How Should We Regulate Cryptocurrencies via Consensus?: A Strategic Framework for Optimal Legal Transaction Throughput

ADITYA AHUJA, Indian Institute of Technology Delhi, India
VINAY RIBEIRO, Indian Institute of Technology Bombay, India
RANJAN PAL, Massachusetts Institute of Technology, USA

Permissionless blockchain consensus protocols have been leveraged for defining decentralized economies for the (commercial or private) trade of virtual and physical assets, using cryptocurrencies. In most instances, the assets being traded are *regulated*, which mandates that the legal right to their trade and their trade value are determined by the governmental regulator of the jurisdiction in which the trade occurs. Unfortunately, existing blockchains do not formalize proposal of legal cryptocurrency transactions, as part of the execution of their respective consensus protocols, resulting in illegal activities in the associated crypto-economies. In this contribution, unlike existing non-consensus solutions, which are prone to be more compute-time and audit-time intensive, we present a novel regulatory framework for blockchain protocols, for ensuring legal transaction confirmation as part of the blockchain consensus. As per our regulatory framework, we derive, through a stochastic game analysis, block proposal strategies under which legal transaction throughput supersedes throughput of traditional transactions, which are, in the worst case, an indifferentiable mix of legal and illegal transactions. Finally, we show that when a majority of the consensus protocol participants are licensed by the regulator to propose legal transactions, there exists a fair consensus execution policy to maximize the legal transaction throughput in the blockchain network.

CCS Concepts: • **Applied computing** → **Digital cash**; • **Social and professional topics** → **Governmental regulations**; • **Computing methodologies** → *Distributed algorithms;*

Additional Key Words and Phrases: Legal cryptocurrency transactions, regulated blockchain consensus protocols, regulated blockchain stochastic games, Nash Equilibria

ACM Reference format:
Aditya Ahuja, Vinay Ribeiro, and Ranjan Pal. 2023. How Should We Regulate Cryptocurrencies via Consensus?: A Strategic Framework for Optimal Legal Transaction Throughput. *Distrib. Ledger Technol.* 2, 1, Article 4 (March 2023), 20 pages.
https://doi.org/10.1145/3567593

1 INTRODUCTION

Decentralized financial institutions are a novel, emerging economic infrastructure. These institutions are based predominantly on cryptocurrencies for the trade of assets, both physical and virtual. The collective market capitalization of cryptocurrencies peaked to $2 trillion in April 2021 [6]. This shows promise in the long-term

Prior to this publication, this work was unpublished, but was accepted as a peer-reviewed presentation at the Conference on Information Systems and Technology (CIST 2021), a conference that does not have publication proceedings.
Authors' addresses: A. Ahuja, Indian Institute of Technology Delhi, Hauz Khas, New Delhi, Delhi 110016, India; email: aahuja85@gmail.com; V. Ribeiro, Indian Institute of Technology Bombay, Powai, Mumbai, Maharashtra 400076, India; email: vinayr@iitb.ac.in; R. Pal, 77 Massachusetts Ave, Cambridge, MA 02139, United States; email: ranjanp79@mit.edu.

2769-6472/2023/03-ART4 $15.00
https://doi.org/10.1145/3567593

presence and viability of cryptocurrency-based markets, in competition with (and possibly as a replacement of) federally administered centralized financial institutions. However, these cryptocurrency-based markets survive solely on the correctness of the underlying computational principles, which are a basis of the efficacy of these economies. More specifically, to sustain these cryptocurrency-based decentralized economies, blockchain consensus protocols serve as a technical foundation.

Existing blockchain protocols for cryptocurrencies are designed keeping in mind one of (or any combination of) the following system goals: *speed, security, and decentralization*. Unfortunately, these system goals are necessary but insufficient: illegal activities propelled through the strategic use of blockchain-based cryptocurrencies is a serious problem staring at the face of many world governments today [33]. These illegal activities exploit the permissionless nature of the blockchain networks for illegal trade, to strategically defeat regulation by obfuscating the jurisdictions of the blockchain users through anonymity, making federal legal rules inapplicable [24]. In this contribution, we introduce a fourth pillar of correctness for ensuring confidence in blockchain-based cryptocurrencies: *legality*. Specifically, superior to the appealing yet counterproductive strategy of banning cryptocurrencies that can be leveraged for illegal trade, we address the problem of constructing an on-chain regulatory system for the legal trade of *regulated assets:* assets (such as commodities, real-estate, copyrighted digital content, etc.) whose value and trade terms are overseen by their respective governments, through a novel framework having on-chain verifiable legal cryptocurrency transactions and on-chain verifiable regulated consensus protocol participation. We believe we are the first to take such a regulatory approach.

For fear of legal scrutiny and prosecution, law abiding cryptocurrency blockchain users may sign up and get authorization from their respective governments (for both (a) off-chain regulatory frameworks, such as BitLicense in New York, USA [4] or MiCA in the EU [41], and (b) the on-chain regulatory system that we propose) to commit solely to legal cryptocurrency-based trade of regulated assets. However, this does not preclude illegal transactions going on-chain. Remembering that the blockchain network is permissionless, there will always exist unregulated transactors and executors of the consensus protocol, outside regulatory jurisdictions, that propose and mine/validate dubious transactions having an indeterminate legal status, while faithfully following the consensus protocol. Consequently, there opens up a competition in dubious versus legal block proposal between unregulated and regulated consensus protocol executors, respectively, and that competition is dependent on how much consensus resource (for instance, mining hashrate in proof-of-work blockchains and stake in proof-of-stake blockchains) in the blockchain network, do the regulated consensus protocol executors possess as a whole. This finally results as a problem for the federal regulatory body to strategically decide on how much consensus resource to license in the blockchain network, and what block proposal strategies to advise to the regulated consensus protocol executors, for reasonable guarantees on legal transaction throughput.

The resultant open questions that we address, are: *(i) given a permissionless blockchain network for cryptocurrency-based regulated asset trade, can there exist a framework where, without violating the protocol compatibility or degrading the anonymity/privacy of the blockchain users, legal transactions can be clearly identified and confirmed in the blockchain network?; and (ii) can we derive conditions, as a function of the regulated consensus resource in the blockchain network, in which legal transaction throughput supersedes dubious transaction throughput?*

Our Research Contributions

We highlight the need for regulatory frameworks for cryptocurrencies, through a case study of the Silk Road darknet online market [15, 34] (Section 2), after which we make the following contributions:

(1) (A Regulatory Framework). We motivate the need for regulating cryptocurrency blockchains at the consensus layer (Section 3.1), and provide a regulated blockchain consensus system with a novel on-chain evidence of both legal transactions and licensed consensus protocol execution by regulated executors,

where the goal of the protocol executors is to maximize their rewards from protocol participation, and the regulator's mandate is to maximize the legal transaction throughput in the blockchain (Section 3).

(2) (Block Proposal Competition). Consequent to our regulated consensus framework, there ensues a competition in block proposal between regulated and unregulated consensus executors. This competition results in the blockchain state evolving as a consensus strategy-based random process. We motivate the formalization of this competition through a two-player stochastic game [31] inspired from References [20, 22] (Section 4), and we show that:
   (a) *(Under Immediate Block Release [20]).* When the regulator licenses between 58% and 100% of the consensus resource, the unregulated executors can do no better than adding legal blocks at the end of the longest branch of legal blocks (Section 4.3), thereby maximizing the legal transaction throughput.
   (b) *(Under Immediate Block Release with an Oversight Compliance Fee [22]).* When the regulator licenses between 50% and 58% of the consensus resource, given that the regulator incentivizes to build on the branch of legal blocks with a pay forward scheme (similar to Reference [22]), the unregulated executors can do no better than adding legal blocks at the end of the longest branch of legal blocks (Section 4.4), again maximizing the legal transaction throughput.
   (c) *(Under Strategic Block Release [11, 20]).* When the regulator licenses between 33% and 50% of the consensus resource, given that regulated executors strategically release a subset of the blocks notarized by them (similar to the selfish mining attacks [11, 30]), and the unregulated executors faithfully follow the longest branch rule, the regulated executors can prune/orphan some notarized but unconfirmed dubious blocks to increase the legal transaction throughput, beyond their fair share of legal transaction throughput. However, when the regulator licenses between 0% and 33% of the consensus resource, the regulated consensus executors can do no better than building on the longest branch of dubious blocks (Section 4.5), resulting in legal transaction throughput proportional to their consensus resource.

   Further, we show that our results can be applied to the Bitcoin blockchain in practice (Sections 3.4 and 4.6).

Blockchain-based crypto-economies are defined using a four-layer system stack [36]. The difference between a traditional instantiation of the blockchain stack and an instantiation corresponding to our regulated blockchain system is depicted in Figure 1.

2 CASE STUDY: THE SILK ROAD DARK WEB MARKET

We first give a brief study on the operation of the Silk Road Darknet Market, which flourished through the illegal use of the Bitcoin cryptocurrency.

2.1 An Overview of the Silk Road Marketplace

Anonymity is the most prominent institution of the Deep Web. Each user (buyer and seller) is identified by a username, with a secret true identity. Deep Web users record market interactions through forums and blogs. Consequent to the anonymity it provides, black market activity over the Deep Web is highly feasible and attractive. Web traffic is anonymized through TOR, and Bitcoin serves as an untraceable virtual currency. Email interactions to discuss illicit transaction details are encrypted through PGP. These three network, email, and currency elements serve as the technological foundation to build an illegal market, with low cost illegal transactions. Given that previously illegal transactors relied heavily on in-person deals and reputations built on personal encounters, Deep Web-based illicit markets resulted in a paradigm shift for illegal activities on a global scale [15].

The Silk Road online (mostly) narcotics trade marketplace has flourished anonymously on the Deep Web since 2011. A study aimed at the discovering the realities and motives of operations (navigation and purchase) by drug users on the Silk Road marketplace has been conducted [34]. The study was conducted through strategic online observations, four-month-long fieldwork on marketplace site discussion threads and 20 anonymous online interviews of a sample of adult users.

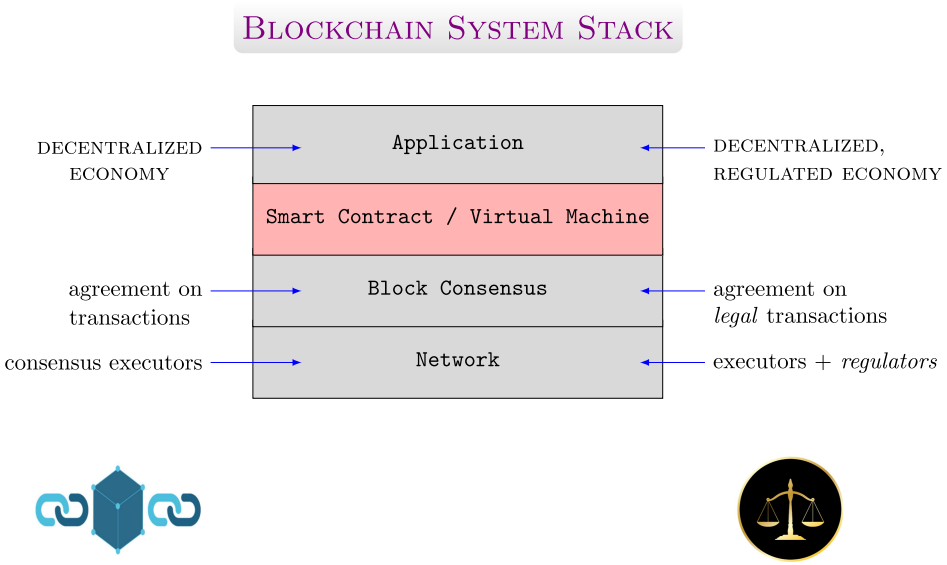

Fig. 1. Traditional vs. regulated blockchain systems.

2.2 Illicit Transactions Employing Bitcoin

The Silk Road marketplace is inferior to traditional online sites (such as eBay), due to its bad Bitcoin *escrow implementation*: the ability to undo a transaction. Standard escrow requires that if the trade is deemed fraudulent, the traded assets are returned to the seller, and the escrow service refunds the currency to the buyer. In case of fraud, market users only lose their service fee. Typical of illegal marketplaces, Silk Road purchases cannot be undone: drug sellers do not provide return addresses, and a perfect escrow service cannot exist (although a rudimentary escrow can) that satisfies both the buyer and the seller, simultaneously [15].

A prominent drug study [34] concluded that many narcotics buyers were not technically proficient and faced trouble in arranging for Bitcoin credit and accessing the Silk Road website via the Tor browser. An anonymous interview of an adult drug user revealed his drug procurement process over Silk Road. The said user was able to procure Bitcoins with minimal paperwork from a particular bank, with no self identifying information submitted to the bank. By the end of the day, the user had Bitcoins credited to his Silk Road account. (S)He then went to the narcotics' vendor webpage, added the drugs to his shopping cart and entered an encrypted postal address for the drug delivery, thereby confirming the order. The user even employed an escrow system to avoid being scammed by the vendor. Consequently, the Bitcoins are not delivered to the vendor until the drug package reached the user and the order was finalized.

Thousands of Bitcoin worth approximately a billion U.S. dollars connected with Silk Road-based drugs and goods trade have been confiscated by the United States Justice Department, the biggest seizure in history of the agency [5]. This motivates the need for preemptive monetary investment by the regulator to ensure only legal transactions are confirmed on-chain (as is suggested in Section 4.4) to minimize the cost associated with law enforcement and the recovery of illegal cryptocurrency, and reduce illegal activity through the blockchain.

Very recently, senior authorities from the U.S. Treasury Department and the European Central Bank have also formally recognised the use of Bitcoin and other cryptocurrencies for illegal activities, and are strongly considering regulation in these digital economies [27, 28].

The drug study, seizures, and recent concerns raised by authoritative figures in prominent financial bodies advocate that, at least the Bitcoin protocol is rife with issues of confirmed illegal transactions, and appropriate regulatory mechanisms are need to be enforced to define legal, decentralized crypto-economies.

3 THE REGULATED BLOCKCHAIN SYSTEM

3.1 Motivation for Regulating Blockchain Consensus

Blockchain systems are defined with a four-layer system stack (from bottom to top): the network layer, the consensus layer, the smart contract layer, and the application layer [36]. There are two problems associated with regulatory policy enforcement at the smart contract layer: (i) Most times when a blockchain user is involved in illegal trade, its digital identity is difficult to map to a specific federal jurisdiction. This makes it hard to enforce regulation rules (as a distributed program) at the smart contract layer. (ii) A smart contract layer regulatory enforcement will take *time to achieve consensus + time to execute the smart contract (which may be computationally intensive [7])*. This would be slower in contrast to consensus layer only solutions. Thus, to ensure legal transaction proposal and confirmation, it is prudent to license the blockchain consensus protocol executors who take it upon themselves to add provably legal transactions to their blocks, and run the consensus protocol on these blocks.

We now detail our regulated blockchain system model for the consensus layer.

3.2 Stakeholders, Terminology, Assumptions, and Notation

We define the stakeholders in our regulated decentralized economy, and give the associated terminology and assumptions, first.

- *Transaction and Block Types:* We will assume there are two types of transactions: *legal* or *dubious*. Transactions whose legal status can be established for certain will be called legal. All other transactions would be called dubious. A block that contains at least one dubious transaction will be called a *dubious block*. A block that contains only legal transactions will be called a *legal block*. A legal block generated by a regulated consensus protocol executor (defined later) will be called a *regulated block*.
- *A Body of Regulators:* We will assume the existence of a cross-jurisdictional network of regulators, which are federal associations in-charge of ensuring legal practices in the blockchain network (similar to principles in Reference [32]).
- *Blockchain Transactors:* We will refer to blockchain users that define and propose cryptocurrency transactions as *transactors*. The transactors can be of two types: regulated and unregulated. Regulated transactors will always propose transactions that are legal and verifiable within the blockchain network. Unregulated transactors can propose either of legal or dubious transactions.
- *Blockchain Executors:* We will refer to blockchain users that execute the consensus protocol as *consensus executors*, or *executors* for short. These executors will be miners in **proof-of-work (PoW)** blockchains, or validators in **proof-of-stake (PoS)** blockchains. We will assume that all executors are perfectly rational, and want to maximize their reward / revenue resulting from their participation in the consensus protocol (a standard notion of rationality [20, 22]). We will also refer to the consensus resource associated with each executor, where the resource is hash power in PoW blockchains, or stake in PoS blockchains. Here too, we will assume executors will be of two types: regulated and unregulated. Regulated executors will propose blocks that contain only verifiably legal transactions, with an evidence of regulation of the said executor, and so their blocks will be called regulated blocks. Unregulated executors can propose blocks that may be either legal (containing legal transactions only) or dubious (containing at least one dubious transaction).
- *Block Notarization and Confirmation:* We say that a proposed block is *notarized* (similar terminology in Reference [3]), once it is successfully mined by a PoW executor, or successfully validated by a PoS executor. We say that a block is *confirmed* once it is sufficiently deep in the blockchain and all the transactions contained in it are finalized (for instance, transactions in Bitcoin are finalized once they are six blocks deep [26]).
- *Block Proposal in Discrete Time:* We assume that the consensus protocol executors have loosely synchronized clocks by employing protocols such as NTP [14]. We will ignore network delays, and assume

that blocks are proposed in discrete sequential epochs of time, with the time difference between two consecutive epochs equal to the block proposal time of the base protocol (for instance, 10min in Bitcoin [26] and 15s in Ethereum [10]).

- *Dubious and Legal Block Branches:* Given the block proposal competition ensuing between two categories (regulated and unregulated) of consensus executors, there would exist a fork in the blockchain with block branches corresponding to each category of executors. We would refer to the block where this fork originates as the root block (this would be the block at the end of the trunk of the unambiguous part of the blockchain). The block branch corresponding to regulated executors will be referred to as the *legal branch* (as all blocks in this branch will be legal), and that corresponding to unregulated executors will be referred to as a *dubious branch*. Given any one of the legal or dubious branches, we would refer to the most recently notarized block in a branch as a *frontier* block for that branch, and every other notarized block as an *interior* block for that branch.

We present the notation that will be used throughout the article. There exists a set of consensus protocol executors N, where the normalized consensus resource of each executor $i \in N$ will be denoted by α_i. Given any blockchain user i (may it be a transactor or executor), its private signing key will be denoted by sk_i and its public verification key will be denoted by vk_i. We will assume the existence of a signature scheme $\Pi^{\mathtt{sig}} := (\mathtt{sign}, \mathtt{ver})$, where, for any message m, given $\mathtt{Sig}_i(m) := (m, \mathtt{sign}_{sk_i}(m))$, it is true that $\forall i, \mathtt{ver}_{vk_i}(\mathtt{Sig}_i(m)) = 1$ and $= 0$ otherwise (verification succeeds for a correctly signed message only). We will also assume the existence of a random oracle H^*, realizable through an ideal collision resistant hash function. We will denote the set of (possibly networked and cross-jurisdictional) regulators by $\mathcal{F}$. Some executors in N will be under the jurisdiction of regulators in $\mathcal{F}$, and we will denote them by R $(\subseteq N)$. We will denote the set of unregulated executors with $\bar{R} := N \setminus R$. Membership in R requires permission from $\mathcal{F}$, whereas $\bar{R}$ is permissionless. We will denote the block proposal rounds/epochs by e. Finally, we will denote the regulatory oversight window, the number of sequential block proposal rounds for which the regulatory licenses are valid, by E. Our notation is summarized in Figure 2.

3.3 Regulated Blockchain Protocol Goals

Given an existing blockchain consensus protocol BChain, we re-engineer the same to define a regulated blockchain protocol RBChain. Under RBChain, the regulatory body $\mathcal{F}$ only licenses the consensus protocol transactors and executors to ensure that these blockchain users undertake the responsibility of distributed consensus on legal transactions. Also, the RBChain protocol (defined in Section 3.4 for Bitcoin) must have the following features:

- *Transactions under RBChain should be distinguishable from those under BChain.* This feature would allow the blockchain network to distinguish between legal and dubious transactions by regulated and unregulated transactors, respectively.
- *Block composition under RBChain should be different from that under BChain.* This feature would allow the blockchain network to distinguish between regulated blocks and unregulated (which could be either of legal or dubious) blocks proposed by regulated and unregulated executors, respectively.
- *RBChain and BChain should have equivalent block proposal times and transaction confirmation times.* This would guarantee, for fairness and backward compatibility, that the regulated executors do not have an unfair advantage over unregulated executors in their transaction confirmation, as part of the execution of their protocol.[1]

[1]Note that the design philosophy behind RBChain is to define block proposal strategies that will maximize the expected number of legal blocks going on-chain for each consensus epoch, and not achieving that goal by altering the block proposal time (say, by changing the crypto-puzzle difficulty in proof-of-work consensus).

Symbol	Description
N	Network of Blockchain Executors
vk_i	Public verification key of blockchain user i
sk_i	Private signing key of blockchain user i
α_i	Consensus resource of blockchain executor i
$\Pi^{\mathtt{sig}} := (\mathtt{sign}, \mathtt{ver})$	A Signature scheme
$\mathtt{Sig}_i(m)$	Signed message m by blockchain user i
H^*	A Random Oracle / ideal CRHF
$\mathcal{F}$	Set of Networked Regulators
$R\ (\subseteq N)$	Permissioned Set of Regulated Executors
$\overline{R} := N \setminus R$	Permissionless Set of Unregulated Executors
e	Block Proposal Round Number
E	Size of the Regulatory Oversight Window

Fig. 2. Notation for our regulatory framework.

3.4 Regulated Blockchain Consensus for Bitcoin: Compliance Registration, Rules, Transaction, and Block Structures

We now give an exact construction of the regulated version of the Nakamoto consensus protocol to be followed by the regulated Bitcoin miners R. Before that, we specify how for each miner in R, compliance registration is achieved, how legal rules are announced, and how subsequently legal transactions and blocks are constructed.

The unregulated miners $\overline{R}$ follow the standard protocol.

3.4.1 Regulatory KYC and Legal Rules Announcement. Prior to be eligible for participation in the regulated Bitcoin protocol, regulated blockchain executors (denoted by i individually) apply for a participation license from the regulatory body $\mathcal{F}$. In their application, the regulated executors furnish details (given next) to disclose their physical identity, and protocol specific parameters, which is collated by the regulator in a **Know-Your-Customer (KYC)** document $KYC_{i,\mathcal{F}}$.[2]

$KYC_{i,\mathcal{F}}$ details submitted to $\mathcal{F}$ by Miner i: Personal: Name, Cell Number, Passport (Social Security) Protocol Related: Bitcoin Wallet, Mining hashrate h

The regulator next prepares the legal rules applicable to the cryptocurrency-based purchases of asset classes (in a set of asset classes $\mathcal{A}$) in the regulatory jurisdiction $\mathcal{F}$. More specifically, $\Gamma_{\mathcal{F},a}$ is a document prepared by $\mathcal{F}$, which lists the legal rules pertaining to cryptocurrency-based purchase of asset a in jurisdiction $\mathcal{F}$. Next, given that the regulator conducts the KYC of executors R, the regulator licenses each authorized executor $i \in R$ for executing the regulated version of the Bitcoin protocol, by generating signed permissions, denoted by $\beta_i^{\mathcal{F}}$, that i is to include only transactions consistent with $\Gamma_{\mathcal{F},a}$ ($\forall a \in \mathcal{A}$) in the blocks that it proposes. Finally, the regulator broadcasts the legal rules, mining licenses, and normalized regulated mining hashrate α_R (by querying the Bitcoin network for its total hashrate h_N), over the network.

[2]Kindly note that a similar KYC document may optionally be collated by the regulator for each transactor in the collective jurisdiction of $\mathcal{F}$, given that the said transactor is willing to furnish its details.

Regulatory Information announcement by $\mathcal{F}$:
GENERATE:
$\forall a \in \mathcal{A}$: $\rho_a^{\mathcal{F}} := \mathtt{Sig}_{\mathcal{F}}(\Gamma_{\mathcal{F},a})$
$\forall i \in R$: $\beta_i^{\mathcal{F}} := \mathtt{Sig}_{\mathcal{F}}(H^*(KYC_{i,\mathcal{F}}))$
$\alpha_R := (\sum_{i \in R} h_i)/h_N$
ANNOUNCE:
$(vk_{\mathcal{F}}, \{\rho_a^{\mathcal{F}}\}_{a \in \mathcal{A}}, \{\beta_i^{\mathcal{F}}\}_{i \in R}, \mathtt{Sig}_{\mathcal{F}}(\alpha_R))$ over the network.

3.4.2 Construction of Legal Transactions and Regulated PoW Blocks. We assume that every standard Bitcoin transaction tx_j (given any transactor j), is *dubious*: its legal status cannot be established as is. Most transactions involve a *quid-pro-quo*: the transaction is made in exchange for an asset. If tx_j is made in exchange for an asset in some class $a \in \mathcal{A}$, then j prepares a signed receipt (using sk_j) for the asset received, toward preparing a verifiably legal transaction by modifying tx_j. This signed receipt is given by σ_a^j, and is included in tx_j along with the legal rules $\rho_a^{\mathcal{F}}$ for checking the legal correctness on the validity and valuation toward the trade of a in jurisdiction $\mathcal{F}$, thereby generating ltx_j. Given an arbitrary coinbase transaction ctx_i by miner(/executor) i, in the instance that i is regulated, ctx_i is also modified using the license $\beta_i^{\mathcal{F}}$ to generate the regulated coinbase transaction rctx_i and establish the regulated status of i during protocol execution. The legal transaction and block structures are given next.

Transaction Structure (for transactor j, miner i):
ltx_j: tx_j with $(\sigma_a^j, \rho_a^{\mathcal{F}})$ in the *Txout-Script* [37] field.
rctx_i: ctx_i with $\mathtt{Sig}_i(\beta_i^{\mathcal{F}})$ in the coinbase *Txout-Script* field.
Block Structure:
Regulated Block $\mathcal{RB}$: contains one rctx with ltxs only.
Legal Block $\mathcal{LB}$: contains one ctx with ltxs only.
Dubious Block $\mathcal{DB}$: contains one ctx with at least one tx.

Note that all the signed messages as part of the announcement of the legal rules, the legal transactions, and the regulated coinbase transactions are deterministically verifiable under the signature scheme $\Pi^{\mathtt{sig}}$ (by appropriately using the public verification key(s) and the verification algorithm).

Status of dubious-but-legal transactions. We now consider legal transactions proposed by a transactor, which are constructed and announced as standard dubious transactions. In regulated jurisdictions, that is where the said transactor is governed by some regulator in $\mathcal{F}$, according to our model, to incentivize regulatory compliance, there is no acceptance of such dubious-but-legal transactions, and these transactions are treated as dubious transactions only. In unregulated jurisdictions, that is where the said transactor is not governed by any regulator in $\mathcal{F}$, the design of such dubious-but-legal transactions can be considered in future as open-for-audit pseudo-legal transactions. The corresponding dubious transaction ltx_j by transactor j for an asset in class a can contain $(\sigma_a^j, \mathtt{Sig}_j(\text{OPEN-FOR-AUDIT}))$ in the *Txout-Script* field, implying that these transactions are claimed to be legal with an openness to an audit and the corresponding blocks containing these transactions only can be considered open-for-audit pseudo-legal blocks. A formal audit characterization and block proposal competition under this framework for dubious-but-legal transactions is left as future work.

3.4.3 The RBitcoin Protocol. The Bitcoin [26] consensus protocol requires the executors (called miners) to solve a compute intensive crypto-puzzle, to notarize a block. Our proposed regulated Bitcoin protocol is called RBitcoin, where the regulated miner adds legal transactions and evidence of its license in the coinbase transaction script before trying to solve the crypto-puzzle associated with the regulated block $\mathcal{RB}$ that it wishes to go on-chain.

ALGORITHM 1: Regulated Nxt Proof-of-Stake Protocol

Given:
The Nxt Consensus Protocol [23].
procedure NxtPoS-RIsEligible
Given a legal block $\mathcal{LB}$, regulated validator $i \in R$ receives a regulated block $\mathcal{RB}$ (formed by adding $\beta_i^{\mathcal{F}}$ to $\mathcal{LB}$). i then finds nonce η such that $H^*(vk_i \circ \beta_i^{\mathcal{F}} \circ \eta)$ lies in the target window, which is a function of time and α_i, to become eligible to validate $\mathcal{RB}$.
end procedure

We now show that RBitcoin and Bitcoin have equivalent block proposal times. First, it is known that the image distribution of the random oracle (ideal CRHF) H^* is uniform, for any pre-image distribution. So, given a regulated block $\mathcal{RB}$ mined on for an appropriate nonce η in the RBitcoin protocol, for any block $\mathcal{B} \in \{\mathcal{DB}, \mathcal{LB}\}$ mined on for an appropriate nonce η' in the standard Bitcoin protocol, it is true that $H^*(\eta' \circ \mathcal{B})$ and $H^*(\eta \circ \mathcal{RB})$ are statistically indistinguishable distributions. Next, since the crypto-puzzle target window in unaltered in RBitcoin, the block proposal times of RBitcoin and Bitcoin are statistically equivalent[3] (with 10 min in expectation).

3.5 Regulating Nxt Proof-of-Stake

Nxt [23] is a proof-of-stake consensus protocol that uses a deterministic eligibility algorithm IsEligible to elect a validator for notarizing a block. We propose the regulated version of the eligibility algorithm, to validate a regulated block, called RIsEligible, using the regulatory license in the hash pre-image for the eligibility proof generation. RIsEligible is given in Algorithm 1. The proof of equivalent block proposal times between RIsEligible and IsEligible is identical to that of the argument for RBitcoin (Section 3.4.3).

Competition in a Regulated Setting. The regulator $\mathcal{F}$ can determine the total consensus resource (mining hashrate) regulated in the blockchain network, through its KYC of the executors (miners). Given the permissionless nature of cryptocurrency blockchain networks, including Bitcoin, the consensus resource in these networks can never be wholly regulated. This would entail a strategic competition between legal and dubious block proposal by regulated and unregulated executors, respectively, which is discussed next.

4 BLOCK PROPOSAL COMPETITION ACROSS EXECUTORS

Given our regulatory framework, the next blockchain state is a random variable, as a function of the present blockchain state and the block notarization strategies of two categories of entities: the regulated executors and the unregulated executors. A non-cooperative stochastic game [31] is conducive for the analysis of such a two entity competitive system. Since there exists a clear reduction between our competitive framework of two entities distinguished on the basis of regulatory compliance, to any non-cooperative two-player, preferably economic, analytical block proposal competition model (as is seen for instance in References [20, 22]), we so analyze the competition between the regulated and unregulated executors as a two-player stochastic game, inspired from References [20, 22].

We define the regulated blockchain stochastic game, and state best responses by the regulated executors R and unregulated executors $\bar{R}$ in the form of their Nash Equilibria [20, 31] strategies, as a function of the total consensus resource regulated by $\mathcal{F}$. We briefly discuss the practical properties of these equilibria in Section 4.6.

We start with the formalization and details of the competition between the regulated and unregulated executors, and then give the consequential provable consensus strategies by regulated executors toward their goal of maximizing the legal transaction throughput.

[3]Note that the mining hashrate of RBitcoin miners is the same as that when they were operating unregulated. So regulation does not give miners an added advantage (or disadvantage) to propose blocks faster (or slower).

4.1 The Regulated Blockchain Game Features

Preliminaries. Our blockchain stochastic game defines competition between two-player categories: the regulated executors R and the unregulated executors $\bar{R}$. We assume that the total consensus resource in the blockchain network is normalized: $\sum_{i \in N} \alpha_i = 1$; and the expected revenue/reward per epoch of the blockchain for any category of players $\mathbf{p} \in \{R, \bar{R}\}$ is denoted by $g_{\mathbf{p}}$, and is a function of $\alpha_{\mathbf{p}} = \sum_{i \in \mathbf{p}} \alpha_i$. Unless the regulator $\mathcal{F}$ adds extra transactions to the blockchain (Section 4.4), $g_R + g_{\bar{R}} = 1$. Our game evolves as a block tree of width two, with one branch consisting of regulated blocks notarized by R, and the other branch consisting of legal or dubious blocks notarized by $\bar{R}$, and the forking point of the block tree has a root block, say B^{e_0}. If either of R or $\bar{R}$ abandons its branch for the competing branch, then the root block B^{e_0} moves accordingly, and the game starts afresh. We also allow the regulator $\mathcal{F}$ to add an additional reward $\rho_{\mathcal{F}}$ in the regulated blocks, when R is in a small majority in the blockchain network ($0.5 < \alpha_R < 0.58$), resulting in $g_R + g_{\bar{R}} \geq 1$. Our game has depth E, equal to the oversight window and the window for collecting the notarization reward (coinbase reward in Bitcoin [22]). The game depth E means that the first branch originating from B^{e_0} that achieves height E is confirmed as part of the blockchain, and the game starts afresh. Finally, we assume that the executors collect their block notarization reward at the end of the game depth (for example, for $E = 100$ in Bitcoin [20]). For a simplified game analysis, we assume $E = \infty$, unless stated otherwise.

We will denote the normalized legal transaction throughput, which can also be interpreted as the expected number of legal blocks agreed at each epoch of the blockchain, by $t_{\mathcal{F}}$. Given that regulated executors only propose legal transactions, and unregulated executors may propose either of legal or dubious transactions, it is easy to see that $t_{\mathcal{F}} \geq g_R$.

Stochastic Game Summary: Our results on normalized legal transaction throughput $t_{\mathcal{F}}$ and normalized expected block rewards for regulated executors g_R and unregulated executors $g_{\bar{R}}$ are summarized in Figure 3. These results are formally detailed in Sections 4.3, 4.4, and 4.5.

We now define *how* executors choose to release their notarized blocks, and which blocks they may select to append future blocks on.

Block Release Models. We first define the block release models (from References [20, 22]), which elucidate *when* consensus executors choose to reveal information about their notarized blocks.

The first block release model stated below can be adopted by both R and $\bar{R}$.

Definition 1 (Immediate Release Model). A consensus executor follows the ***immediate block release (IR)*** *model* when, any block notarized by it is immediately released and added to the blockchain for use by other executors.

Due to prevalent distrust among $\bar{R}$ in the fair distribution of notarization rewards [19] (explained in Section 4.5), the second block release model stated below can be adopted by R alone.

Definition 2 (Strategic Release Model). A consensus executor follows the ***strategic block release (SR)*** *model* when, on successful notarization of block(s) by it, the block notarization pool leader executor *announces* its existence, but the block(s) can only be used by other executors outside the pool when the leader decides to *release* them.

Consensus Execution Strategies. The honest strategy where a consensus executor notarizes blocks at the end of the longest branch of the blockchain, is traditionally referred to as the `Frontier` strategy [20, 22]. Under the `Frontier` strategy, the expected gain per epoch of the associated executor is equal to the consensus resource possessed by it. We now give definitions of equivalent (to `Frontier`) consensus execution strategies in our regulated setting.

Definition 3 (`DubFrontier`). An unregulated consensus executor follows the `DubFrontier` strategy, when it notarizes legal ($\mathcal{LB}$) or dubious ($\mathcal{DB}$) blocks chained at the frontier block of the longest dubious branch of the blockchain.

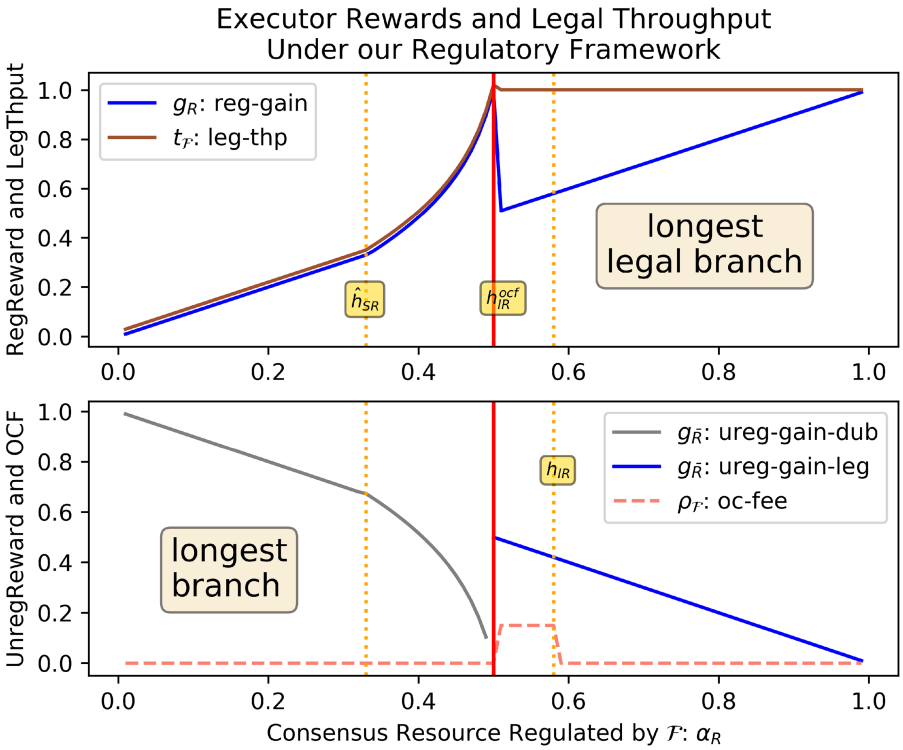

Fig. 3. When $\alpha_R \leq 0.5$, the legal transaction throughput $t_{\mathcal{F}}$ is sub-optimal under the longest branch rule. However, when $\alpha_R > 0.5$, the longest legal branch wins, $\bar{R}$ can do no better than proposing legal blocks, and $t_{\mathcal{F}}$ is maximized. Blue curve denotes reward for legal blocks, and gray curve denotes reward for dubious blocks.

Definition 4 (`LegFrontier`*).* An unregulated consensus executor follows the `LegFrontier` strategy, when it notarizes legal ($\mathcal{LB}$) blocks chained at the frontier block of the longest legal branch of the blockchain.

Definition 5 (`RegFrontier`*).* A regulated consensus executor follows the `RegFrontier` strategy, when it notarizes regulated ($\mathcal{RB}$) blocks chained at the frontier block of the longest legal branch of the blockchain.

Definition 6 (`RegFrontier`$(\rho_{\mathcal{F}})$*).* A regulated consensus executor follows the `RegFrontier`$(\rho_{\mathcal{F}})$ strategy, when it notarizes regulated ($\mathcal{RB}$) blocks chained at the frontier block of the longest legal branch of the blockchain, with a pay-forward [22] of $\rho_{\mathcal{F}}$ (which is a function of α_R) by the regulatory body $\mathcal{F}$ in the regulated blocks, as an **oversight compliance fee (OCF)**.

Definition 7 (`RDubFrontier`*).* A regulated consensus executor follows the `RDubFrontier` strategy, when it notarizes regulated ($\mathcal{RB}$) blocks chained at the frontier block of the longest dubious branch of the blockchain.

The longest legal branch rule: The block notarization strategies `LegFrontier`, `RegFrontier` and `RegFrontier`$(\rho_{\mathcal{F}})$ constitute notarization on the longest legal branch: at every epoch, all executors following these strategies add legal blocks to the longest existing branch of legal blocks.

Our competition analysis: We first define the regulated blockchain stochastic games in Section 4.2. In the following analysis of the first two games (in Sections 4.3 and 4.4), deal with deriving the conditions under which attacks by the unregulated executors on the legal branch fail, given that the regulator licensed the majority of the consensus resource. The third game analysis (in Section 4.5) deals with deriving conditions under which attacks

by the regulated executors on the dubious branch succeed, given that the unregulated consensus resource is in a majority.

4.2 Regulated Blockchain Stochastic Games

The block proposal stochastic games between the regulated and unregulated executors are defined next.

Blockchain Game with Regulated Executor Dominance. Our first regulated blockchain stochastic game RBChain-Rdom-Game is applicable when the regulated executors are in a majority in the blockchain network ($\alpha_R > 0.5$). Given a root block, the blockchain state is given by $(b_{\bar{R}}, b_R)$, where $b_{\bar{R}}$ blocks are proposed by $\bar{R}$, and b_R blocks are proposed by R. The regulator may include an OCF in all of b_R blocks.

RBChain-Rdom-Game States:

- *Mining States.* This set of states, denoted by M, is a collection of states $(b_{\bar{R}}, b_R)$ where both R and $\bar{R}$ notarize blocks on their own branch. Note that $(0, 0) \in M$.
- *Defection/Capitulation States.* This set of states, denoted by C, is when executor $\bar{R}$ defects and abandons its own branch, and adds (legal or dubious) blocks linked to some regulated block in the competing regulated branch, transitioning the game from state $(b_{\bar{R}}, b_R)$ to state $(0, s_R)$ where $s_R \in \{0, 1, \ldots, b_R - 1\}$.
- *Legal Winning States.* This set of states is given by $W_{leg} := \{(b_{\bar{R}}, b_R) : b_{\bar{R}} = b_R + 1\}$ and all $b_{\bar{R}}$ blocks in each state of W_{leg} are legal. Under W_{leg}, when executor $\bar{R}$ overtakes, the game transitions to state $(0, 0)$.

Blockchain Game with Unregulated Executor Dominance. Our second regulated blockchain stochastic game RBChain-URdom-Game is applicable when the unregulated executors are in a majority in the blockchain network ($\alpha_{\bar{R}} > 0.5$). Given a root block, the blockchain state is given by $(b_R, b_{\bar{R}})$, where $b_{\bar{R}}$ blocks are proposed by $\bar{R}$, and b_R blocks are proposed by R. The regulated executors release $min(b_R, b_{\bar{R}})$ blocks.

RBChain-URdom-Game States:

- *Mining States.* This set of states, denoted by M, is a collection of states $(b_R, b_{\bar{R}})$ where both $\bar{R}$ and R notarize blocks on their own branch. Note that $(0, 0) \in M$.
- *Dubious Cut Defection/Capitulation States.* This set of states, denoted by C_{dub}, is when executor R defects and abandons its own branch, and adds regulated blocks linked to some regulated block in the competing dubious branch, transitioning the game from state $(b_R, b_{\bar{R}})$ to state $(0, s_{\bar{R}})$ where $s_{\bar{R}} \in \{0, 1, \ldots, b_{\bar{R}} - 1\}$, and all $s_{\bar{R}}$ blocks are dubious.
- *Winning States.* This set of states is given by $W := \{(b_R, b_{\bar{R}}) : b_R = b_{\bar{R}} + 1\}$. Under W, when executor R overtakes, the game transitions to state $(0, 0)$.

Original Blockchain Stochastic Games. We will refer to the original blockchain mining game under the immediate release model, proposed by Kiayias et al. (Sections 2 and 3 in Reference [20]) as the K1-IR-Game. We will refer to the blockchain mining game with a pay-forward scheme, under the immediate release model, proposed by Koutsoupias et al. (Sections 2 and 3 in Reference [22]) as the K2-IR-Game. Also, we will refer to the original blockchain mining game under the strategic release model (Section 4 in Reference [20]) as the K1-SR-Game. Both blockchain mining games [20, 22] do not consider a distinction between legal and dubious blocks, which is formally introduced in our regulated stochastic games.

4.3 A Stochastic Game with Immediate Block Release

Our first two-player game consists of competition between the regulated executors R and the unregulated executors $\bar{R}$, when both players notarize and release their blocks immediately, the regulator $\mathcal{F}$ licenses more than

$1 - h_{IR} = 58\%$ of the consensus resource in the blockchain network, and the regulated executors add regulated blocks to the existing longest legal branch. The best responses (in terms of expected gain maximization) for both players are formalized in the following theorem (depicted in Figure 5(a)).

Theorem 1 (Equilibrium under IR). *In the IR model, given regulated executors R follow the "longest legal branch" rule, and $\alpha_{\overline{R}} < h_{IR} = 0.42$, then R playing* `RegFrontier` *and $\overline{R}$ playing* `LegFrontier` *is a Nash Equilibrium.*

Proof. The K1-IR-Game considers two miners, named 1 and 2, where miner 2 is in a majority in the Bitcoin network ($\alpha_2 > 0.5$), and is always following the `Frontier` strategy. Theorem 3.2 [20] from K1-IR-Game proves that when miner 1 has hash power α_1 less than the root of the polynomial $2\alpha^2 - (1-\alpha)^3 \approx 0.361$, then `Frontier` is a Nash equilibrium strategy for miner 1. Theorem 3.2 is proven by eliminating the possible set of mining states under the given condition. Next, through Theorem 3.12 [20] in the K1-IR-Game, it has been proven that, for game depth E = 3, the expected gain g_1 per epoch of miner 1 is equal to $\frac{\alpha_1^2(2+2\alpha_1-5\alpha_1^2+2\alpha_1^3)}{1-\alpha_1^2+2\alpha_1^3-\alpha_1^4} > \alpha_1$, by demonstrating strategies more rewarding than the `Frontier` strategy for $\alpha_1 > 0.455$. By considering alternate game depths E, the K1-IR-Game experimentally establishes (Table 1 in Reference [20]) the lower bound for a deviating strategy to be $\alpha_1 > h_{IR} \approx 0.42$. The RBChain-Rdom-Game reduces to an instance of the K1-IR-Game, when the first miner is the unregulated executor $\overline{R}$, the second miner is the regulated executor R, the first miner's `Frontier` strategy is replaced by the `LegFrontier` strategy, and the second miner's `Frontier` strategy is replaced by the `RegFrontier` strategy. Consequently, the results on the threshold h_{IR} from the K1-IR-Game directly apply to the RBChain-Rdom-Game. □

Theorem Implication: This theorem implies that, if the regulatory body $\mathcal{F}$ is successful in licensing more than 58% of the total consensus resource, then no executor can do better than adding legal blocks at the frontier block of the legal notarized but unconfirmed branch in the blockchain, resulting in a fair block reward for each executor type: $g_R = \alpha_R, g_{\overline{R}} = \alpha_{\overline{R}}$, and a 100% legal transaction throughput in the blockchain network: $t_{\mathcal{F}} = 1$.

The consensus resource upper-bound h_{IR} on unregulated executors, is a function of the oversight window E, with experimental values given in Figure 4, and an approximate value of 0.42 (derived from the computation of the parameters of the underlying stochastic game in Reference [20]).

4.4 A Stochastic Game with Immediate Block Release and a Compliance Fee

Our second two-player game consists of competition between the regulated executors R and the unregulated executors $\overline{R}$, when both players notarize and release their blocks immediately, the regulator $\mathcal{F}$ licenses more than $h_{IR}^{ocf} = 0.50$ of the consensus resource in the blockchain network. In this game, the regulator additionally remits an OCF $\rho_{\mathcal{F}}$ as an extra transaction in each regulated block (to incentivize legal block proposal over dubious block proposal), which is claimed by the executor corresponding to the confirmed block following the said regulated block: given that some block B^e is regulated and contains the OCF, then notarizer of block B^{e+1} claims the said OCF. This OCF is a function of α_R. Here again, the best responses for both players, given that the regulated executors add regulated blocks to the existing longest legal branch, are formalized in the following theorem (depicted in Figure 5(b)).

Theorem 2 (Equilibrium under IR with an OCF). *In the IR model, given regulated executors R follow the "longest legal branch" rule, and $\alpha_R > h_{IR}^{ocf} = 0.50$, then R playing* `RegFrontier(`$\rho_{\mathcal{F}}$`)` *and $\overline{R}$ playing* `LegFrontier` *is a Nash Equilibrium.*

Proof. The K2-IR-Game has an identical setting to the K1-IR-Game in terms of defining the miners, and their best response strategies. However, K2-IR-Game allows miner 1 to add a pay-forward reward w (as some unknown function of α_1) to the blocks mined by it. This reward w is collected by the miner who confirms a block immediately succeeding the block that contains the announcement of w. In this setting, it is proven through

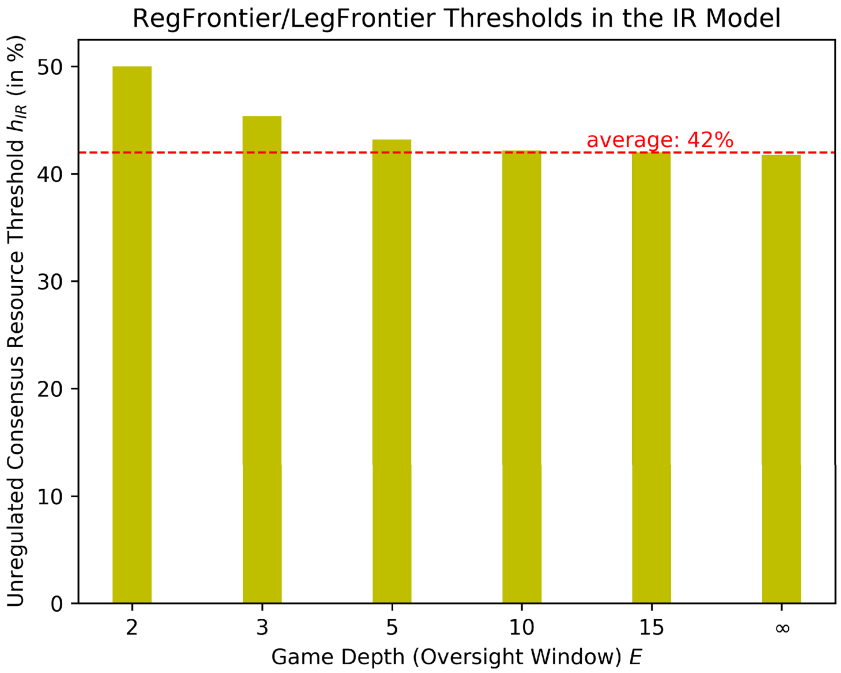

Fig. 4. Upperbound on the Unregulated Consensus Resource for the RegFrontier/LegFrontier strategies, as a function of the Game Depth (base results from Reference [20]).

Theorem 3.2 [22], that `Frontier` is a Nash equilibrium strategy for miner 1, when miner 2 has consensus resource $\alpha_2 > h_{IR}^{ocf} = 0.5$. The RBChain-Rdom-Game with a regulator contributed OCF $\rho_{\mathcal{F}}$ in the regulated blocks, reduces to an instance of the K2-IR-Game, when the first miner is the unregulated executor $\bar{R}$, the second miner is the regulated executor R, the first miner's `Frontier` strategy is replaced by the `LegFrontier` strategy, and the second miner's `Frontier` strategy is replaced by the `RegFrontier`($\rho_{\mathcal{F}}$) strategy. Consequently, the results on the threshold h_{IR}^{ocf} from the K2-IR-Game directly apply to the modified RBChain-Rdom-Game. □

Theorem Implication (in conjunction with Theorem 1): If the regulatory body $\mathcal{F}$ is successful in licensing between 50% and 58% of the total consensus resource, *and* mandates legal blocks to an oversight compliance transaction fee $\rho_{\mathcal{F}}$ (which is paid by $\mathcal{F}$ and is a function of α_R), then again, no executor can do better than adding legal blocks at the frontier block of the legal branch in the blockchain, resulting in a fair block reward for each executor type: $g_R \geq \alpha_R, g_{\bar{R}} \geq \alpha_{\bar{R}}$ (inequality due to $\rho_{\mathcal{F}}$), and a 100% legal transaction throughput in the blockchain network: $t_{\mathcal{F}} = 1$. Note that when the regulated consensus resource in the blockchain network is between 50% and 58%, if the regulator $\mathcal{F}$ does not include the OCF in the regulated blocks, it would still be true that $t_{\mathcal{F}} = 1$, but the unregulated executors $\bar{R}$ can attack and successfully add legal blocks linked to an interior block in their competing branch, resulting in $g_R < \alpha_R$. Thus, it is imperative that the regulator adds the OCF in the regulated blocks, to save the expected gain g_R ($\geq \alpha_R$) of the regulated executors R.

Justification for a pay-forward in regulated blocks alone: Assuming that world governments, and consequently the regulatory bodies, are richer than the executors and want to preserve the revenue generated by their regulated executors (to motivate licensing within the blockchain network). If the unregulated miners even decide to pitch some money per block for the unregulated branch, say $w_{\bar{R}}$, then the regulators can counterbalance the legal branch by pitching $w_R = w_{\bar{R}} + \rho_{\mathcal{F}}$, where $\rho_{\mathcal{F}}$ is defined as a function of α_R before. This way, the branch of

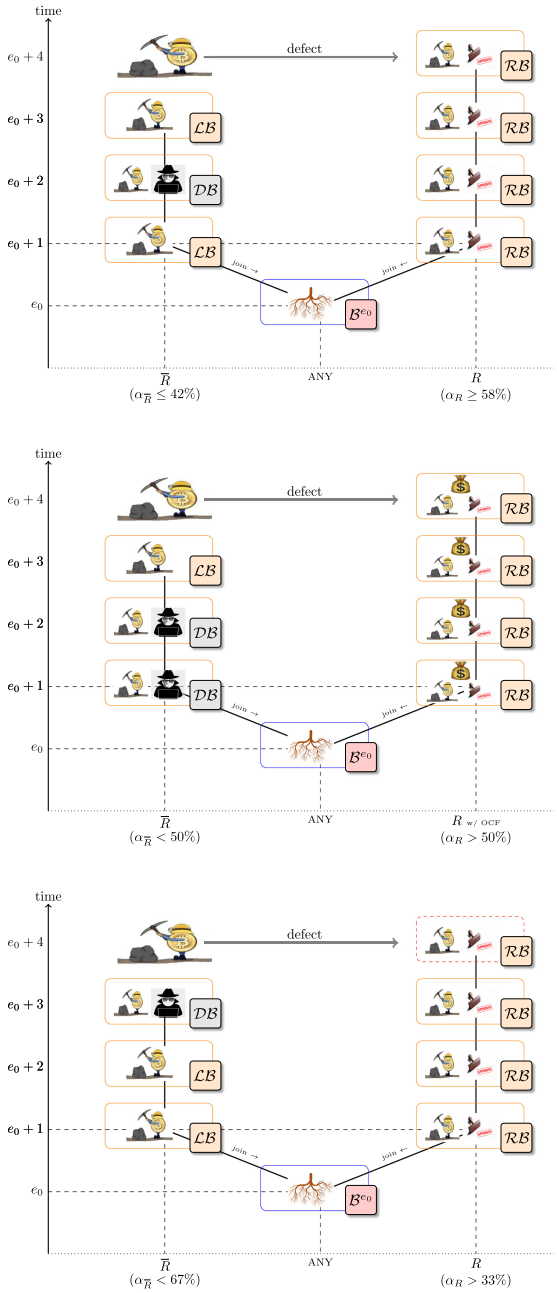

Fig. 5. (a) [Top] When ≥58% of the consensus resource is regulated, the legal branch (right) corresponding to R wins, by forcing $\overline{R}$ to abandon and defect from their branch. (b) [Middle] When >50% of the consensus resource is regulated, and the regulator adds an OCF (denoted by the money bag in $\mathcal{RB}$), the legal branch (right) corresponding to R wins, by forcing $\overline{R}$ to abandon their branch. (c) [Bottom] When >33% but <50% of the consensus resource is regulated, R can force $\overline{R}$ to abandon their branch through strategic release (unreleased $\mathcal{RB}$ block denoted by a dashed box in epoch $e_0 + 4$).

the regulated executors will have an additional weight of $\rho_{\mathcal{F}}$, and our model is equivalent to the blockchain pay-forward mining game in Reference [22].

4.5 A Stochastic Game with Strategic Block Release by Regulated Executors

Our final stochastic game considers best responses by R and $\bar{R}$, given that the regulator $\mathcal{F}$ licenses less than one-third ($\hat{h}_{SR} = 0.33$) of the total consensus resource, the unregulated executors (being in a majority) follow the longest branch rule, and the regulated executors can follow the SR model. The best responses are given in the following theorem.

Theorem 3 (Equilibrium under SR from R). *In the SR model for regulated executors R, given unregulated executors $\bar{R}$ play* `DubFrontier` *with IR, R playing* `RDubFrontier` *is a Nash Equilibrium only if $\alpha_R \leq \hat{h}_{SR} = 0.33$.*

Proof. The K1-SR-Game again considers two miners, named 1 and 2, where miner 2 is in a majority in the Bitcoin network ($\alpha_2 > 0.5$) and is always following the `Frontier` strategy while immediately releasing blocks. However, when it comes to miner 1, in the K1-SR-Game, the said miner only releases $min(b_1, b_2)$ blocks, where b_i blocks are successfully mined by miner $i \in \{1, 2\}$. In this regime, it is proven in Theorem 4.1 [20], that the best response for miner 1 is `Frontier` only when α_1 is less than the root of the polynomial $\alpha^3 - 6\alpha^2 + 5\alpha - 1 \approx 0.308$, but this bound can be improved to 0.33 through results in References [22, 30]. The RBChain-URdom-Game reduces to an instance of the K1-SR-Game, when the first miner is the regulated executor R following strategic release, the second miner is the unregulated executor $\bar{R}$, the first miner's `Frontier` strategy is replaced by the `RDubFrontier` strategy, and the second miner's `Frontier` strategy is replaced by the `DubFrontier` strategy. Consequently, the results on the threshold $\hat{h}_{SR}$ from the K1-SR-Game directly apply to the RBChain-URdom-Game. □

Theorem Implication (jointly with Theorem 2): In the case that $\mathcal{F}$ licenses less than 33% of the total consensus resource, R can do no better than adding legal blocks at the tip of the dubious branch, inducing a small increase in $t_{\mathcal{F}}$. However, if $\mathcal{F}$ is successful in licensing more than 33% and less than 50% of the total consensus resource, then it can orphan some of the dubious blocks through strategic release (or using SM1 [11]), thereby inducing a higher throughput: $t_{\mathcal{F}} \geq g_R > \alpha_R$ (and also $g_{\bar{R}} < \alpha_{\bar{R}}$). This scenario is depicted in Figure 5(c).

Justification of SR by regulated executors alone: The executors on the unregulated branch are of two types: law-abiding (but not licensed by the regulator), and law-breaking. It is clear from the illegal trading on the Silk Road market [33], that a major reason why law breakers choose Bitcoin for illegal trade is to misuse the anonymity it provides. If the law breaking executors decide to form an untrustworthy notarization (mining) pool with unlicensed law abiding executors for strategic release, it has been established [19] that such pools will not sustain due to mistrust that a dishonest notarization pool administrator may not fairly distribute notarization rewards to pool members.

Regulated executors may (righteously) attack the blockchain: When the regulated executors R are in a majority in the blockchain network, with $\alpha_R > 0.5$, these executors might attack the blockchain by using selfish mining strategies from References [11, 20, 30], thereby ensuring $t_{\mathcal{F}} = g_R = 1 > \alpha_R$. However, this policy is controversial for two reasons: (i) this requires hijacking the blockchain by a majority of the consensus executors, and more importantly (ii) it kills the legal transactions notarized in any competing branch. So, it is prudent to employ the "longest legal branch" rule when the regulated executors are in a majority, thereby fairly maintaining $g_R = \alpha_R$, and achieving $t_{\mathcal{F}} = 1$. When $0.33 < \alpha_R < 0.5$, assuming that $\bar{R}$ might misuse their dominance in the blockchain network to notarize dubious transactions, R may resort to a white hat attack on the blockchain by adopting a selfish mining strategy [11, 20, 30], to ensure $t_{\mathcal{F}} \geq g_R > \alpha_R$.

4.6 Discussion: Practical Application to Bitcoin

Practical Achievement of the Equilibrium Strategies from Sections 4.3, 4.4, and 4.5: Given any blockchain state, our regulated blockchain game analysis ensures the *existence* and *uniqueness* of the equilibrium strategies

mathematically, as per the Theorems 1–3. These equilibrium strategies are *reachable*, assuming there exists a consistent blockchain view across all executors, if (a) the executors are perfectly rational, then (b) the blockchain network knows the consensus resource divided between the regulated and unregulated executors. In the Bitcoin consensus protocol, the miners are incentivized by coinbase rewards to generate new blocks, and so they conform to rational behaviour. Further, in the Bitcoin network, α_R can be determined by all miners through the regulatory license announcement detailed in Section 3.4. Thus, for all the game-theoretic analysis in this section, all the equilibrium results discussed apply to the Bitcoin blockchain (with game depth $E = 100$ for the coinbase reward), and can be reached immediately by all miners for any blockchain state: The analysis from References [20, 22] changes negligibly on modifying the game depth E, and the stochastic game Markov chain stationary distributions and consequent utility function values can be computed efficiently by all miners on knowing α_R.

Practical Realization of Unfairly increased Legal Transaction Throughput (Section 4.5): The selfish mining results [11, 20, 30] are well established and can be used in practice for mounting the white-hat attack discussed in Section 4.5, for unfairly increasing the legal transaction throughput in the Bitcoin network. More specifically, given an α_R when R attack the blockchain for a higher legal transaction throughput, it has been simulated in Reference [30] using **Markov Decision Process (MDP)** solvers, that selfish miners (in our case R) can earn a higher block reward g_R (as compared to Reference [11]) by employing the attack strategy in Reference [30], for $\alpha_R \in (0.33, 0.5)$.

Drop in Regulated Miner Revenue: Finally, note that there is a significant decrease (by a factor $\frac{1}{2}$) in the expected reward g_R for the regulated miners once they cross the $\alpha_R = 0.5$ barrier. This is unavoidable due to their change from a selfish mining to an honest mining strategy, while preserving the maximum legal transaction throughput.

An open question: Another important aspect of the mining strategy equilibria is their *stability:* will the blockchain view across miners be same to allow miners to be consistent on the underlying stochastic game and determine the same equilibria? As long as a Byzantine adversary does not induce a large worst case message delay in the Bitcoin network and/or a large adversarial hashrate to violate the Bitcoin consistency condition in Reference [13], the equilibria from Theorems 1–3 would be stable. We leave it as an open question as to how the regulator $\mathcal{F}$ can regulate enough miners, so that it may bound the adversarial hashrate and adversary induced message delays in the Bitcoin network, so that the Bitcoin blockchain system is consistent (as per Reference [13]), and the mining equilibria are stable.

5 RELATED WORK

Existing cryptocurrencies can be leveraged for illegal transactions. Regulators have identified that the illegal use of blockchain-based cryptocurrencies includes money laundering and terror financing [18]. None of the existing blockchain protocols, be them permissionless or permissioned, are designed with regulation in the consensus mechanism itself [1]. This has introduced skepticism in the minds of regulatory authorities in the adoption of these protocols as is, and introduced regulation as a separate mechanism to be enforced by legal authorities. Even given separately enforced regulation, no comprehensive international regulatory framework exists for blockchain technology [21], and cross jurisdictional governmental collaboration for regulated trade via legal transactions over blockchains is needed [40].

Pocketed adoption of regulation on cryptocurrencies across the world. Licensing for legal use of cryptocurrencies was initially proposed by the New York financial services department, with the issuance of the "BitLicense" [4] virtual currency business license. Recently, the European Commission has proposed a new regulatory framework with a legislative proposal called **Markets in Crypto-Assets (MiCA)** [41], which mandates the legal rules to regulate crypto-asset types (such as stablecoins) and crypto-asset service providers. There have also been legislative proposals in Germany, Switzerland, Estonia, Singapore, Dubai, Malta, and Liechtenstein (among other countries), for regulating cryptocurrencies [16, 17, 29].

Permissionless blockchains introduce an untrusted decentralized cryptocurrency-based financial system. Apart from jurisdiction, blockchain technology can be an enabler of **decentralized autonomous organisations (DAOs)**, which have an uncertain legal status [38]. These systems facilitate illegal transactions for which conflict resolution or penalisation claims cannot be legally enforced with complete authority [8]. This drawback of these blockchains has already resulted in a fallout for the acceptance of Bitcoin, which has suffered a blow to being a trustworthy trade platform due to the large scale illegal trading in the Silk Road darknet market [33]. Given this illegal trade, and the existing mistrust in the deployment of Bitcoin for financial services in general, Bitcoin has been banned in many countries [39]. Further, decentralized regulatory frameworks for Bitcoin have been suggested for the application layer (and not the protocol layer) [25]. Regulatory proposals for Facebook's Libra cryptocurrency project have also been suggested, in the regulatory paradigms of consumer protection, market functions, and market integrity [42].

Central bank solutions and other approaches. Blockchain-based **central bank digital currencies (CBDCs)** are emerging as a competitive digital currency solution, parallel to cryptocurrencies. However, CBDCs retain the bias to the oligopolistic structure of the banking system, unlike cryptocurrencies, which have emerged as a democratized hedge against traditional financial systems [2]. Further, there have been proposals for regulation, using decentralized group signatures and verifiable encryption, to selectively reveal the physical identity of transactors to tracing authorities [24]. Finally, a recent tutorial on the performance evaluation of blockchain-based systems, for security and privacy in **Internet of Things (IoT)** networks [12], points to the use of the MIRACL cryptographic library in Reference [24] for analyzing the computational cost in the enforcement of traceability for a regulatory scheme.

Difference of existing regulatory frameworks from our proposal. None of the existing regulatory approaches allow (a) deterministic, verifiable agreement on legal transactions as part of the blockchain consensus, and (b) block proposal strategies, as a function of the regulated consensus resource, to maximize the legal transaction throughput. Both these features are integral to our regulatory system.

6 CONCLUSION AND FUTURE DIRECTIONS

In this contribution, we have proposed a framework for the legal trade of regulated assets via cryptocurrencies through the appropriate regulation of the consensus resource of existing blockchain protocols. We have given guarantees on legal transaction throughput as a function of the total fraction of the regulated consensus resource. We have shown that the legal transaction throughput can be maximized when the regulated consensus resource is in a majority in the blockchain network, under a "longest legal branch" block notarization rule.

In future, we would like to analyze the effect of adversarial behaviour with malicious mining and adversary induced network delays, to render an inconsistent blockchain view across protocol participants, resulting in unstable block notarization equilibrium strategies, similar to the analysis in References [9, 13, 35]. We would also like to perform a formal, novel MDP selfish mining analysis for block proposal competition between regulated and unregulated executors, similar to the proposal in Reference [43].

ACKNOWLEDGMENT

The authors thank Leana Golubchik (Professor, USC) for her constructive critique on an earlier version of this contribution.

REFERENCES

[1] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. 2019. SoK: Consensus in the age of blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*. 183–198.

[2] 101 Blockchains. (Online accessed 2021-07-06). Crypto vs. CBDC. Retrieved from https://101blockchains.com/crypto-vs-cbdc/.

[3] Benjamin Y. Chan and Elaine Shi. 2020. Streamlet: Textbook streamlined blockchains. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. 1–11.

[4] U. W. Chohan. 2018. Oversight and Regulation of Cryptocurrencies: BitLicense. SSRN.
[5] CNBC. (Online accessed 2020-11-06). Silk Road Cryptocurrency Bust by the U.S. Government. Retrieved from https://www.cnbc.com/2020/11/05/1-billion-worth-of-bitcoin-linked-to-the-silk-road-seized-by-the-us.html.
[6] CoinDesk. (Online accessed 2021-04-06). Altcoin Season pushes Crypto Market Value to $2T. Retrieved from https://www.coindesk.com/crypto-market-capitalization-2-trillion-first-time.
[7] Sourav Das, Vinay Joseph Ribeiro, and Abhijeet Anand. 2018. YODA: Enabling computationally intensive contracts on blockchains with Byzantine and Selfish nodes. Retrieved from https://arXiv:1811.03265.
[8] Blocks Decoded. (Online accessed 2020-05-21). 5 Blockchain Problems: Security, Privacy, Legal, Regulatory, and Ethical Issues. Retrieved from https://blocksdecoded.com/blockchain-issues-security-privacy-legal-regulatory-ethical/.
[9] Amir Dembo, Sreeram Kannan, Ertem Nusret Tas, David Tse, Pramod Viswanath, Xuechao Wang, and Ofer Zeitouni. 2020. Everything is a race and nakamoto always wins. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 859–878.
[10] Ethereum.org. (Online accessed 2021-09-09). Blocks. Retrieved from https://ethereum.org/en/developers/docs/blocks/.
[11] Ittay Eyal and Emin Gun Sirer. 2018. Majority is not enough: Bitcoin mining is vulnerable. *Commun. ACM* 61, 7 (2018), 95–102.
[12] Mohamed Amine Ferrag and Lei Shu. 2021. The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. *IEEE Internet Things J.* 8, 24 (2021), 17236–17260.
[13] Peter Gaži, Aggelos Kiayias, and Alexander Russell. 2020. Tight consistency bounds for bitcoin. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 819–838.
[14] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. 2017. Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles*. 51–68.
[15] Robert Augustus Hardy and Julia R. Norgaard. 2016. Reputation in the Internet black market: An empirical and theoretical analysis of the Deep Web. *Journal of Institutional Economics* 12, 3 (2016), 515–539.
[16] Mondaq (India). (Online accessed 2021-06-15). Global Cryptocurrency Regulatory Landscape. Retrieved from https://www.mondaq.com/india/fin-tech/1044546/global-cryptocurrency-regulatory-landscape.
[17] Analytics Insight. (Online accessed 2021-06-15). A Rundown of Cryptocurrency Regulations across the World. Retrieved from https://www.analyticsinsight.net/a-rundown-of-cryptocurrency-regulations-across-the-world/.
[18] Global Legal Insights. (Online accessed 2020-05-21). Blockchain and Cryptocurrency Regulation 2019, First Edition. Retrieved from https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775-1.pdf.
[19] Irni Eliana Khairuddin and Corina Sas. 2019. An exploration of bitcoin mining practices: Miners' trust challenges and motivations. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–13.
[20] Aggelos Kiayias, Elias Koutsoupias, Maria Kyropoulou, and Yiannis Tselekounis. 2016. Blockchain mining games. In *Proceedings of the ACM Conference on Economics and Computation*. 365–382.
[21] Trevor I. Kiviat. 2015. Beyond bitcoin: Issues in regulating blockchain tranactions. *Duke LJ* 65 (2015), 569.
[22] Elias Koutsoupias, Philip Lazos, Foluso Ogunlana, and Paolo Serafino. 2019. Blockchain mining games with pay forward. In *Proceedings of the World Wide Web Conference*. 917–927.
[23] Wenting Li, Sebastien Andreina, Jens-Matthias Bohli, and Ghassan Karame. 2017. Securing proof-of-stake blockchain protocols. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 297–315.
[24] Yannan Li, Willy Susilo, Guomin Yang, Yong Yu, Xiaojiang Du, Dongxi Liu, and Nadra Guizani. 2019. Toward privacy and regulation in blockchain-based cryptocurrencies. *IEEE Netw.* 33, 5 (2019), 111–117.
[25] Hossein Nabilou. 2019. How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency. *Int. J. Law Info. Technol.* 27, 3 (2019), 266–291.
[26] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentral. Bus. Rev.* (2008), 21260.
[27] Bitcoin News. (Online accessed 2021-01-26). ECB Chief Christine Lagarde Calls for Global Bitcoin Regulation, Says BTC Conducts 'Funny Business'. Retrieved rom https://news.bitcoin.com/ecb-christine-lagarde-global-bitcoin-regulation-btc/.
[28] Bitcoin News. (Online accessed 2021-01-26). Janet Yellen Reveals Plans for Bitcoin, Sees Cryptocurrencies Used Mainly for Illicit Financing. Retrieved from https://news.bitcoin.com/janet-yellen-bitcoin-cryptocurrencies-illicit-financing/.
[29] Perkinscoie. (Online accessed 2021-04-06). Digital Currencies: International Actions and Regulations. Retrieved from https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html.
[30] Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar. 2016. Optimal selfish mining strategies in bitcoin. In *Proceedings of the International Conference on Financial Cryptography and Data Security*. Springer, 515–532.
[31] Eilon Solan and Nicolas Vieille. 2015. Stochastic games. *Proc. Natl. Acad. Sci. U.S.A.* 112, 45 (2015), 13743–13746.
[32] Volker Stocker, Georgios Smaragdakis, and William Lehr. 2020. The state of network neutrality regulation. *ACM SIGCOMM Computer Communication Review* 50, 1 (2020), 45–59. Available at: https://dl.acm.org/doi/pdf/10.1145/3390251.3390258
[33] Lawrence J. Trautman. 2014. Virtual currencies: Bitcoin & what now after liberty reserve, silk road, and Mt. Gox? *Richmond J. Law Technol.* 20, 4 (2014).
[34] Marie Claire Van Hout and Tim Bingham. 2013. "Surfing the silk road": A study of users' experiences. *Int. J. Drug Policy* 24, 6 (2013), 524–529.

[35] Luming Wan, David Eyers, and Haibo Zhang. 2019. Evaluating the impact of network latency on the safety of blockchain transactions. In *Proceedings of the IEEE International Conference on Blockchain (Blockchain'19)*. IEEE, 194–201.
[36] Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim. 2019. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access* 7 (2019), 22328–22370.
[37] Bitcoin Wiki. (Online accessed 2021-07-07). Transaction. Retrieved from https://en.bitcoin.it/wiki/Transaction.
[38] Wikipedia. (Online accessed 2020-05-21). Decentralized Autonomous Organisations. Retrieved from https://en.wikipedia.org/wiki/Decentralized-autonomous-organization.
[39] Wikipedia. (Online accessed 2020-05-21). Legality of bitcoin by country or territory. Retrieved from https://en.wikipedia.org/wiki/Legality-of-bitcoin-by-country-or-territory.
[40] Peter Yeoh. 2017. Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance* 25, 2 (2017), 196–208.
[41] Dirk A. Zetzsche, Filippo Annunziata, Douglas W. Arner, and Ross P. Buckley. 2021. The markets in crypto-assets regulation (MiCA) and the EU digital finance strategy. *Cap. Markets Law J.* 16, 2 (2021), 203–225.
[42] Dirk A. Zetzsche, Ross P. Buckley, and Douglas W. Arner. 2019. Regulating LIBRA: The transformative potential of Facebook's cryptocurrency and possible regulatory responses. European Banking Institute Working Paper Series 2019/44, University of New South Wales Law Research Series UNSWLRS 19-47, University of Hong Kong Faculty of Law Research Paper No. 2019/042, University of Luxembourg Faculty of Law Research Paper, Oxford Journal of Legal Studies (Forthcoming). Available at SSRN: https://ssrn.com/abstract=3414401.
[43] Roi Bar Zur, Ittay Eyal, and Aviv Tamar. 2020. Efficient MDP analysis for selfish-mining in blockchains. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. 113–131.

Received 29 December 2021; revised 5 September 2022; accepted 27 September 2022