ANNUAL REVIEWS

Annual Review of Financial Economics

Bitcoin and Beyond

Kose John,[1] Maureen O'Hara,[2] and Fahad Saleh[3]

[1]Stern School of Business, New York University, New York, NY, USA;
email: kjohn@stern.nyu.edu

[2]Johnson College of Business, Cornell University, Ithaca, New York, USA;
email: mo19@cornell.edu

[3]School of Business, Wake Forest University, Winston-Salem, North Carolina, USA;
email: salehf@wfu.edu

Annu. Rev. Financ. Econ. 2022. 14:95–115

First published as a Review in Advance on
March 22, 2022

The *Annual Review of Financial Economics* is online at
financial.annualreviews.org

https://doi.org/10.1146/annurev-financial-111620-011240

JEL codes: G00, D4

Keywords

blockchain, Bitcoin, fees, proof-of-work, PoW, proof-of-stake, PoS

Abstract

We survey extant literature on the economics of blockchain fundamentals, with particular focus on Bitcoin, proof-of-work, and proof-of-stake. We formally clarify Bitcoin's economic significance in solving the double-spending problem without a centralized entity. We then transition to the economics literature, highlighting the key endogenous economic interactions among participants in the Bitcoin ecosystem as well as the economics of proof-of-stake and other potential consensus algorithms. Along the way, we discuss various literature that provides important insights regarding fees, forks, and price volatility. We conclude by reflecting on the next generation of blockchain innovations.

1. INTRODUCTION

This article summarizes the economics literature covering Bitcoin and related concepts. We survey seminal works, highlighting key results and clarifying how the literature forms a unified and coherent picture. We focus especially on workhorse models that provide a theoretical framework from which to understand key concepts. We identify an important dichotomy in blockchains between the features required for security and those arising from economic forces. As we discuss, this dichotomy leads to a variety of economic limitations of the Bitcoin design, and it is the basis for the next generation of blockchain innovations.

We begin with Nakamoto (2008), which introduces Bitcoin. Our goal in discussing that paper is to clarify the initial innovation of Bitcoin. In particular, Nakamoto (2008) invented neither blockchain nor digital currency, with many of the underlying technical details of Bitcoin already well established in the computer science literature (see Narayanan & Clark 2017).[1] Indeed, viewing Bitcoin only as a technological innovation misses its most important contribution—it is a solution for an economic problem.

The economic problem that Bitcoin solves is the double-spending problem. The double-spending problem is a generic problem for any payment system. As the name suggests, a double-spend is an instance in which a user spends the same unit of currency twice. This is a problem because a single-spend should transfer ownership of the currency being spent, precluding subsequent spends by the initial owner of the currency. The described problem is trivial to resolve in a centralized setting, because the centralized entity would reject all but the first spending attempt. However, in a setting without a centralized entity, the same problem becomes nontrivial, and Bitcoin's significance is that it solved the double-spending problem without incorporating a centralized entity. It did so by defining a new mechanism for obtaining consensus in a decentralized setting.

In the next section, we set out some useful context for how the Bitcoin blockchain operates and identify several practical and strategic issues that arise from this structure. Section 3 then develops more fully the specific contribution of Nakamoto, and Section 4 turns to the literature developing economic models of the blockchain, focusing on equilibrium levels of mining, fees, and users and on the emergence of forks. Section 5 sets out the literature addressing a variety of structural issues with the Bitcoin protocol. Section 6 examines the literature on an alternative consensus protocol, proof-of-stake. We conclude with thoughts on the evolution beyond Bitcoin.

2. SOME NECESSARY CONTEXT FOR BITCOIN AND BLOCKCHAIN

A blockchain is an electronic ledger that records transactions in discrete chunks referred to as blocks.[2] The blocks are concatenated together into a single immutable chain, hence the term blockchain. Transactions are added to a blockchain only by being incorporated into a new block that is appended to the end of the existing blockchain.[3] Therefore, the process by which new blocks are created and accepted to the blockchain is especially important. Within the context of

[1] For an earlier blockchain, see Haber & Stornetta (1991); for an earlier version of digital currency, see Chaum (1983).

[2] Actually, a blockchain can accept any data, not just transaction data. We focus our discussion on blockchains that accept only transactions because Bitcoin is such a blockchain and because that focus simplifies our discussion. The interested reader may consult Irresberger et al. (2021) for details on existing blockchains that possess additional functionality beyond payments.

[3] The transactions are typically stored within a block in an efficient data structure known as a Merkle tree.

Bitcoin, whether a block can be accepted to the blockchain is determined by a consensus protocol known as proof-of-work (PoW). PoW specifies a computational puzzle as a function of each chain of blocks. Under PoW, for a new block to be accepted at the end of a particular chain, the block must contain the solution to the computational puzzle defined by the full chain on which the new block is being added. The process of attempting to solve these PoW puzzles is known as mining, and agents participating in the process are known as miners. Thus, mining solves two problems on the blockchain—security and transaction processing.

As we discuss in Section 3, Nakamoto (2008) establishes that the ability of Bitcoin to overcome the double-spending problem depends upon the amount of computational power employed by Bitcoin miners in the process of solving the PoW puzzles. More formally, the main result of Nakamoto (2008) is that the probability of a successful double-spend on Bitcoin can be made arbitrarily close to zero so long as the amount of computational power used by Bitcoin miners is sufficiently high. Although this main result emphasizes the need for Bitcoin to maintain a high level of mining, it does so in the context of providing security for the underlying blockchain. Nakamoto (2008) does not explore the economic issue of exactly how much mining would emerge in equilibrium, treating this (and other) economic issues as exogenous. But does this exogeneity make sense? Important issues such as the cost of all this mining surely matter not only for the feasibility of the blockchain but also for whether the system can sustain enough participation by miners (and users).

As noted, under PoW, a block can be added to a chain only if it includes the solution to a computational puzzle, with the puzzle being defined by the chain of blocks to which the block is being added.[4] This specification implies that two blocks solving the same puzzle cannot both be included in the same blockchain—by the definition of a chain, any two blocks in the same chain must be ordered sequentially. But to be ordered sequentially, the two blocks have to solve different puzzles because the puzzle that enables a block inclusion is a function of the chain that precedes it, and the two chains that respectively precede any two blocks in a sequence necessarily differ.[5]

PoW computational puzzles are designed to ensure that exhaustive enumeration is optimal. The probability that a miner wins any particular contest is consequently determined by the miner's level of computational expenditure, because greater computer power enables more attempts to solve a puzzle in any fixed amount of time. Such computation is costly from an economic perspective, so for nontrivial mining to sustain in equilibrium, the computational cost must be offset by sufficient revenue to generate incentive compatibility for that level of mining. As we discuss in Section 4, Easley, O'Hara & Basu (2019) model miners as economic agents and determine the total amount of mining endogenously. These authors provide a theoretical framework that models both users and miners, examining the endogenous economic interactions between and within those groups. But here, as well, a dichotomy arises; while solving for these endogenous economic variables, these authors take the structure defining the security of the blockchain as exogenous (or more precisely, as given in Nakamoto 2008). As we discuss later in this article, it is this tension between security and economics that underlies many of the issues being addressed in the literature.

[4] Formally, the puzzle is to ensure that the hash of the block header being mined is below a certain target. The Bitcoin protocol requires that the block header must include the hash of the previous block header for miners to accept it as a valid successor of the previous block. We say that two miners are solving the same puzzle when their block headers include the same previous block hash. Alternatively, one may think of the puzzles as differing across miners in the sense that the block header also includes the Merkle root for the transaction Merkle tree, and this differs across miners, but we use the former framing because it simplifies our exposition.

[5] Note that the first of any two sequenced blocks is part of the chain that precedes the second block but not part of the chain that precedes the first block.

Bitcoin miners accrue revenues in two forms: block rewards and transaction fees. Block rewards are newly created units of Bitcoin, with Bitcoin (BTC) being the asset created on the Bitcoin blockchain. Those new units of BTC enter into circulation only by being paid to a miner when that miner creates a new block that is accepted to the blockchain. The number of new units created for a given block is determined according to an exogenous schedule that was specified at Bitcoin's inception. In contrast, fees are voluntary payments by users and are thus endogenous.

Bitcoin blocks possess a capacity constraint so that all unprocessed transactions cannot necessarily be included in the next block. Easley, O'Hara & Basu (2019) highlight that this capacity constraint implies that miners optimally accept transactions in descending fee order. Accordingly, a user paying a higher fee reduces their expected wait time relative to a user paying a lower fee, because the user paying the higher fee may be included in an earlier block due to their higher priority. And, assuming that Bitcoin users dislike waiting to have their transactions included in the Bitcoin blockchain, users trade off reduced expected wait time against the cost of paying a higher fee, thereby selecting an optimal fee endogenously. The Easley, O'Hara & Basu (2019) framework then determines the equilibrium fee paying behavior of Bitcoin users and thereby also the equilibrium Bitcoin mining level. We formally discuss Easley, O'Hara & Basu (2019) in Section 4.

Bitcoin was envisioned to be a platform not controlled by a particular entity. To implement that vision, Bitcoin's design enables any agent to add a block to the Bitcoin blockchain. More precisely, since the Bitcoin blockchain is publicly observable and the computational puzzles are public knowledge, participating in mining is feasible for any agent. In economic terms, this implies that Bitcoin mining is a competitive activity. In turn, the set of agents that serve as miners in equilibrium must be determined by a free entry condition. Easley, O'Hara & Basu (2019) highlight that insight and implement it to determine the equilibrium number of miners, thereby filling an important gap left by Nakamoto (2008).

Another seminal work that examines endogenous interactions among Bitcoin users and miners is Huberman, Leshno & Moallemi (2021). These authors also model users as impatient, so that users optimally set fees to balance wait disutility against the cost of the fee. Moreover, akin to Easley, O'Hara & Basu (2019), Huberman, Leshno & Moallemi (2021) employ a free entry condition to determine the equilibrium mining level. More generally, the insights that we discuss from Easley, O'Hara & Basu (2019) are consistent with those found by Huberman, Leshno & Moallemi (2021).[6]

Although multiple blocks solving the same computational puzzle cannot both be included in the same chain, this does not imply that multiple blocks solving the same puzzle cannot be created. This phenomenon is well-known and is referred to as a fork. A fork represents an existential problem for any blockchain, because it introduces ambiguity regarding which transactions have been settled by the blockchain. Multiple blocks solving the same puzzle correspond to multiple chains, with each block that solves the same puzzle being the last block in different chains. Moreover, since each subsequent block must solve a puzzle that is a function of that chain, miners must select one of the existing chains before attempting to add a further block. If different miners select different chains, then multiple chains will receive additional blocks. In such a case, we say that the blockchain lacks consensus, because miners do not agree on which chain represents the blockchain. This lack of consensus is significant because each chain of blocks represents a different

[6] The models do differ in one important way. Huberman, Leshno & Moallemi (2021) argue for shortening the time between blocks, thus departing from the Nakamoto (2008) specification. The block time specification is fundamental to the security of the blockchain, but whether it is optimally set is unclear. Security issues are not addressed by Huberman, Leshno & Moallemi (2021).

payment history, so ambiguity regarding which chain represents the blockchain implies ambiguity regarding which transactions have settled.

Nakamoto (2008) recognized this problem and offered a rule in addition to PoW to enable miners to coordinate on a single chain even in the presence of forks. The longest chain rule (LCR) specifies that miners should add blocks only to the longest chain of blocks. If multiple chains are equally long, miners should add blocks only to the chain that became longest first, as that chain was the most recent chain to strictly be the longest. When all miners coordinate on adding blocks to a single chain, the blockchain is in a state of consensus and that chain is said to be the unambiguous blockchain. Moreover, only payments on the unambiguous blockchain are payments that have been settled by the blockchain. Nakamoto (2008) believed that abiding by the rules stipulated by PoW for accepting blocks and the rules stipulated by LCR for selecting among chains would ensure consensus. However, formal economic analysis highlights that Nakamoto (2008) overlooked some crucial issues associated with forks, including practical constraints that lead to limited adoption (Hinzen, John & Saleh 2021) and incentives for miners to purposefully deviate from LCR (Biais et al. 2019). We discuss those points in detail in Section 5.1.

With regard to practical constraints, Hinzen, John & Saleh (2021) establish that forks arise even when miners are trying to avoid creating them. Forks arise in that context because Bitcoin involves many miners, and these miners do not observe all blocks that solve a particular puzzle at the same time. To see this point, suppose that initially there existed a single chain of blocks. Then, if all miners were following LCR, all miners would attempt to produce a block that solves the same computational puzzle that is defined by the single chain of blocks. Suppose that some miner, Alice, produces a block that solves the referenced computational puzzle. For another miner, Bob, to observe Alice's block, Alice must first send her block to Bob, and latency constraints imply that some time must elapse for Alice's block to reach Bob. In that time, unaware of Alice's block, Bob would continue attempting to solve the puzzle that Alice has already solved. Consequently, with some probability, Bob produces a block that solves the same puzzle already solved by Alice. This is problematic because Bob believes that his block predates Alice's block, whereas Alice believes the opposite. Due to the difference in the time order in which Alice and Bob observe the two blocks, LCR leads Alice and Bob to disagree regarding which block should be included in the blockchain and thus also regarding which chain represents the blockchain, thereby implying a lack of consensus.

Note that the described problem of disagreement among miners does not arise in a centralized setting, because a centralized authority may arbitrate such disagreements by time order using their own local time. For example, Alice and Bob's disagreement could be settled by which of them communicated the respective solution to the centralized authority first. In contrast, in Bitcoin's case, such disagreements are inescapable and cannot be resolved easily. More formally, Hinzen, John & Saleh (2021) demonstrate that the probabilistic nature of the PoW computational puzzle and the time delay in communication among miners ensure that disagreements will arise regularly within Bitcoin, with these disagreements becoming more persistent when Bitcoin processes transactions at a higher rate. Bitcoin thus faces a dilemma: It either maintains a slow transaction rate, which results in large settlement delays, or increases its transaction rate, which increases the rate of disagreement among miners and thereby prolongs transaction settlement times due to the time needed for miners to regain consensus. In either case, most users face such sufficiently long settlement delays that widespread adoption of Bitcoin as a payment system does not arise in equilibrium. Note that this is not just a problem for Bitcoin. Genser et al. (2018) point out that the faster transaction rate of Ethereum results in 3 to 4 times the number of forks on that platform relative to the number on Bitcoin.

Biais et al. (2019) examine whether forks may arise and persist for purely strategic reasons. Biais et al. (2019) provide the first formal economic model of the game among miners induced by Bitcoin's PoW protocol. They consider a dynamic model in which miners select the chain of blocks on which to attempt to add a block at any point in time. LCR is one of many possible strategies for miners in the analysis of Biais et al. (2019), and a central point of inquiry is whether all miners follow LCR in equilibrium as suggested by Nakamoto (2008). To that question, Biais et al. (2019) find that an equilibrium exists in which all miners follow LCR but that other equilibria also exist. Of particular concern, the authors demonstrate the existence of a persistent forking equilibrium, which is an equilibrium in which multiple chains receive blocks in perpetuity. Such an equilibrium is especially concerning because it implies a perpetual disagreement regarding which chain represents the Bitcoin blockchain and thus a perpetual disagreement regarding the set of transactions that have settled on the Bitcoin blockchain.

Carlsten et al. (2016) also examine whether forks may arise but in the absence of block rewards. They find that the absence of block rewards can lead to equilibria with undesirable properties in which miners strategically fork the blockchain. Their key insight is that, with only transaction fees, the fees in a given block can become very high due to the possibility of large time gaps between blocks being produced. Then, miners have an incentive to fork behind a block with high fees to earn the fees within that block.

The results of Carlsten et al. (2016), Biais et al. (2019), and Hinzen, John & Saleh (2021) cast doubt on Bitcoin's ability to serve as a viable payment system. Those same results, however, do not imply that BTC cannot remain a prominent asset. In fact, Biais et al. (2020) demonstrate that BTC price movements are largely detached from its adoption as a means of payment. Thus, the extant literature indicates that BTC should be viewed not as a medium of exchange on a payment system but rather as a speculative asset.

Apart from forks, some other concerns have been raised regarding the functioning of Bitcoin. Some works that highlight significant concerns are Basu et al. (2021), Pagnotta (2022), Aune et al. (2017), and de Vries (2018). Basu et al. (2021) demonstrate instability in the fees paid by Bitcoin users and offer a remedy. Pagnotta (2022) establishes that Bitcoin's design implies extreme volatility for BTC. Aune et al. (2017) examine front-running issues and suggest a mechanism to ameliorate the front-running problem. de Vries (2018) shows that Bitcoin expends a high level of energy due to the computation employed by miners to solve PoW puzzles.[7] We discuss those findings in further depth within Section 5.2.

While Bitcoin remains the most prominent feature in the blockchain ecosystem, hundreds of other blockchains have arisen in the last few years (see Irresberger et al. 2021).[8] Many such blockchains replace Bitcoin's PoW protocol with a protocol known as proof-of-stake (PoS), which generates different economic implications than PoW. As PoS is the dominant protocol among new blockchains, we conclude our discussion by surveying the nascent literature highlighting some of the fundamental economic implications of PoS.

PoS was introduced by King & Nadal (2012) with the primary motivation of avoiding the extreme energy expenditure of Bitcoin. To achieve that goal, PoS omits the computational contests that generate Bitcoin's extreme energy expenditure and employs a different rule based on lotteries to determine which blocks should be accepted to the blockchain. These lotteries are held on each

[7] Cong, He & Li (2021) highlight that financial innovations exacerbate this energy expenditure problem by enhancing incentives for miners to expend energy.

[8] Indeed, as of February 2022, more than 15,000 cryptoassets and tokens were available. For more information, see **https://coinmarketcap.com**.

chain over units of the blockchain's cryptocurrency, with each individual unit of the cryptocurrency being equally likely to be selected as the winner.[9] Once a cryptocurrency unit is selected, the owner of that unit receives the authority to add the next block to the blockchain. The probability that a particular agent wins a PoS lottery is thus proportional to her holding of cryptocurrency units or stake. PoS lotteries involve negligible energy expenditure, so PoS trivially resolves the problem of extreme energy expenditure. Nonetheless, PoS's viability was unclear initially due to two primary concerns: the double-spending problem and the nothing-at-stake problem. As discussed, the double-spending problem is a generic problem for payment systems; in contrast, the nothing-at-stake problem is a novel problem that applies to PoS but not to PoW. Saleh (2021) provides the first formal economic analysis of PoS, studying both the double-spending problem and the nothing-at-stake problem, establishing that PoS overcomes both problems under certain conditions.

A key insight from Saleh (2021) is that PoS imposes financial costs upon agents to participate in the updating of the blockchain, and those financial costs enable PoS to overcome the double-spending problem. Crucially, for an agent to successfully double-spend on a PoS blockchain, she must control which blocks are accepted to the blockchain. Under PoS, an agent's ability to control which blocks are added to the blockchain depends upon the agent's ability to win the PoS lotteries, as winning those lotteries confers authority to add blocks to the blockchain. In turn, an agent's ability to win a PoS lottery depends upon her holding of the PoS cryptocurrency as a proportion of the total PoS cryptocurrency units. Accordingly, the cost of successfully double-spending on a PoS blockchain increases with the market value of the PoS cryptocurrency, because the cost of purchasing any particular proportion of cryptocurrency units increases with the market value of that cryptocurrency. Saleh (2021) highlights this insight and thereby demonstrates that the probability of a successful double-spend on a PoS blockchain can be made arbitrarily small for a sufficiently high cryptocurrency market value. Moreover, Saleh (2021) establishes that attempting a double-spend can be made sufficiently costly so that it does not arise in equilibrium at all.

Saleh (2021) also studies the nothing-at-stake problem. The nothing-at-stake problem argues that all forks on a PoS blockchain are persistent, relying on a premise that no agent would ever decline to add a block to a chain if she won the associated lottery. This follows, because adding a block to a PoS blockchain is without cost and the revenue from the block reward for adding a block makes adding the block a weakly dominant strategy. Saleh (2021) points out that this argument overlooks the impact that adding a block to the blockchain has upon the value of the PoS cryptocurrency. In particular, adding a block to a chain other than the longest chain undermines the ability of any agent to exchange the PoS cryptocurrency, due to the fact that multiple chains receiving blocks creates ambiguity regarding which chain represents the blockchain. In turn, adding a block to a chain which is not the longest chain imposes financial costs upon PoS cryptocurrency holders via devaluation of the PoS cryptocurrency. Then, as the PoS protocol selects only PoS cryptocurrency holders by construction, adding a block to a chain other than the longest chain is costly precisely for the set of agents who have the opportunity to add the block. Saleh (2021) leverages that insight and demonstrates that all PoS cryptocurrency holders coordinate on LCR to resolve all forks when the block reward is sufficiently small. The referenced result arises because the block reward serves as a countervailing incentive for an agent to coordinate on adding blocks to the longest chain, because the block reward provides a gain for adding a block even to a shorter chain. When the block reward is sufficiently small, the incentive for an agent to avoid

[9] Many PoS protocols administer the lottery over only a subset of units of the blockchain's cryptocurrency that are selected into the lottery by the holders of the cryptocurrency. Fanti, Kogan & Viswanath (2021) and John, Rivera & Saleh (2021) model such protocols formally.

a loss on her PoS cryptocurrency holding is the dominant incentive; thus, PoS cryptocurrency holders coordinate on a single chain in equilibrium.[10]

Our survey focuses on Bitcoin, PoW, and PoS. While those topics are foundations of the blockchain economics literature, they do not encompass the full literature, which also includes other important topics such as smart contracts, initial coin offerings (ICOs), tokenomics, empirical analysis of cryptocurrency markets, blockchain for business, and most recently, decentralized finance (Defi). For the sake of brevity, we do not discuss any of those topics, instead highlighting influential works in each area for the interested reader below.

Cong & He (2019) study the economic implications of smart contracts. Chod & Lyandres (2021), Gan, Tsoukalas & Netessine (2021), and Li & Mann (2020) theoretically analyze ICOs, whereas Howell, Niessner & Yermack (2020) and Lee, Li & Shin (2021) provide an empirical analyses of ICOs. Cong, Li & Wang (2021) provide a theoretical framework from which to analyze the economics associated with blockchain tokens, whereas Cong, Li & Wang (2022) and Mayer (2021) build upon that framework. Makarov & Schoar (2019) examine apparent arbitrage opportunities in cryptocurrency markets, highlighting important trading frictions. Liu & Tsyvinski (2021) and Liu, Tsyvinski & Wu (2022) empirically examine cryptocurrency risk and return dynamics. Griffin & Shams (2020) and Li, Shin & Wang (2021) study instances of cryptocurrency market manipulation. Chod et al. (2020) and Iyengar et al. (2021) examine the economic implications of blockchain in business settings, with particular focus upon supply chains. Lehar & Parlour (2021), Capponi & Jia (2021), Park (2021), and Harvey, Ramachandran & Santoro (2021) examine the behavior of blockchain-based Defi. Abadi & Brunnermeier (2019) offer a useful abstract description of how distributed ledgers operate.

3. NAKAMOTO

Nakamoto (2008) invented Bitcoin with the aim that it would be the first payment system neither controlled by a centralized entity nor vulnerable to the double-spending problem. Formally, a payment system is not vulnerable to the double-spending problem if the probability of a successful double-spend can be made arbitrarily close to zero. A successful double-spend is defined as an instance in which a user spends the same BTCs twice.

Nakamoto (2008) considers a static environment involving three types of agents: an attacker, a merchant, and Bitcoin miners. The attacker purchases a physical good from the merchant in exchange for some BTCs, with the payment of BTCs from the attacker to the merchant being made via the Bitcoin blockchain. Following this purchase, the attacker seeks to double-spend. For the attacker to be successful, she must gain possession of the merchant's physical good while also regaining ownership of the BTCs used to purchase the physical good. The attacker conducts a successful double-spend in such a case because the attacker maintains possession of the proceeds from an initial spend but has the ability to spend the BTCs from that initial spend a second time.

To gain possession of the physical good while also regaining ownership of the BTCs used for the purchase, the attacker waits to receive delivery of the physical good and then attempts to reverse her payment to the merchant. The reversal of the payment restores the attacker's ownership of the BTCs she initially spent, but it does not affect possession of the physical good, because physical goods cannot be exchanged via the blockchain. Consequently, the attacker's attempt to reverse her payment only after receiving delivery of the physical good ensures that the merchant cannot retaliate and regain possession of the physical good.

[10] Saleh (2021) also examines the long-range attack within appendix B of his paper. For the sake of brevity, we do not discuss that analysis here.

To reverse the attacker's payment to the merchant, she conducts two steps. First, the attacker generates a new chain on the Bitcoin blockchain, with this new chain omitting her payment to the merchant. Second, she induces Bitcoin miners to accept this new chain as the unambiguous Bitcoin blockchain instead of the original chain that includes her payment to the merchant. These two steps imply the reversal of her payment, because if she succeeds, then the Bitcoin miners will have accepted a chain that excludes the attacker's payment to the merchant from the Bitcoin blockchain. In essence, it will be as if the payment never happened, and the attacker will retain the ownership of the BTCs.

To implement the first step of creating a chain that omits the attacker's payment, the attacker forks the blockchain from the block that directly precedes the block that includes her payment to the merchant. More precisely, the attacker creates a new block that solves the same PoW puzzle as the block that includes her payment to the merchant. As previously discussed, this new block cannot be part of the same blockchain as the block that includes the attacker's payment to the merchant, because both blocks solve the same puzzle. Accordingly, the creation of this new block represents a new chain for which the attacker's newly created block is the last block of the chain, and the new chain excludes the attacker's payment to the merchant.

To implement the second step of inducing all Bitcoin miners to accept the attacker's new chain as the unambiguous Bitcoin blockchain, the attacker exploits the previously discussed fact that Bitcoin miners apply LCR to achieve consensus. Thus, the attacker implements the second step by adding blocks to her new chain until and unless the new chain becomes longer than the original chain including the attacker's payment to the merchant.

The attacker's described strategy for double-spending would succeed trivially if the attacker can add blocks to a chain without cost. But if adding a block is costly, then executing a successful double-spend can be made increasingly difficult if the merchant waits before transferring possession of the good to the attacker. This increasing difficulty arises because Bitcoin miners continue to add blocks to the chain including the attacker's payment to the merchant in the time that the merchant waits to transfer the good to the attacker. In turn, the additional blocks increase the initial deficit of the attacker's new chain relative to the original chain including her payment to the merchant. Consequently, to solve the double-spending problem, Nakamoto (2008) both includes a cost for appending a block to the Bitcoin blockchain and advises that merchants wait before transferring physical possession of a good to any buyer. Nakamoto (2008) imposes the cost for appending a block by implementing PoW as the protocol that governs which Bitcoin blocks can be accepted. Recall that PoW specifies a computational puzzle to be solved for a block to be appended to the blockchain, and solving this computational puzzle is costly.

Formally, the number of blocks produced by any miner under PoW follows a Poisson process, with the rate of the process being proportional to the computational power employed by the miner. Nakamoto (2008) takes the computational power of the attacker and the Bitcoin miners as exogenous, so that the number of blocks produced by the attacker over T time units, $\#_A(T)$, and the number of blocks produced by all Bitcoin miners over T time units, $\#_M(T)$, are given by

$$\#_A(T) \sim \mathit{Poisson}(\pi \cdot C_A \cdot T), \qquad \#_M(T) \sim \mathit{Poisson}(\pi \cdot C_M \cdot T), \tag{1.}$$

where $C_A > 0$ denotes the computational power of the attacker, $C_M > 0$ denotes the computational power of all Bitcoin miners, and $\pi \in (0, 1)$ denotes an exogenous constant.

Nakamoto (2008) allows that the merchant waits an exogenous $z \in \mathbb{N}_+$ blocks to be added after the attacker's payment (or for that matter, any payment) enters the blockchain before transferring physical possession of the good. As the attacker's chain has not yet been created at that point, the z blocks are all added to the original chain that includes the attacker's payment to the merchant. Once the attacker receives the good, she attempts to create a new chain by adding a block after the block that precedes the block including her payment to the merchant. Note that this new chain is initially strictly shorter than the original chain, so that the Bitcoin miners would add blocks only to the original chain until and unless the new chain becomes the longest chain. In contrast, the attacker adds blocks only to her new chain. As a consequence, the difference between the lengths of the original chain and the attacker's new chain T time units after the merchant delivers the physical good to the attacker, $\Delta(T)$, is given as follows:[11]

$$\Delta(T) = z + 1 + \#_M(T) - \#_A(T) \text{ for } T \leq \tau, \qquad 2.$$

where $\#_M(T)$ and $\#_A(T)$ are independent Poisson processes with probability laws given by Equation 1, and τ represents the random time at which the attacker's chain becomes the longest chain (if ever). For exposition, we adopt the convention that the attacker's chain is the longest chain if it becomes equally long as the initial chain. Then, τ is given by

$$\tau := \min\{t \geq 0 : \Delta(t) \leq 0\}, \qquad 3.$$

so that the probability of a successful double-spend is given by

$$\mathbb{P}(\text{successful double-spend}) = \mathbb{P}(\tau < \infty). \qquad 4.$$

Equations 1 and 2 imply the following:

$$\mathbb{P}(\tau < \infty) = \begin{cases} \left(\frac{C_A}{C_M}\right)^{z+1} & \text{if } C_M > C_A \\ 1 & \text{if } C_M \leq C_A \end{cases}. \qquad 5.$$

Applying Equation 5 to Equation 4 then yields the main result of Nakamoto (2008):

$$\lim_{z\to\infty} \mathbb{P}(\text{successful double-spend}) = 0 \text{ if } C_M > C_A. \qquad 6.$$

This result is of great practical importance, because it implies that the probability of a double-spend can be made arbitrarily small at the merchant's discretion (i.e., by selecting z sufficiently large) under certain conditions (i.e., if $C_M > C_A$). Recall that z represents the number of blocks that are appended to the original chain after the attacker's payment to the merchant enters the blockchain but before the merchant transfers possession of the physical good to the attacker. The variable z is typically referred to as the number of confirmations, and merchants trading in cryptocurrencies widely adhere to the guidance of Nakamoto (2008) in that it is common for merchants to impose a number of confirmations, z, to mitigate risk.

Note, however, that the argument of Nakamoto (2008) requires that the computational power employed by the attacker, C_A, cannot exceed the computational power employed by all Bitcoin miners, C_M. This requirement is why the computational power of the Bitcoin network is viewed as the main determinant of its security. More formally, Equations 4 and 5 also imply the following:

$$\mathbb{P}(\text{successful double-spend}) = 1 \text{ for all } z \text{ if } C_M \leq C_A, \qquad 7.$$

which establishes that merchants are powerless to reduce the likelihood of a successful double-spend if the computational power of the Bitcoin mining network, C_M, is too low.

Nakamoto (2008) takes the computational power of the Bitcoin mining network as exogenous despite the fact that its level is crucial for Bitcoin to overcome the double-spending problem. This significant gap left in the literature by Nakamoto (2008) is filled by Easley, O'Hara & Basu (2019), who determine Bitcoin's level of mining endogenously.

[11] Nakamoto (2008) allows that the attacker creates blocks before receiving delivery of the good. This allowance does not affect the main result that we discuss but complicates the supporting mathematics. Thus, for exposition, we maintain the simplifying assumption that the attacker cannot create blocks until after she receives delivery of the good.

4. THE ECONOMIC DIMENSIONS OF BITCOIN

Easley, O'Hara & Basu (2019) model a setting with $N \in \mathbb{N}_+$ users. Each User $i \in \{1, \ldots, N\}$ earns transaction surplus $V > 0$ from transacting via the Bitcoin blockchain but also faces a wait disutility of $a > 0$ per unit time that elapses for transaction processing. User i may reduce her total wait disutility by paying a fee, $f > 0$, which reduces her expected wait time, but her utility also decreases in the fee. Formally, User i accrues utility $V(f)$ from transacting via the Bitcoin blockchain when she pays fee f, where

$$V(f) = V - p \cdot f - a \cdot w(f). \qquad 8.$$

Fees are denoted in terms of BTC so that $p \cdot f$ denotes the total cost of the fee, with $p > 0$ denoting the price of BTC. Additionally, $w(f)$ denotes the endogenous expected wait time for User i as a function of her fee, f, so that $a{\cdot}w(f)$ denotes the total expected wait disutility for User i when paying fee f. User i balances her dislike of waiting with her dislike for paying a fee to select her optimal fee, f_i, which is therefore given by

$$f_i = \begin{cases} \arg\max\limits_{f \in \Psi} V(f) & \text{if } \max\limits_{f \in \Psi} V(f) \geq 0 \\ 0 & \text{otherwise} \end{cases}, \qquad 9.$$

where $\Psi \subseteq [0, \infty)$ denotes the set of feasible fee levels. A user may opt not to transact via the Bitcoin blockchain, in which case she receives zero utility. That case occurs only if the utility from transacting via the Bitcoin blockchain is negative [i.e., $\max_{f \in \Psi} V(f) < 0$]. Moreover, in that case, User i pays no fee (i.e., $f_i = 0$).

A transaction is processed once it is included in a block that has been appended to the Bitcoin blockchain. Blocks are added to the Bitcoin blockchain by miners, with each miner producing blocks according to a Poisson process with rate $\lambda > 0$. Easley, O'Hara & Basu (2019) assume that blocks are transmitted through the Bitcoin network instantaneously and that miners add blocks to a single chain so that no forks arise within their analysis.[12] As a consequence, the Bitcoin blockchain receives blocks according to a Poisson process with rate $\Lambda > 0$, where

$$\Lambda = \lambda \times M, \qquad 10.$$

with M denoting the endogenous number of miners.

For each miner, block production involves both fixed and variable costs. In particular, block production involves a fixed cost of purchasing computational hardware, $F > 0$, and a variable cost of electricity per unit time, $e > 0$. The total expected cost incurred by a miner for a PoW computational contest is therefore given by

$$\text{expected mining cost per contest} = \delta F + e \times \frac{1}{\Lambda}, \qquad 11.$$

where $\delta \in (0, 1)$ denotes the depreciation rate of computational hardware and $\frac{1}{\Lambda}$ refers to the expected time required for a PoW computational contest to complete.

Offsetting the referenced costs, whenever a miner creates a block, she receives both a block reward of $S > 0$ BTC and all fees from transactions included in the block. The expected revenue for a miner from a PoW computational contest is thus given by

$$\text{expected mining revenue per contest} = \frac{1}{M} \times p \cdot \left(S + \mathbb{E}\left[\sum f_i\right]\right), \qquad 12.$$

[12] We discuss the implications of allowing for forks in Section 5.

where $\frac{1}{M}$ represents the probability that the miner wins the contest and thus produces the next Bitcoin block and $p \cdot \left(S + \mathbb{E}\left[\sum f_i\right]\right)$ represents the payoff from producing that block. $\sum f_i$ refers to the fees from transactions included in the block. Miners optimally select transactions for inclusion in a block on the basis of descending fee order until the block reaches its capacity.

Bitcoin is designed to allow free entry among miners so that positive expected mining profits would induce entry of miners, whereas negative expected mining profits would induce exit of miners. As a consequence, expected mining profits must equal zero in equilibrium. Easley, O'Hara & Basu (2019) highlight this insight and employ it to deduce the equilibrium number of miners, M, as follows:

$$M = \frac{p\left(S + \mathbb{E}\left[\sum f_i\right]\right)}{\delta F + e/\Lambda}. \qquad 13.$$

The aforementioned result arises from equating Equations 11 and 12 to form a zero-profit condition. This result highlights that the equilibrium number of miners depends positively upon the BTC price and transaction fees paid by users. Thus, relating this finding back to the analysis of Nakamoto (2008), Bitcoin's ability to overcome the double-spending problem depends upon a combination of sufficiently high BTC prices and sufficiently high transaction fees. Nonetheless, since the Bitcoin block reward has been prespecified to eventually equal zero (i.e., $S = 0$ eventually), Easley, O'Hara & Basu (2019) focus upon transaction fees, establishing how they arise endogenously. In particular, solving Equation 9 explicitly shows that the total equilibrium fee revenue depends upon the arrival rate of transactions. When the arrival rate of transactions is low, then equilibrium fees are low. Similarly, when the arrival rate of transactions is high, then equilibrium fees are high.

5. ECONOMIC LIMITATIONS OF BITCOIN

The literature has uncovered several economic limitations of Bitcoin. One particularly significant group of limitations arises because Bitcoin's design enables forks to arise in equilibrium. Forks do not arise in centralized systems, so the associated limitations distinguish Bitcoin from traditional payment systems. We discuss the economic implications of forks within Section 5.1 and highlight other economic limitations in Section 5.2.

5.1. Forks

Hinzen, John & Saleh (2021) consider an economic model similar to that of Easley, O'Hara & Basu (2019) but relax the assumption that Bitcoin blocks are transmitted through the mining network instantaneously. Instead, Hinzen, John & Saleh (2021) allow that the average time to disseminate a single transaction to all other miners, referred to as network delay, equals $\Delta(M)$, where M denotes the equilibrium number of miners. The authors establish that the probability a block produced by any miner corresponds to a fork is given by

$$\mathbb{P}(\text{fork}) = 1 - e^{-\Lambda \times T \times \Delta(M)}, \qquad 14.$$

where, as before, $\Lambda > 0$ denotes the rate at which Bitcoin produces blocks while $T > 0$ denotes the number of transactions per Bitcoin block so that $\Lambda \times T$ equals Bitcoin's transaction rate.

Hinzen, John & Saleh (2021) assume that miners follow LCR, implying that forks can arise in their analysis when miners observe different longest chains. This phenomenon of different miners observing different longest chains occurs precisely due to blocks not being transmitted across the entire mining network instantaneously. Specifically, since time must elapse for a given block to become known to the entire mining network, different miners might observe different chains at any given point in time. As a consequence, two miners might disagree regarding whether a particular block corresponds to the longest chain when each becomes aware of that block. Equation 14 establishes that this phenomenon of disagreement occurs routinely with a particular probability that depends upon not only network delay, $\Delta(M)$, but also Bitcoin's transaction rate, $\Lambda \times T$.

An important insight in Hinzen, John & Saleh (2021) is that the probability of a fork increases in Bitcoin's transaction rate [i.e., P(fork) increases in $\Lambda \times T$], which in turn leads to limited adoption for Bitcoin as a payment system. More precisely, although a centralized payment system may achieve widespread adoption by increasing its transaction rate sufficiently fast so that the payment system becomes desirable for most users, Bitcoin cannot do the same because a high transaction rate leads to forks occurring too frequently. This high frequency of forks drives limited adoption, because such forks must be resolved for payments to be settled, and Hinzen, John & Saleh (2021) also establish that the expected time to resolve forks diverges as the fork probability goes to one.

More formally, akin to Easley, O'Hara & Basu (2019), Hinzen, John & Saleh (2021) assume that Bitcoin users dislike both waiting and paying fees. Hinzen, John & Saleh (2021) demonstrate that fees endogenously increase in congestion so that a low transaction rate for Bitcoin translates to not only long wait times but also high fees. In turn, they demonstrate that Bitcoin does not achieve widespread adoption for low transaction rates because payment processing is too slow and expensive. Of particular note, they also find that Bitcoin does not achieve widespread adoption for high transaction rates. This latter finding arises because an increase in Bitcoin's transaction rate corresponds to the fork probability increasing to one [i.e., $\lim_{\Lambda \times T \to \infty} \mathbb{P}(\text{fork}) = 1$], and an increased fork probability leads wait times to diverge due to an increase in the time needed to resolve forks. Thus, prohibitive wait times result irrespective of the transaction rate, and limited adoption arises for Bitcoin as a consequence.

While Hinzen, John & Saleh (2021) assume that miners follow LCR, Biais et al. (2019) allow that miners strategically decide to which chain to add a block. In such a context, Biais et al. (2019) establish that there exists an equilibrium in which miners purposefully create a fork and that the fork persists indefinitely. This persistent forking equilibrium is particularly problematic, because it implies a perpetual disagreement regarding what constitutes the Bitcoin blockchain.

Biais et al. (2019) highlight that the probabilistic manner in which blocks are generated implies that a sequence of blocks produced might disproportionately favor a minority subset of miners. In such a case, the complementary majority subset of miners have an incentive to ignore this recent sequence of blocks by forking the blockchain, starting from a block preceding the streak that favors the minority subset of miners. The authors establish incentive compatibility for the majority subset to add blocks to this new chain in perpetuity, simultaneous to the minority subset continuing to add blocks to the original chain, thereby establishing a persistent forking equilibrium.

Biais et al. (2019) assume that the market value of a block reward depends upon the number of miners adding blocks to the chain on which the block reward is earned. Then, since more miners add blocks to the new chain in equilibrium, any miner who accrues block rewards on the new chain earns a higher reward than a miner accruing block rewards on the old chain. This higher block reward for miners adding blocks to the new chain creates an incentive for miners to abandon the old chain in favor of the new chain. This incentive is sufficient for miners in the majority subset to abandon the old chain in favor of the new chain, but it is not sufficient for miners in the minority subset who have accrued a disproportionate share of block rewards on the old chain. Importantly, a miner abandoning the old chain implies fewer miners adding blocks to that chain and thus a lower market value for block rewards from that chain. Consequently, abandoning the old chain entails imposing a loss on block rewards received on the old chain. This loss is especially costly for the minority subset of miners, because they possess a large quantity of block rewards on the old chain. Biais et al. (2019) demonstrate that the cost of abandoning the old chain is sufficiently large for the minority subset of miners, so that they add blocks only to the old chain in perpetuity. Then, since the majority subset abandons the old chain and adds blocks only to the new chain, the described equilibrium constitutes a persistent forking equilibrium.

Biais et al. (2019) also establish existence of another equilibrium in which all miners follow LCR in perpetuity. This equilibrium arises because any miner deviating to create a fork receives negligible block rewards from doing so. Consequently, no miner benefits in deviating from LCR when all other miners follow LCR.

Harvey, Ramachandran & Santoro (2021) provide a different perspective on forks, viewing them as a mechanism to incentivize efficiency. These authors are particularly focused on what is known as Defi, which involves smart contract platforms often built on the Ethereum blockchain. They argue that forks create competition and provide the best possible platforms. They also identify a potential problem, or what they call a complicating factor, termed vampirism, in which near exact copies of an existing platform attempt to poach liquidity from the existing platform. These developments suggest that forks will continue to be an important issue for blockchains going forward.

5.2. Other Limitations

Beyond the implications of forks, various papers have highlighted other important economic limitations arising within Bitcoin. These limitations include instability of fees (Basu et al. 2021), extreme volatility (Pagnotta 2022), front-running issues (Aune et al. 2017), vulnerability to attack (Eyal & Sirer 2014; Narayanan et al. 2016), and extreme energy expenditure (de Vries 2018).

5.2.1. Fee instability. Basu et al. (2021) establish that Bitcoin's mechanism for setting fees induces instability in the level of fees. They argue that this instability arises because Bitcoin's current fee mechanism implies an equilibrium strategy for users that depends upon parameters not typically known to a user. As a remedy, they offer an alternative fee mechanism. Under that alternative fee mechanism, Basu et al. (2021) demonstrate the existence of an approximate equilibrium in which each user sets her fee using only her private information rather than needing to rely upon parameters that are likely to be difficult to ascertain in practice.

More formally, Basu et al. (2021) model a finite number of Bitcoin users, each of whom accrues some utility from having her transaction included in the next Bitcoin block. The utility accrued to each user, a user's private valuation, is generated as a draw from an exogenous distribution. Users set their fees without observing the fees of any other users. Miners then produce a block by including the transactions with the highest fees until the block is full. Any user with a transaction included in the block accrues total utility equal to her private valuation minus her fee. All other users accrue zero utility.

An important insight of Basu et al. (2021) is that the Bitcoin fee-setting mechanism corresponds to a first-price sealed-bid auction (FPSBA) with multiple identical goods. User fees are akin to auction bids, and being included in the subsequent block is akin to winning one of the identical goods. In turn, the equilibrium user strategy under Bitcoin's current fee-setting mechanism is the well-known equilibrium bidding strategy for a FPSBA. This strategy, however, depends upon the exogenous distribution from which private valuations are drawn, and that distribution is difficult to obtain. As a consequence, such a mechanism is likely to induce fee instability in practice just as observed for Bitcoin.

To overcome the referenced instability, Basu et al. (2021) propose an alternative mechanism by which (*a*) a Bitcoin user is required to pay the minimum fee offered by any transaction on the block that includes the user's transaction and (*b*) the fee paid to the miner of any block is based on the average fees over the last *n* blocks. This mechanism approximates a second-price sealed-bid auction (SPSBA). Importantly, the SPSBA induces truth-telling as a dominant strategy, so that all users bidding their private valuations constitutes an equilibrium. As *n* grows large, it also reduces the incentive of miners to manipulate fees by introducing extraneous transactions. Basu et al. (2021) demonstrate that the analogous strategies of all users setting fees equal to their private valuations constitutes an approximate equilibrium under their proposed alternative mechanism. This approximate equilibrium becomes exact in the limit as the number of Bitcoin users grows.

5.2.2. Extreme volatility. Pagnotta (2022) demonstrates that BTC's extreme volatility arises due to the design of the underlying Bitcoin blockchain. More precisely, Pagnotta (2022) demonstrates that an increase in the number of users transacting via the Bitcoin blockchain generates an increase in BTC prices beyond that which would arise in a typical setting. This effect also applies in the downward direction, so that a decrease in users transacting via the Bitcoin blockchain generates a decrease in BTC prices beyond that which would arise in a typical setting. Since the described effect applies in both the upward and downward directions, it implies extreme volatility for BTC.

Formally, Pagnotta (2022) considers a model in which Bitcoin users value not having their transactions reversed and allows for endogenous BTC prices in that setting. An increase in the number of users transacting via the Bitcoin blockchain results in not only a direct increase in demand for BTC but also an amplification effect due to the design of the Bitcoin blockchain. The referenced direct increase in demand for BTC implies higher BTC equilibrium prices, and those higher BTC equilibrium prices imply an increase in mining revenues via an increase in the value of block rewards. In turn, an increase in mining revenues induces higher computational expenditures by miners, which results in a lower probability that any attacker could successfully reverse a transaction on the Bitcoin blockchain. Since users value not having their transactions reversed, the described reduction in the likelihood of a transaction reversal generates additional demand for BTC. This additional demand amplifies the initial increase in demand, leading to commensurately higher BTC prices. The same amplification occurs in the downward direction; thus, the Bitcoin blockchain's design leads to extreme volatility of BTC.

5.2.3. Front-running and manipulation. The process of gathering transactions for inclusion in a block sets up the potential for miner front-running in distributed ledgers. This problem arises because transactions are not immediately posted to the blockchain but rather are held in mempools, where they await selection for inclusion in a block. There is no time priority in the mempool, so transactions are selected at the discretion of the miner. Aune et al. (2017) demonstrate how, in a trading context, this gives miners advance information of pending activity and so can allow the miner to step in front of a user's transaction. These authors suggest a mechanism to reduce this front-running problem but argue that it remains a concern for any distributed ledger system. Such front-running behavior can also contribute to fee instability, as miners, seeing the orders in the mempool, insert their own orders ahead of pending orders to strategically affect transaction fees (see Basu et al. 2021).

5.2.4. Vulnerability to attack. Another area of concern is the vulnerability of the blockchain to attack by malicious actors. Attacks can occur in a variety of ways. Eyal & Sirer (2014) identify problems connected with selfish mining, which arises when a miner hides a solved block while trying to find the next block before the network does. If successful, the miner can publish the two blocks, causing the network to waste computational power to find a block that the selfish miner can immediately cause to be stale. This strategy increases the selfish miner's effective computational power and thus expected profits, but it can also spread as other rational miners decide to join with the selfish miners. As the colluding group grows, Bitcoin ceases to be decentralized. These authors demonstrate that such an outcome can occur even when the level of selfish mining controls less than a majority of the computational power.

Punitive forking is another vulnerability that can undermine the functioning of the blockchain. Here, the goal is to blacklist certain Bitcoin addresses believed to be owned by particular people, so that they can never spend any of their BTCs. These actions can be motivated by greed (pay me, so that I do not blacklist you) or other motivations (a government orders certain addresses to be blacklisted by miners whom they can control); however, in any case, successful punitive forking requires controlling a majority of the computational power. There are a wide variety of similar strategies (feather forking and the like), all of which pervert the efficacy of the blockchain protocol.

5.2.5. Extreme energy expenditure. The most prominent and longstanding concern associated with Bitcoin is the extreme energy expenditure generated by the Bitcoin mining network. de Vries (2018) examines the level of this expenditure empirically and finds that Bitcoin expends energy at a level comparable with that of countries such as Austria and Ireland. Benetton, Compiani & Morse (2021) investigate the negative spillovers of Bitcoin mining on local communities. Adding to this concern, Cong, He & Li (2021) demonstrate that financial innovations have strengthened incentives for miners to expend computational power. In turn, these concerns have led the blockchain community to explore alternatives to the design of Bitcoin—the most prominent such alternative being the use of PoS to replace PoW in determining which blocks should be accepted to the blockchain.

6. PROOF-OF-STAKE

The viability of PoS as an alternative to Bitcoin was initially in question due to two potential problems: the double-spending problem and the nothing-at-stake problem. A further concern associated with PoS is that PoS cryptocurrency wealth shares might tend toward concentration. We now consider the economic models addressing these concerns.

6.1. Double-Spending Problem

Saleh (2021) considers an environment with three types of agents: an attacker, a merchant, and cryptocurrency holders. The attacker transacts with the merchant via the blockchain, sending the merchant cryptocurrency in return for a physical good. The attacker has the singular goal of committing a double-spend against the merchant. To commit that double-spend, the attacker acquires possession of the merchant's physical good and then reverses her payment to the merchant. The payment reversal returns the cryptocurrency used by the attacker to purchase the physical good but does not return possession of the physical good. The described course of action thus corresponds to a double-spend, because it enables the attacker to spend once to acquire the physical good and then spend the same units of cryptocurrency again after the first payment is reversed.

The setting of Saleh (2021) parallels that examined by Nakamoto (2008). The primary difference arises in the manner in which the blockchain is updated. Nakamoto (2008) assumes that blockchain updates follow the PoW protocol, whereas Saleh (2021) assumes that blockchain updates follow the PoS protocol. Concretely, Saleh (2021) assumes that time is subdivided into discrete intervals known as slots. During each slot, each existing chain of the PoS blockchain holds a lottery over all cryptocurrency units, with each cryptocurrency unit being equally likely to be selected. Any owner of a winning cryptocurrency unit on a particular chain receives the option to append a block to the end of that chain. All lotteries are conducted independently of each other.

To execute the double-spend, the attacker waits to receive possession of the physical good and then forks the blockchain from the block directly preceding the block that includes her payment to the merchant. If the attacker's new chain becomes the unambiguous blockchain, then the payment to the merchant has been reversed because that payment does not appear on the new chain by construction. Saleh (2021) assumes that all cryptocurrency holders (except the attacker) follow LCR so that they add blocks only to the original chain including the attacker's payment to the merchant until and unless the attacker's new chain becomes equally long as the original chain. If the attacker's chain becomes longer than the original chain, then all cryptocurrency holders abandon the original chain and add blocks only to the attacker's chain, thereby making the attacker's chain the unambiguous blockchain and also rendering the attacker's double-spend successful. The attacker anticipates the described behavior and thus adds blocks only to her new chain, hoping that her chain will eventually become longer than the initial chain, thereby rendering her double-spend successful. The merchant anticipates the behavior of both the cryptocurrency holders and the attacker and consequently withholds transferring possession of any physical goods to any buyer for $z \in \mathbb{N}_+$ blocks after that buyer's payment to the merchant enters the blockchain.

Note that once the attacker has forked the blockchain, the blockchain involves two chains. Then, following the prior discussion, there are two lotteries per time slot—one for each chain. The outcomes of the lotteries in one time slot can be grouped into three categories defined by the three possibilities of the number of lotteries that the attacker wins (0, 1, or 2). In turn, each of the three possibilities has an unambiguous effect on the difference between the length of the two chains. Specifically, if the attacker wins both lotteries, she adds a block to her own chain but not to the original chain so that her chain advances on the original chain by one block, bringing her closer to a successful double-spend. Alternatively, if the attacker wins neither lottery and her chain has not already become the longest chain, then the other cryptocurrency holders follow LCR and add a block only to the original chain and not the attacker's chain. Such a course of action increases the deficit of the attacker's chain by one block and thereby undermines the likelihood that the attacker's chain ever becomes the longest chain. Finally, if the attacker wins exactly one lottery, then the difference in the length of the two chains remains unchanged.[13]

Saleh (2021) assumes that the attacker does not hold any cryptocurrency initially but that the attacker may endogenously amass a holding by purchasing cryptocurrencies. Saleh (2021) assumes that the attacker finances any purchases at an interest rate $r > 0$ and faces a borrowing constraint $B > 0$. Then, with $\mathcal{M}^{PoS}$ denoting the market value of the PoS cryptocurrency, Saleh (2021) establishes the following result:

$$\lim_{z\to\infty} \mathbb{P}(\text{successful double-spend}) = 0 \text{ if } \mathcal{M}^{PoS} \text{ is sufficiently large.} \qquad 15.$$

This result parallels the main result of Nakamoto (2008), in that it establishes that the probability of a successful double-spend vanishes as the number of confirmations, z, diverge. Note, however, that the result of Nakamoto (2008) requires that the computational power of the Bitcoin mining network is sufficiently high, whereas the result of Saleh (2021) requires that the market value of the cryptocurrency is sufficiently large and that the attacker faces a borrowing constraint. This difference reflects that taking control of Bitcoin requires amassing sufficient mining power to have an advantage in winning subsequent PoW computational contests, whereas taking control

[13] If the attacker wins the lottery on her own chain, then she adds a block to that chain, but the winner of the lottery on the original chain also adds a block to the original chain. If the attacker wins on the original chain, then she neglects to add a block on the original chain, but the winner of the lottery on the attacker's chain also neglects to add a block to the attacker's chain. In either case, the difference in the length of the chains is preserved.

of a PoS blockchain requires amassing a sufficient proportion of cryptocurrency units to have an advantage in winning subsequent PoS lotteries. In turn, since the cost of acquiring a fixed proportion of cryptocurrency units increases in the cryptocurrency market value, a sufficiently high cryptocurrency market value renders a PoS blockchain resistant to double-spending.

6.2. Nothing-at-Stake Problem

The nothing-at-stake problem alleges that any chain on a PoS blockchain would receive blocks in perpetuity, so that the appearance of multiple chains, by itself, leads to perpetual ambiguity regarding which chain of blocks represents the blockchain. Saleh (2021) examines the nothing-at-stake problem formally and establishes that it is incentive compatible for all cryptocurrency holders to coordinate on the longest chain (and abandon all other chains) so long as the blockchain possesses sufficiently low block rewards. This result implies that the nothing-at-stake problem can be averted with sufficiently modest block rewards.

Saleh (2021) shows that appending a block to a chain that is not the longest chain entails both earning a block reward and reducing the value of the cryptocurrency. Consequently, since PoS enables only those who hold cryptocurrency units to add blocks, any agent who appends a block to a chain that is not the longest chain imposes a cost upon herself in the form of devaluation of her cryptocurrency holdings. For a sufficiently low block reward, the referenced cost outweighs the benefit of the block reward gained from appending the block, so that all cryptocurrency holders coordinate on the longest chain and the nothing-at-stake problem is overcome.

A key point in this argument is that appending a block to a chain that is not the longest chain has a negative impact on the value of the cryptocurrency. This effect arises because appending a block on a chain that is not the longest chain exacerbates ambiguity regarding which chain of blocks represents the blockchain. In turn, this ambiguity undermines the ability of cryptocurrency holders to exchange their cryptocurrency units expediently and reduces cryptocurrency value commensurately.

6.3. Wealth Concentration

Rosu & Saleh (2021) model a PoS blockchain in an infinite horizon economy with finitely many risk-neutral investors. The investors possess exogenous endowments, but their cryptocurrency holdings are determined endogenously in each period. In that context, Rosu & Saleh (2021) establish that PoS cryptocurrency wealth shares possess the martingale property in that the expected value of an investor's cryptocurrency wealth share in the next period equals its value in the current period.

An important finding that contributes to this result is that investors do not have an incentive to amass a large cryptocurrency holding despite a larger cryptocurrency holding increasing the probability of accruing subsequent block rewards. To understand this point, it is important to recognize that any cryptocurrency units purchased face dilution due to future block rewards increasing the number of outstanding cryptocurrency units. Consequently, a purchase of cryptocurrency units involves a trade-off that weighs increased expected future block rewards against the loss in value of the purchased cryptocurrency units due to dilution. Rosu & Saleh (2021) establish that the two effects offset in equilibrium and thus investors do not endogenously enlarge their cryptocurrency holdings via trading.

7. WHAT LIES BEYOND...

The blockchain literature has demonstrated various important economic findings regarding Bitcoin, PoW, and PoS. This survey provides an overview of several such findings, along with context regarding the models that generate those findings. A particular point of focus has been to highlight the complex interplay between the security-based protocols of the Bitcoin blockchain and the economic interactions of the participants in the Bitcoin ecosystem. This interplay sets the stage for our offering brief reflections on what comes next.

What is incontrovertible is that Bitcoin, and the blockchain revolution it fostered, is now a permanent feature of the digital economy. What is less clear is the consensus structure that will underpin future developments. While it seems highly likely that Bitcoin will remain based on PoW, the environmental issues connected with this consensus protocol seem out of touch with modern economic realities. There are a growing number of alternative blockchains using variants of PoS or even newer consensus protocols. For example, Avalanche, which was introduced in September 2020, uses a sampling-based consensus structure, a mechanism that avoids the wasteful electricity use inherent in PoW. Ethereum, the second-most prominent blockchain, has announced plans to shift to a PoS structure in the future. With much of the new Defi taking place on the Ethereum platform, the shift away from PoW seems well underway. Such a shift is consistent with reducing the dichotomy between the economic and security features of blockchains we have discussed here.

A second area of development going forward surrounds the issue of scalability. Scalability problems arise because blockchains based on PoW protocols have fixed capacity dictated by the need for every transaction to be appended to the chain by miners. Moreover, as discussed earlier, increasing the capacity constraint of a PoW blockchain does not resolve scalability problems, because such an increase leads to a higher rate of forks, which in turn prolongs transaction settlement times. With the ever-increasing popularity of Bitcoin and Ethereum, both blockchains have faced difficulties processing existing transactions, with little headroom to provide capacity for future growth. This has engendered extensive research, largely in the computer science literature, to find better approaches to scaling, latency, and other physical limitations of the blockchain. Examples of such approaches are Prism (Bagaria et al. 2019), GHOST (Kiayias & Panagiotakos 2017), and Bitcoin-NG (Eyal et al. 2016).[14] Shifting to an alternative consensus protocol may help—in fact, John, Rivera & Saleh (2021) demonstrate that PoS possesses a scaling advantage over PoW. Harvey, Ramachandran & Santoro (2021) discuss how vertical and horizontal scaling techniques are also being applied to increase capacity. Vertical scaling shifts all transaction processing to a single machine, while horizontal scaling (also called sharding) divides the processing work over multiple blockchains (for more discussion, see Harvey, Ramachandran & Santoro 2021). Which approach proves more successful remains to be seen, but the underlying capacity problems have risen to a point that continued growth of the blockchains is in jeopardy. The search for how to increase blockchain throughput will be an important area of future development.

Finally, the current near-explosive growth of Defi makes clear how important this area will be in the future. Defi rests on blockchains, and the varied activities it allows speaks to a future financial system reliant not on centralized intermediaries but on smart contracts in decentralized settings. How well such a system will work, and how quickly we get there, remains to be seen.

DISCLOSURE STATEMENT

M.O. is an advisor to a cryptocurrency company; however, this company is not Bitcoin related, and her role does not bias this review. The authors are not aware of any other affiliations, memberships, funding, or financial holdings that might be perceived as affecting the objectivity of this review.

[14] Prism, for example, proposes decoupling the proposition, validation, and confirmation of blocks, something that is currently done by single miners in the Bitcoin blockchain. For a discussion of how Prism and other proposed systems work, see Bagaria et al. (2019).

LITERATURE CITED

Abadi J, Brunnermeier M. 2019. *Blockchain economics*. Work. Pap., Princeton Univ., Princeton, NJ

Aune RT, Kellenstein A, O'Hara M, Slama O. 2017. Footprints on a blockchain: trading and information leakage in distributed ledgers. *J. Trading* 12(3):5–13

Bagaria V, Kannan S, Tse D, Fanti G, Viswanath P. 2019. Prism: deconstructing the blockchain to approach physical limits. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 585–602. New York: Assoc. Comput. Mach.

Basu S, Easley D, O'Hara M, Sirer E. 2021. *StableFees: a predictable fee market for cryptocurrencies*. SSRN Work. Pap. 3318327

Benetton M, Compiani G, Morse A. 2021. *When cryptomining comes to town: high electricity-use spillovers to the local economy*. Work. Pap., Univ. Calif., Berkeley

Biais B, Bisière C, Bouvard M, Casamatta C. 2019. The blockchain folk theorem. *Rev. Financ. Stud.* 32:1662–715

Biais B, Bisière C, Bouvard M, Casamatta C, Menkveld AJ. 2020. *Equilibrium Bitcoin pricing*. Work. Pap. 48, EconPol Europe, Munich

Capponi A, Jia R. 2021. *The adoption of blockchain-based decentralized exchanges*. Work. Pap., Columbia Univ., New York, NY

Carlsten M, Kalodner H, Weinberg SM, Narayanan A. 2016. On the instability of Bitcoin without the block reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 154–67. New York: Assoc. Comput. Mach.

Chaum D. 1983. Blind signatures for untraceable payments. In *Advances in Cryptology*, ed. D Chaum, RL Rivest, AT Sherman, pp. 199–203. Boston: Springer

Chod J, Lyandres E. 2021. A theory of ICOs: diversification, agency, and information asymmetry. *Manag. Sci.* 67(10):5969–6627

Chod J, Trichakis N, Tsoukalas G, Aspegren H, Weber M. 2020. On the financing benefits of supply chain transparency and Blockchain adoption. *Manag. Sci.* 66:4378–96

Cong LW, He Z. 2019. Blockchain disruption and smart contracts. *Rev. Financ. Stud.* 32:1754–97

Cong LW, He Z, Li J. 2021. Decentralized mining in centralized pools. *Rev. Financ. Stud.* 34:1191–235

Cong LW, Li Y, Wang N. 2021. Tokenomics: dynamic adoption and valuation. *Rev. Financ. Stud.* 34:1105–55

Cong LW, Li Y, Wang N. 2022. Token-based platform finance. *J. Financ. Econ.* 144:972–91

de Vries A. 2018. Bitcoin's growing energy problem. *Joule* 2:801–5

Easley D, O'Hara M, Basu S. 2019. From mining to markets: the evolution of Bitcoin transaction fees. *J. Financ. Econ.* 134:91–109

Eyal I, Gencer AE, Sirer EG, van Renesse R. 2016. Bitcoin-NG: a scalable blockchain protocol. In *Proceedings of the 13th USENIX Conference on Networked Systems Design and Implementation*, pp. 45–59. Santa Clara, CA: USENIX Assoc.

Eyal I, Sirer EG. 2014. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science, Vol. 8437*, ed. N Christin, R Safavi-Naini, pp. 436–54. Berlin: Springer

Fanti G, Kogan L, Viswanath P. 2021. *Economics of proof-of-stake payment systems*. Work. Pap., Carnegie Mellon Univ., Pittsburgh

Gan J, Tsoukalas G, Netessine S. 2021. Inventory, speculators, and initial coin offerings. *Manag. Sci.* 67:914–31

Genser AE, Basu S, Eyal I, van Renesse R, Sirer EG. 2018. Decentralization in Bitcoin and Ethereum networks. In *Financial Cryptography and Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26–March 2, 2018, Revised Selected Papers*, ed. S Meiklejohn, K Sako, pp. 439–57. Berlin: Springer

Griffin J, Shams A. 2020. Is Bitcoin really un-tethered? *J. Finance* 75:1913–64

Haber S, Stornetta WS. 1991. How to time-stamp a digital document. *J. Cryptol.* 3:99–111

Harvey C, Ramachandran A, Santoro J. 2021. *DeFi and the Future of Finance*. Hoboken, NJ: Wiley

Hinzen FJ, John K, Saleh F. 2021. Bitcoin's limited adoption problem. *J. Financ. Econ.* 144(2):347–69

Howell ST, Niessner M, Yermack D. 2020. Initial coin offerings: financing growth with cryptocurrency token sales. *Rev. Financ. Stud.* 33:3925–74

Huberman G, Leshno JD, Moallemi C. 2021. Monopoly without a monopolist: an economic analysis of the Bitcoin payment system. *Rev. Econ. Stud.* 88(6):3011–40

Irresberger F, John K, Mueller P, Saleh F. 2021. *The public blockchain ecosystem: an empirical analysis.* Work. Pap., Stern Sch. Bus., New York Univ., New York, NY

Iyengar G, Saleh F, Sethuraman J, Wang W. 2021. *Economics of permissioned blockchain adoption*. Work. Pap., Columbia Univ., New York, NY

John K, Rivera T, Saleh F. 2021. *Economic implications of scaling blockchains: why the consensus protocol matters.* Work. Pap., Stern Sch. Bus., New York Univ., New York, NY

Kiayias A, Panagiotakos G. 2017. On trees, chains and fast transactions in the blockchain. In *Progress in Cryptology—LATINCRYPT 2017. 5th International Conference on Cryptology and Information Security in Latin America*, ed. T Lange, O Dunkelman, pp. 327–51. Cham, Switz.: Springer

King S, Nadal S. 2012. *PPCoin: peer-to-peer crypto-currency with proof-of-stake.* Work. Pap. **https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf**

Lee J, Li T, Shin D. 2021. The wisdom of crowds in FinTech: evidence from initial coin offerings. *Rev. Corp. Finance Stud.* 11(1):1–46

Lehar A, Parlour C. 2021. *Decentralized exchanges.* Work. Pap., Univ. Calgary, Can. **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3905316**

Li J, Mann W. 2020. *Digital tokens and platform building.* SSRN Work. Pap. 3088726

Li T, Shin D, Wang B. 2021. *Cryptocurrency pump-and-dump schemes.* Work. Pap., Univ. Florida, Gainesville. **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3267041**

Liu Y, Tsyvinski A. 2021. Risks and returns of cryptocurrency. *Rev. Financ. Stud.* 34:2689–727

Liu Y, Tsyvinski A, Wu X. 2022. Common risk factors in cryptocurrency. *J. Finance* 77:1133–77

Makarov I, Schoar A. 2019. Trading and arbitrage in cryptocurrency markets. *J. Financ. Econ.* 135:293–319

Mayer S. 2021. *Token-based platforms and speculators*. SSRN Work. Pap. 3471977

Nakamoto S. 2008. *Bitcoin: a peer-to-peer electronic cash system.* Work. Pap. **https://bitcoin.org/bitcoin.pdf**

Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ: Princeton Univ. Press

Narayanan A, Clark J. 2017. Bitcoin's academic pedigree. *Commun. ACM* 60(12):36–45

Pagnotta ES. 2022. Decentralized money: Bitcoin prices and blockchain security. *Rev. Financ. Stud.* 35(2):866–907

Park A. 2021. *The conceptual flaws of constant product automated market making*. Work. Pap., Univ. Toronto, Toronto

Rosu I, Saleh F. 2021. Evolution of shares in a proof-of-stake cryptocurrency. *Manag. Sci.* 67:661–72

Saleh F. 2021. Blockchain without waste: proof-of-stake. *Rev. Financ. Stud.* 34:1156–90

Annual Review of Financial Economics

Volume 14, 2022

Contents

Indexes

Errata

An online log of corrections to *Annual Review of Financial Economics* articles may be found at http://www.annualreviews.org/errata/financial