Park, S., Kwon, A., Fuchsbauer, G., Gaži, P., Alwen, J., and Pietrzak, K. (2018). Spacemint: A cryptocurrency based on proofs of space. In *International Conference on Financial Cryptography and Data Security*, pages 480–499. Springer.

Pass, R., Seeman, L., and Shelat, A. (2017). Analysis of the blockchain protocol in asynchronous networks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 643–673. Springer.

Prat, J. and Walter, B. (2018). An equilibrium model of the market for bitcoin mining.

Saleh, F. (2019). Blockchain without waste: Proof-of-stake. *Available at SSRN 3183935*.

Sapirshtein, A., Sompolinsky, Y., and Zohar, A. (2016). Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 515–532. Springer.

Schilling, L. and Uhlig, H. (2018). Some simple bitcoin economics. Technical report, National Bureau of Economic Research.

Schilling, L. M. and Uhlig, H. (2019). Currency substitution under transaction costs. In *AEA Papers and Proceedings*, volume 109, pages 83–87.

Schrijvers, O., Bonneau, J., Boneh, D., and Roughgarden, T. (2016). Incentive compatibility of bitcoin mining pool reward functions. In *International Conference on Financial Cryptography and Data Security*, pages 477–498. Springer.

Skaperdas, S. (1996). Contest success functions. *Economic theory*, 7(2):283–290.

Sompolinsky, Y. and Zohar, A. (2015). Secure high-rate transaction processing in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 507–527. Springer.

Stoll, C., Klaaßen, L., and Gallersdörfer, U. (2019). The carbon footprint of bitcoin. *Joule*.

Szidarovszky, F. and Okuguchi, K. (1997). On the existence and uniqueness of pure nash equilibrium in rent-seeking games. *Games and Economic Behavior*, 18(1):135–140.

Tullock, G., Buchanan, J. M., and Tollison, R. D. (1980). Toward a theory of the rent-seeking society. *Efficient rent seeking*, 97:112.

Yermack, D. (2013). Is bitcoin a real currency? an economic appraisal. Technical report, National Bureau of Economic Research.

Electrum 0.18.8 is available for details at github.
Upgrade to the latest stable version of iOS, go to Settings–Universal–Restore–Restore network settings, and restart the system once, plugging in the SIM card.
You can download electrum Bitcoin Wallet on the official website "electrum.org". Electrum is also available to users of Ledger Nano S, KeepKey, and TREZOR hardware wallets.
Send the coin to another wallet for long–term bitcoin storage. There should be a full node behind the wallet, such as the Electrum node pointing to your own Electrum server.
The electrum and Electrum–LTC versions below 3.3.3 are vulnerable to phishing attacks in which a malicious server displays a message asking the user to download the fake Electrum. To prevent user exposure, versions older than 3.3 can no longer connect to public servers and must be upgraded. Do not download software updates from sources other than electrum.org and electrum–ltc.org.
Attackers reportedly created their own Electrum servers, which hosted the attacked version of Electrum in order to implement the attack. When the user will be vulnerable.
In August–September, Bitcoin wallet Electrum was hacked twice, and according to multiple sources, at least 1,450 BTCs worth $11.6 million were stolen from phishing attacks that faked Electrum upgrade tips.
Go to Settings – Advanced Settings – Select Network – TomoChain.
Electrum

is understood to have added features such as PSBT (partially signed Bitcoin transactions), Lightning Network, watchtowers (watchtowers) and Submarine Swaps (subliminal switching) to its version 4.0.
Bitcoin wallet Electrum now supports Lightning online payments, according to Coindesk on July 11. It has previously been reported that Bitcoin Wallet Electrum has released a beta version of Electrum 4.0, adding support for the Bitcoin Lightning Network.
Qtum Electrum Tutorial Qtum Electrum Light Wallet.
Another upgrade under study is the release of a new version of the Electrum–LTC desktop wallet. Electrum–LTC is an SPV wallet that can be used in Windows, Linux, and OS X operating systems.
Digital Wallet Electrum was hacked, losing 250 bitcoins.
In a recent announcement on Twitter, Electrum advised users to disable the automatic connection option and manually select a server, while the company is developing a more powerful Electrum.
Shunto touch melon, open the github of the electrum, we find the following code in the electrum/electrum/ecc.py.
Electrum is a well–known light wallet for Bitcoin that adds new features such as server authentication using SSL to prevent MITM attacks. So unlike other Bitcoin light wallets, Electrum cannot communicate directly with different versions of Bitcoin full nodes, and each startup connects to electrumserver to communicate, and electrum.


WinPlay
BiKi
PARTNERSHIP

2 Random Selection in Decentralized Protocols

Bitcoin's ledger is maintained and updated by a decentralized network of anonymous computers, commonly referred to as miners. A key challenge in the design of the protocol is to maintain consensus (Lamport et al., 1982) among all miners on the ledger (record of accepted transactions) while continuously updating the ledger with new transaction data. Bitcoin achieves this by randomly selecting a single miner that issues an update to the ledger, which is commonly called a "block".

This random selection is carried out through the use of a computational puzzle, without relying on known identities or a trusted randomization device. The Bitcoin protocol asks miners to perform costly computations, whose result is used to determine a single miner to issue the next block. Performing these computations in attempt to issue the next block is commonly referred to as "mining".[8] To incentivize miners to perform these costly computations, Bitcoin rewards miners when they are selected to issue the next block.

We next formalize this random selection of a miner. Let $n \geq 2$, and $N = \{1, \ldots, n\}$ be the set of miners and denote by i a typical miner. Each miner i who takes part in the decentralized system performs a certain amount of computations $x_i \geq 0$, which we refer to as miner i's *contribution*. The probability with which miner i is selected in the Bitcoin protocol equals his computational contribution divided by the total contribution by all miners

$$\frac{x_i}{\sum_{j=1}^{n} x_j}.$$

This selection is achieved by having the miners compute cryptographic hashes. Each computation of a hash is equally likely to lead to a value[9] that allows the miner to write the next block and receive the associated reward.[10]

The selection rule is a critical ingredient of any decentralized protocol, as it determines the incentives of miners to contribute to the system. Abstracting away from computational aspects of the problem, we define a random selection rule as follows:

Definition 1 (Selection Rule)**.** *A random selection rule p is described by a family of functions $p^n : \mathbb{R}^n_+ \to \Delta^n$ indexed by $n \in \mathbb{N}$ such that the probability with which miner $i \in N$ is selected at the contribution profile $x = (x_1, \ldots, x_n)$ equals*

$$p_i^n(x_1, \ldots, x_n),$$

which is non-decreasing in x_i.

[8] While miners need to perform other computational tasks (such as validating transactions, storing the ledger, etc.), the vast majority of the miner's computational resources is spent on mining (Croman et al., 2016).

[9] The target value is adjusted periodically, so that on average a single miner is selected to issue a new block every ten minutes.

[10] Under standard cryptographic assumptions, there is no computational method for finding a valid solution that is more efficient than simply attempting many hashes.

A Proofs

Lemma 1. *Consider a selection rule that is robust to Sybil attacks. For every $x \in \mathbb{R}_+^n$ and every $y \in \mathbb{R}_+^k$ with $\sum_{j=1}^k y_j = x_n$*

$$p_n^n(x_1, \dots, x_n) \geq \sum_{j=n}^{n+k-1} p_j^{n+k-1}(x_1, x_2, \dots, x_{n-1}, y_1, \dots, y_k)\,.$$

Proof. The result follows by sequentially applying the robustness to Sybil attacks to miner $r \in \{n, \dots, n+k-2\}$ with $\Delta_r = \sum_{j=r+1}^{n+k-1} y_j$. □

Lemma 2. *We have that for all $i \in \{1, \dots, n\}$*

$$p_i^n(x_1, \dots, x_n) = p_i^{n+1}(x_1, \dots, x_n, 0)\,,$$

and $p_{n+1}^{n+1}(x_1, \dots, x_n, 0) = 0$.

Proof. The robustness to Sybil attacks by Lemma 1 implies that for each agent i

$$p_i^n(x_1, \dots, x_n) \geq p_i^{n+1}(x_1, \dots, x_n, 0) + p_{n+1}^{n+1}(x_1, \dots, x_n, 0)\,.$$

Summing up over all agents $i \in \{1, \dots, n\}$ yields

$$\begin{aligned} 1 &\geq \left(\sum_{i=1}^n p_i^{n+1}(x_1, \dots, x_n, 0)\right) + n\, p_{n+1}^{n+1}(x_1, \dots, x_n, 0) = 1 + (n-1) p_{n+1}^{n+1}(x_1, \dots, x_n, 0) \\ \Rightarrow 0 &= p_{n+1}^{n+1}(x_1, \dots, x_n, 0)\,. \end{aligned}$$

Where we used in the first equality that the combined winning probability of all miners equals 1 and in the second equality that winning probabilities are non-negative.

We thus have that $p_i^n(x_1, \dots, x_n) \geq p_i^{n+1}(x_1, \dots, x_n, 0)$ for all agents $i \in \{1, \dots, n\}$. As winning probabilities sum up to 1 we get that

$$p_i^n(x_1, \dots, x_n, 0) = 1 - \sum_{j \neq i} p_j^{n+1}(x_1, \dots, x_n, 0) \leq 1 - \sum_{j \neq i} p_j^n(x_1, \dots, x_n) = p_i^n(x_1, \dots, x_n)\,.$$

This establishes the lemma. □

Lemma 3. *In any selection rule that is robust to merging we have that for every $x \in \mathbb{R}_+^n$ and every $y \in \mathbb{R}_+^k$ with $\sum_{j=1}^k y_j = x_n$*

$$p_n^n(x_1, \dots, x_n) \leq \sum_{j=n}^{n+k-1} p_j^{n+k-1}(x_1, x_2, \dots, x_{n-1}, y_1, \dots, y_k)\,.$$

Robustness to Merging Consider the winner-take-all rule (definition 3). This rule is anonymous and robust to Sybil attacks, but not robust to merging. To see this note that if two miners merge they still win whenever one (or both) of them would have won, but in addition also win whenever the sum of the contributions exceeds the maximal contribution.

4 Risk-Averse Miners

So far we have been agnostic about the risk attitudes of miners. Axiom 3 presents a weak requirement that is necessary for risk-neutral miners not to have incentives to merge. However, if miners are risk-averse their incentives to merge increase and Axiom 3 is not sufficient to ensure that miners do not want to merge.

Consider any protocol that is anonymous, robust to Sybil attacks and merging (i.e. satisfies Axiom 1-3). By Theorem 1 such a protocol induces a proportional selection rule. Suppose that in such a selection rule miners i and j who are winning with probability p_i and p_j merge and split the price in case they win according to their relative contributions. Together, they now win with probability p_i+p_j. If they win miner i receives a share of $\frac{x_i}{x_i+x_j}$ of the reward from mining the block and miner j receives a share of $\frac{x_j}{x_i+x_j}$. The reward given to either miner in this sharing scheme equals exactly the expected reward of that miner conditional on either i or j winning the block before merging. The original lottery over rewards when not merging is thus a mean preserving spread of the lottery faced by a miner when merging. Hence, it is strictly better for the two miners to merge whenever they are risk-averse. This argument leads to the following corollary:

Corollary 1. *For every selection rule that satisfies Axiom 1-3 any two risk averse miners have a strict incentive to merge their computational contributions and share the reward from mining a block proportional to their respective contributions.*

An economic implication of Corollary 1 is that large mining pools, where miners pool their resources[17] can not be avoided in any decentralized protocol when miners are sufficiently risk-averse. Corollary 1 thus suggests that risk aversion of the miners is an impediment to the decentralization of the network.

5 Equilibrium Contributions

We next endogenize the computing power x_i contributed by each miner i to the system. This section does not produce any novel results, but illustrates the power of our main result. As by Theorem 1 it suffices to understand Tullock contests to reason about the computational contributions in any decentralized protocol we can leverage known results about Tullock contests to better understand

[17]For analysis of mining pools see Fisch et al. (2017), Cong et al. (2019), and Schrijvers et al. (2016).

Computational contributions induced by proportional and WTA selection Different selection rules can lead to very different outcomes. To illustrate this, consider a situation with n miners and compare two selection rules: The first one is the proportional selection rule used by Bitcoin.

Definition 2 (Proportional Selection Rule)**.** *In the proportional selection rule miners are selected with probability proportional to their contribution*

$$p_i^n(x_1, \ldots, x_n) = \frac{x_i}{\sum_{i=1}^n x_j}$$

In the second rule the miner who contributed the most always wins.

Definition 3 (Winner-Take-All Rule)**.** *In the winner-take-all rule the miner who contributed the most wins and ties are broken randomly*

$$p_i^n(x_1, \ldots, x_n) = \begin{cases} \frac{1}{|\{i\colon x_i = \max_{j\in N} x_j\}|} & \text{if } x_i = \max_{j\in N} x_j \\ 0 & \text{else} \end{cases}.$$

To illustrate the different behaviour induced by these selection rules, assume for the example that each miner's marginal cost of performing computations equals 1 and that the reward when mining a block equals 1. It is easily seen that under the proportional selection rule there is a unique Nash equilibrium where each miner contributes[11]

$$x_i = \frac{n-1}{n^2}.$$

In contrast, under the winner-take-all (WTA) rule there is a unique symmetric Nash equilibrium where each miner randomizes his contribution on $[0, 1]$ according to[12]

$$\mathbb{P}[x_i \leq s] = \sqrt[n-1]{s}.$$

These two equilibrium outcomes resulting from different selection rules differ across several dimensions. For example, under the proportional rule miners follow a simple pure strategy in equilibrium, while under the WTA rule there are no pure strategy equilibrium and miners must randomize. Furthermore, the expected equilibrium contributions differ between the two selection rules.

A Mechanism Design Perspective We are interested in which selection rules can be used to maintain a decentralized system. In terms of the miners' behaviour the two above selection rules

[11] We argue this formally in Section 5.

[12] This follows from the strategic equivalence between this game and the complete information all-pay auction, and the characterization of all-pay auction equilibria given in Barut and Kovenock (1998).

Related Literature This paper joins a large and growing literature of papers that analyzed miner's incentives to follow Bitcoin's protocol (Eyal and Sirer 2014, Biais et al. 2018, Sapirshtein et al. 2016, Pass et al. 2017, Carlsten et al. 2016, Kiayias et al. 2016), analyzed miners' entry decisions (Prat and Walter 2018, Arnosti and Weinberg 2019), analyzed the implied market for transaction processing (Easley et al. 2017, Huberman et al. 2019, Chiu and Koeppl 2017, Lavi et al. 2019), criticized its resource inefficiency (Budish 2018, Auer 2019), and suggested alternative designs (for example, Chen and Micali 2016, Benet et al. 2017). Most of the literature focuses on analyzing specific protocols, or presents challenges to a general class of protocols (Abadi and Brunnermeier 2018, Brown-Cohen et al. 2019). Our focus is in providing a characterization of protocols that satisfy axiomatic properties. We hope this approach will help elucidate the limitations and trade-offs for any decentralized protocol.[7]

The economic literature also explored other related issues raised by Bitcoin, exploring the question of adoption and competition between different cryptocurrencies (Athey et al. 2016, Halaburda and Sarvary 2016, Gandal and Halaburda 2014, Gans and Halaburda 2015), the valuation of cryptocurrencies and implication for fiscal policy (Schilling and Uhlig 2018, 2019, Fernández-Villaverde and Sanches 2019, Garratt and Wallace 2018, Benigno et al. 2019), and asking whether Bitcoin functions as a currency (Yermack 2013).

Contests where each player wins with a probability equal to her effort divided by total effort have been called Tullock contests in the economic literature. As our axioms imply a functional form that is equivalent to a Tullock contest, our work is distantly related to the literature that proposes axiomatizations of contest success functions (Skaperdas 1996; Clark and Riis 1998). Skaperdas (1996) show that requiring consistency of the winning probabilities in which only a subset of player participates and symmetry with respect to the players implies a functional form that generalizes the Tullok contest. Clark and Riis (1998) generalize this insight to asymmetric contests. The main axiom in both papers states that when a player stops to participate and exerts zero effort the winning probabilities of each other player increases proportionally. While this axiom is very natural in many contexts it is fundamentally different from the axioms we impose that state that there should be no benefit to Sybil attacks or merging.

This note is structured as follows: Section 2 defines a random selection rule based on the number of computations performed by each miner and provides a characterization of all random selection rules that are anonymous and robust to Sybil attacks and merging. Section 3 argues that all three axioms are necessary to obtain the result. We discuss risk-averse miners in section 4. Section 5 shows how existing results for Tullock contests can be used to characterize how many computations miners perform for the network in any decentralized protocol that satisfies our axioms. We conclude in Section 6.

[7] Subsequent to a first version of our paper Chen et al. (2019) also show that the proportional selection rule is the unique selection rule satisfying similar axioms.