contributing miners. This trend reflects a social adaptation of the network protocol, as economic pressures favored a different network topology. Unfortunately, pooled mining challenges not only the decentralization of the network, but also its security, as pools approach and have crossed the computational threshold for a 51% attack [9]. Miners often lack clear communication channels with the pools that they participate in, and might become unwitting participants in such an attack or other pool scheme that does not reflect their mining interests.

Beyond attacks, pool managers hold power over voting in the Bitcoin system. Messages can be encoded in mined blocks and used as a method of voicing approval or disapproval for protocol changes. By embedding their choice in all blocks mined by the collective, pool managers commit the pool's hashrate to voting for a particular update to the Bitcoin protocol—one that the members of said pool may not agree with.

Consolidated, high efficiency hardware, combined with cheap electricity and aggregated software management, has transformed the hobbyist miner into an endangered species. These centralization tendencies reflect the fundamental contradiction in maintaining a "trustless," decentralized system: the lack of central validation and orchestration requires expensive computation to maintain the validity of the self-organizing system; yet the nature of acquiring the means for such computation leads to economies of scale that favor centralization. We can counter these tendencies with creative protocol constraints and external incentives. We present and analyze several such proposals in the following section.

IV. Modification Proposals for the Bitcoin System

Below, we present three categories of solutions—hardware changes, pool software policies and smart electricity management—that bring a holistic context to the Bitcoin system, beyond the core protocol. For each example, we discuss the impact on decentralization, technical and political feasibility and, if applicable, the economic or market-driven consequences.

A. Hardware Proposals

1) The Challenges of "ASIC resistance":

First, we discuss a commonly touted solution and consider its limitations. The hash function used in Bitcoin is SHA-256, which was designed to be relatively simple to implement in hardware. This ease to implement led to the creation of multiple Bitcoin-specific ASIC design firms, and a diverse set of groups producing ASICs for Bitcoin mining.

The rise of ASICs, specially tailored to SHA-256 for quick solutions to the Bitcoin Proof-of-Work algorithm, created an arms race among miners. This led to ultra-efficient, expensive hardware that outcompetes the hardware available to hobbyist-scale miners. In reaction to this inequality in mining participation, some alt-coins (alternative cryptocurrency implementations) such as Litecoin and Dash [10], looked to replace the PoW function used in Bitcoin with an ASIC-resistant algorithm.

Given the substantial resources already invested in the Bitcoin network, it has proven quite infeasible to change the hash function used for PoW. Miners have invested on the order of 100s of millions of dollars in Bitcoin PoW-specific hardware and they exert significant influence over protocol changes through their "voting" mechanisms. Given this political situation, changing something as fundamental as the hash function used in Bitcoin is a non-starter.

Beyond overcoming the inertia of miner investment in the current algorithm, changing Bitcoin's SHA-256 hash function to be "ASIC-resistant" proves difficult for several additional reasons. First, the majority of developers are very thorough with respect to reviewing and critiquing proposals for changes, as well keeping security and stability as priorities for the network. Even simple changes [11] with little controversy take many months to be accepted. Such a fundamental change would lie in direct conflict with the conservative model of Bitcoin development.

Even if the political environment in Bitcoin were more open to fundamental protocol changes, identifying a hash function for which one could *not* make specialized hardware is an unsolved problem. By definition, any suitable hash function can be implemented in hardware, and any ASIC implementation of a hash function will be most efficient by many orders of magnitude. "ASIC-resistant" functions are only ASIC-expensive, and this extra expense is problematic for any PoW implementation. Using falsely "ASIC-resistant" functions gives an inevitable competitive advantage to the miner lucky enough to first get hands on the ASIC-expensive hardware solution.

The existing investment in SHA-256 is ultimately good for the network, as it accelerates the commoditization and eventual re-opening of access to mining hardware. While the distribution of hardware may never be as ideal as that of CPUs, reducing ASIC cost is the next-best option. Given that ASICs are expected to be developed for any Bitcoin-like cryptocurrency, the ideal outcome is a distribution and diversity of ASICs as good as or better than that of other processors such as the CPUs and GPUs used before ASICs were developed. Achieving this requires mature and diverse ASIC designs, and SHA-256 ASICs are the best option for reaching this outcome given their current ubiquity.

2) Open-sourcing Bitcoin Hardware Designs

A valid means for increasing the decentralization of Bitcoin-specific hardware (known as ASICs) would be to develop modern, open-source designs as well as develop open-source PCBs (Printed Circuit Boards) for lost form factors of mining hardware. Increasing the diversity of available mining hardware lowers the barriers to individual participation. Unfortunately, there are no modern ASICs sold in USB powered packages. Open-sourcing the past designs for these products would allow interested parties to recreate a hobbyist level of Bitcoin mining hardware. Crowd-funding could be used to support open-source PCB development (which would accommodate the proprietary ASIC chips), if otherwise deemed unprofitable by hardware manufacturers.

This proposal is purposefully not a protocol change, but rather a market-based intervention. Protocol changes require consensus among not only Bitcoin developers, but also other members of the community (e.g. miners). As a result, even changes that are not controversial but pose stability or security risks take many months to be rolled out. Many Bitcoin developers cite this resistance to change as a positive feature [12], but it does limit the scope of feasible protocol changes. In contrast, market-based changes prove harder to suppress and can be made without permission—much as pools spontaneously arose out of market pressures.

B. Software Proposals

1) Non-outsourceable Proof-of-Work

Another commonly proposed, though currently infeasible, software-based solution to some of Bitcoin's flaws involves modifying the Proof-of-Work submission method. Proofs-of-Work can be made to be non-outsourceable, and this property is independent of the hash function used. Compared to the design used in Bitcoin, the data submitted in a valid non-outsourceable Proof-of-Work is such that a miner in a pool could anonymously steal block rewards from the pool [13]. This augmentation would require adding support for constructing Non-Interactive Zero-Knowledge Proofs [14], a set of tools still relatively young compared to many Bitcoin protocol components. If implemented, this would heavily disincentivize pooled mining, by giving pool participants means to steal rewards from the pool with a high probability of success. This change in worker-pool dynamic would effectively eliminate pools where the workers do not trust each other, causing the pool ecosystem to fragment into many smaller pools.

Updating the Bitcoin protocol to use Non-Outsourceable Proof-of-Work is not feasible at this time, because the tooling for implementing Zero-Knowledge Proofs is not yet ready for use in security-critical environments. As pools rely on “outsourceability” to function, and many miners depend on pools for current profits, both miners and pool managers would oppose this proposal.

2) Pool Communication Channels

We propose certain modifications that would improve the pool member experience in currently existing, centrally structured pools. Many pools lack clear communication channels between management and participating miners. Highly-engaged miners check the pool websites regularly or follow relevant bitcoin-dev mailing lists. This rather passive dissemination of information neglects miners who may not realize the need to actively monitor for pool changes or who are less familiar with “inside the club” communication channels. This becomes particularly problematic, for example, during times when the network needs to resolve a dispute over which version of an updated protocol to run.

We envision a standardized push notification system to help miners make informed choices. This could be integrated with CGMiner [15] and other common mining clients, for pool managers to use when making policy or implementation changes that would affect their pool membership. The content of the notification could be delivered via email (assuming most pools collect an email to create an account) and would include a notification flag propagated via CGMiner. Alternatively, a condensed version of the message could be delivered directly as a command-line update when running a CGMiner shell (similar updates are already used to display confirmations from the pool after receiving miner contributions). Information that pools could push might include: changes in the way shares are calculated; suspension of adding new members if approaching a certain threshold of network mining capacity (i.e. a 51% attack); changes in pool management personnel; version updates to the Bitcoin protocol, etc.

Such a culture of informed choice surrounding pools, how they operate, and how this impacts the miner would facilitate a market for competition and unique pool policies that could diversify, rather than condense, the existing options. With this hypothesis, we are hoping to direct the pool marketplace towards the standard economic model of “perfect competition”: though not in practice fully attainable, a notion that with low barrier to entry and easily accessible, relevant information, consumers will support a multiplicity of different models rather than centralize around just a few [16]. Encouraging a diverse ecosystem of pools, as long as no one pool could claim an unfair productivity edge, would offer one potential mechanism for preservation of decentralized mining.

3) Self-regulated Pool Management

Recent research has highlighted the risk of Selfish Mining, a type of attack on the Bitcoin network that requires less than 50% of network mining power. Ittay Eyal and Emin Gun Sirer show that, indeed, only 25% of the network resources are needed to attain an unfair distribution of block rewards [17].

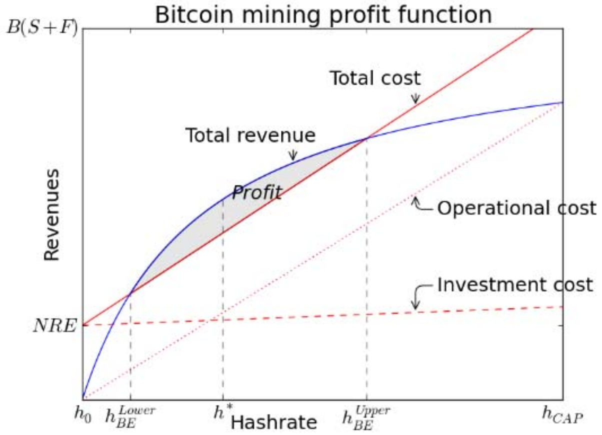

Figure 2. This plot describes a band of profitable mining where the combination of mining reward (S) and transaction fees (F) outweigh the initial "non-recurring engineering" (NRE) costs and operational costs. The h* denotes the hashrate of maximum profitability, between lower and upper bounds of breaking even (BE) [18].

We therefore propose that an additional pool software modification be made for self-regulated pool management. When pools breach the 25% threshold, no new accounts should be added nor shares accepted from new miners.

Such a commitment might be confirmed by asking pools to open source their code to allow for verification of this restriction, or by interfacing with CGMiner and other mining clients to block new, first-time connections to pools that exceed the safe network percentage. An informal, pledge-based approach may be preferred as a less interventionist policy, and more palatable in the current Bitcoin political climate. If the mining community came to collective understanding that selfish mining at the 25% threshold poses a serious threat, then perhaps an automatic, enforceable intervention could feasibly be implemented. Keeping pools below the 25% threshold will help Bitcoin better achieve its founding goals of decentralized network stewardship by preventing pools from obtaining unfair political sway (via block voting) or unduly large revenue rewards.

C. Electricity Price Management Proposals

1) Variable Electricity Pricing

While ASIC prices and availability are hard to control, electricity prices are the other major cost for mining Bitcoin at any scale and are easier to modulate. Much of Bitcoin's centralization problem, with respect to mining hardware, stems from electricity markets being subject to the effects of economies of scale. Since Bitcoin mining is a competition for efficiency, and only those able to purchase long-term electricity contracts can access the lowest electricity prices, residential and small miners cannot compete and mine profitably. Fig. 2 visualizes the profit model for an individual miner, who must find the optimum balance between maximizing hashrate (for increased Bitcoin reward output) and avoiding rising electricity (aka operational) costs associated with these higher hashrates [18].

Mining at home costs thousands of dollars over time and provides little reward. Modern ASICs cost hundreds of dollars to buy [19], and given a common electricity price of 15 cents per kilowatt-hour (kWh), cost dollars a day to run. The expected returns appear at first to be comparable to the operating costs, but quickly drop as competing hashrate joins the network.

However, there is room to make mining electricity costs more affordable on the small scale. Most residences in the U.S. operate on fixed pricing schemes, where a consumer pays a fixed price for electricity throughout the day. In reality, energy markets resemble a bell curve, in that electricity is most expensive to produce during peak hours and very cheap outside of those hours. Variable pricing schemes involve outfitting residences with smart meters, and then charging market price for electricity with the price changing by the hour. This model allows for use of off-peak power that is competitive with the deals industrial miners have. Variable pricing implementations are increasingly available in the U.S. and many E.U. member states [20].

In addition to variable pricing, reuse of excess capacity from renewable energy rigs can be effectively directed at Bitcoin mining, offering lower costs and less energy waste from Proof-of-Work. A recent project demonstrates hobbyist scale, solar-powered Bitcoin mining, for use with currency micropayments [21]. This solution emphasizes low start-up costs, zero steady-state electricity costs, and simple assembly for ease of widespread deployment.

Taking advantage of variable electricity pricing schemes and renewable energy at the residential scale allows for decreased costs and much smaller payoff delays for hardware. In addition, these implementations are feasible outside of Bitcoin's current hotspot for mining (China), potentially re-establishing other areas of the world as centers of mining activity. Geographical distribution helps to prevent some types of attacks by miners against other miners, which is ultimately beneficial for network health. Distributing mining hardware also redistributes control of the network to its users and away from dedicated mining companies, bringing Bitcoin back closer to the robustness of its original threat model.

V. Discussion

Bitcoin was developed as an alternative to closed networks for value creation and exchange, hypothetically eliminating the need for trust by replacing fallible social institutions with self-organizing, algorithmic execution and a self-adaptive protocol for managing network growth. Bitcoin was conceived as a self-contained system, where an incorruptible, peer-to-peer consensus protocol would decentralize currency generation and transfer.

In this paper we have outlined several factors—hardware markets, pool management schemes, and varied global electricity costs—which complicate the story of Bitcoin as a self-contained, decentralized network. As Bitcoin has grown, these externalities have driven dramatic changes in the mining landscape, turning it from a hobbyist sport to a capital-intensive professional activity.

Most attempts to modify this trajectory have focused on technical modifications to Bitcoin's core source code.

TABLE 1. SUMMARY OF HARDWARE, SOFTWARE AND ELECTRICITY PROPOSALS

Properties	ASIC Resistance	Open-Source Specs	Non-Out. PoW	Pool Communication	Pool Self-Regulation	Variable Electricity
Aids Decentralization		✓	✓	✓	✓	✓
Technically Feasible		✓		✓	✓	✓
Politically Feasible		✓		✓	✓	✓
Market-Driven Impact		✓	✓	✓		✓

However, we advocate for a socio-technical approach towards reclaiming decentralization in the Bitcoin network. We argue that the algorithms that govern Bitcoin need support from innovative economic approaches and information management tools outside of the system's core protocol. It has proven quite challenging for the Bitcoin open source community to develop effective processes for implementing key changes to the source code. This pushes us to look for possible solutions beyond the source code itself, by recognizing the external factors that interact with and deeply influence the character of the Bitcoin network. By updating how hardware markets, pool management policies and infrastructural costs like electricity impact the Bitcoin network (summarized in Table 1), we can develop more robust checks and balances for maintaining the integrity of the Bitcoin network.

VI. Conclusion

In an age of growing excitement for algorithmic automation and always-enforced code over flexible interpretations of traditional laws, Bitcoin serves as an invaluable learning experiment. As a system that purports to implement a self-contained protocol through code development alone, Bitcoin has struggled in its eight-year existence to grapple with the messier realities of social precedents, economies of scale, and the human factors involved in its development. Rather than turn away from these realities and attempt to remove all ambiguity through prescient code and software engineering, the Bitcoin network can embrace its role in a broader socio-technical context. We hope that the future of digital currencies, and self-adapting, self-organizing systems more broadly, will be one where elegant algorithms co-exist and integrate with established systems and societal infrastructure, rather than remain in the isolation of algorithmic governance.

Acknowledgment

The authors would like to thank the MIT Digital Currency Initiative and the MIT Media Lab Consortium for their support.

References

[1] S. Nakamoto. "Bitcoin: A peer-to-peer electronic cash system" (2009).

[2] R. O'Dwyer. "When telcos become banks: sociotechnical control in mobile money." *Proceedings of ISIS Summit Vienna 2015—The Information Society at the Crossroads* (2015).

[3] R. O'Dwyer. "Other values: considering digital currency as a commons." RGS-IBG London Panel: *From Co-production to Alternative Futures (1) Creating Cracks: Balue, Commons, and Alternative Economy* (2014).

[4] "Hashrate distribution: An estimation of hashrate distribution amongst the largest mining pools." Blockchain.Info. [Online]. Available: http://blockchain.info/pools. Accessed Apr. 1, 2016.

[5] T. Swanson. "Bitcoins: made in china." May 11, 2014. [Online]. Available: http://www.ofnumbers.com/wp-content/uploads/2014/05/Bitcoins-Made-in-China.pdf

[6] "AvalonMiner Nano." EHash. [Online]. Available: https://ehash.com/product/avalon-nano/. Accessed Apr. 1, 2016.

[7] A. Poelstra. "ASICs and decentralization FAQ." Apr. 8, 2015. [Online]. Available: https://download.wpsoftware.net/bitcoin/asic-faq.pdf

[8] "Pool statistics." Slush Pool. [Online]. Available: https://slushpool.com/stats/. Accessed Apr. 1, 2016.

[9] "51% Attack, Majority Hash Rate Attack." Bitcoin Project. [Online]. Available: https://bitcoin.org/en/glossary/51-percent-attack. Accessed: Jul. 20, 2016.

[10] E. Duffield, D. Diaz. "Dash: A privacy-centric crypto-currency." [Online]. Available: https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf. Accessed Apr. 1, 2016.

[11] P. Todd. "BIP 65 OP_CHECKLOCKTIMEVERIFY." Bitcoin Github Repository. Feb. 1, 2016. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki

[12] B. Bishop. "Cory-fields." Mar. 5, 2016. [Online]. Available: http://diyhpl.us/wiki/transcripts/mit-bitcoin-expo-2016/cory-fields/

[13] A. Miller, A. Kosba, J. Katz, and E. Shi. "Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions." *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15* (2015).

[14] M. Blum, P. Feldman, S. Micali. "Non-Interactive Zero-Knowledge and its applications." *Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC 1988): 103–112.*

[15] "CG Miner." CG Miner Github Repository. [Online]. Available: https://github.com/ckolivas/cgminer. Accessed Jul. 20, 2016.

[16] "Perfect competition." Economics Online. [Online]. Available: http://www.economicsonline.co.uk/Business_economics/Perfect_competition.html. Accessed Apr. 1, 2016.

[17] I. Eyal, E. G. Sirer. "Majority is not enough: Bitcoin mining is vulnerable." *Financial Cryptography and Data Security Lecture Notes in Computer Science* (2014).

[18] S. Valfells and J. H. Egilsson. "Minting money with megawatts." Sep. 2015. [Online]. Available: https://scalingbitcoin.org/montreal2015/presentations/Day2/6-Sveinn-Valfellsmining-slides-montreal.pdf

[19] "AntMiner S7." *Bitmain*. [Online]. Available: https://bitmaintech.com/productDetail.htm?pid=000201603310959482268cfunbq106E5. Accessed Apr. 1, 2016.

[20] J. Harvey-Buschel, C. Kisagun. "ArXiv.org Cs ArXiv:1603.05240. [1603.05240] Bitcoin mining decentralization via cost analysis." ArXiv. Mar. 16, 2016. [Online]. Available: arxiv.org/abs/1603.05240

[21] A. Ekblaw, A. Lippman. "SolarCoin: Making blockchain mining open, green, and ready for micropayments." PubPub. Document Version 1.0. Mar. 9, 2016. [Online]. Available:http://www.pubpub.org/pub/SolarCoin