Game-Theoretic View on Decentralized Proof Generation in zk-SNARK-based Sidechains

Yuri Bespalov[a], Alberto Garoffolo[b], Lyudmila Kovalchuk[c,d], Hanna Nelasa[e], and Roman Oliynykov[c,f]

[a] *Bogolyubov Institute for Theoretical Physics, 14b, Metrolohichna str., Kyiv, 03143, Ukraine*
[b] *Zen Blockchain Foundation,701 Gervais str, Columbia, South Carolina, 29201, USA*
[c] *Input Output HK, Tesbury Centre, Queen's Road East, 24-32, Hong Kong*
[d] *Igor Sikorsky Kyiv Polytechnic Institute, 37 Peremohy ave., Kyiv, 03056, Ukraine*
[e] *Zaporizhzhia Polytechnic National University, 64 Zhukovskogo str., Zaporizhzhia, 69063, Ukraine*
[f] *V. N. Karazin Kharkiv National University, 4 Svobody sq., Kharkiv, 61022, Ukraine*

Abstract

In this paper, we investigate the behavior of provers in decentralized proof generation for zk-SNARK Based Sidechains, specifically, Latus consensus protocol. We obtained results that give necessary and sufficient conditions for the existence of the Nash equilibrium, and the value of the relevant utility function, for various parameters of the sidechain and various price policies. These results allow picking a price policy to ensure the stable operation of the sidechain.

Keywords

Blockchain, sidechain, game theory, Nash equilibrium, Latus, Ouroboros Praos, Merkle tree

1. Introduction

This paper deals with a relatively new direction in cryptology - blockchains and cryptocurrencies. It investigates sidechains as a new instrument in blockchain technology. Sidechains (SCs) [1-4] are very adequate and universal instruments in blockchain technology. They may be used as an extension of a blockchain in the case when we need some additional functionality that is not available in the initial blockchain (that is called the main chain).

SCs may use both Proof-of-Work and Proof-of-Stake protocols. In this paper, we are dealing with Latus Protocol [5] which is a hybrid PoS based on Ouroboros Praos [6] with an additional feature of binding to a PoW mainchain (MC). SCs should bind to MC, as described in [1-5], to provide such necessary blockchain properties as liveness and persistence [7]. SC also should send some information to MC to guarantee the fairness of transformations in SC. This information contains a series of recurrent zk-SNARK-proofs [8, 9] to establish decentralized and verifiable cross-chain transfers. Latus introduces a special dispatching scheme that assigns generation of proofs randomly to interested parties who then perform these tasks in parallel and submit generated proofs to the blockchain. An incentive scheme provides a reward for each valid submission.

The general idea of Latus is to utilize a recursive composition of SNARKs to construct a succinct proof of the sidechain state progression for the period of a withdrawal epoch. Then, a SNARK for a withdrawal certificate is constructed so that it proves the correct sidechain state transition for the whole epoch and validates backward transfers. That allows the mainchain to verify the sidechain efficiently without having to rely on any intermediary—such as certifiers [4]—and still be oblivious to the sidechain construction and interactions within.

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: yu.n.bespalov@gmail.com (A.1); alberto@horizen.global (B.2); lusi.kovalchuk@gmail.com (C.3); annanelasa@gmail.com (D.4); roliynykov@gmail.com (C.5)
ORCID: 0000-0003-0503-953X (A.1); 0000-0003-2874-7950 (B.2); 0000-0002-3708-0089 (C.3); 0000-0002-3494-0493 (D.4); 0000-0002-3494-0493 (C.5)

In an SC, the entity that creates the block, the block forger, shares a list of transactions, which he intends to include into the block, with other entities, called provers. The provers construct SNARK-proofs for these transactions and also for each node of the corresponding Merkle tree. Each prover sets prices for his proofs, according to the price policy of the current epoch that was set at the end of the previous one. If there are a few proofs for a certain node, the block forger chooses the cheapest one.

The results of this paper continue a series on combinatorial, stochastic, and game-theoretic aspects of distributed proof generation for zk-SNARK-based blockchains started in [10].

In what follows, we will describe the operation of SCs, and, first of all, provers' behavior, from the game-theoretical point of view. We will show that the optimal provers' behavior, i.e. Nash equilibrium in the corresponding symmetric game, is fully determined by the price policy and by such parameters as the number of proofs and the number of provers.

We obtained necessary and sufficient conditions for the existence of the Nash equilibrium, for various models, price policies, and parameters, both in pure and mixed strategies. Such results allow modeling and sometimes prediction of the provers' behavior, proof prices, and block forgers' rewards, and help the inadequate setting of the price policy, to provide stable operation of SC.

The paper is organized as follows. In Chapter 2, we recall some basic definitions from game theory and general results on the existence of the Nash equilibrium. Then, in Chapter 3, we:

- Give the mathematical model of a one-step game, that we will use to describe distributed proof generation.
- Obtain some auxiliary results which we need to find Nash equilibrium for different price policies and other parameters.
- Obtain necessary and sufficient conditions for the Nash equilibrium existence.
- Describe these Nash equilibriums and corresponding utility functions.

In Chapter 4 we study the natural continuation and development of the one-step game, described in Definition 1, and formulate new Definition 5. This new game that is also a one-step game, deals with the creation of a sequence of blocks, rather than the creation of only one block. We investigate provers' behavior, allowing them to choose proofs from different blocks.

2. Preliminaries

Let us recall some basic definitions from game theory. More details can be found in one of the textbooks, in particular [11].

Definition 1. A *strategic form game* consists of
the set of *player*s $P = \{1,2, \dots, m\}$;
and for each player i
the non-empty set of *pure strategies* S_i;
the utility (payment) function $u_i : \prod_{i \epsilon P} S_i \to R$.

A *strategy profile* is a combination of strategies of each player, i.e. an element of the Cartesian product $\prod_{i \epsilon P} S_i$.

Definition 2. A game is called *symmetric* if all strategy sets S_i are the same and for each permutation π of strategies

$$u_{\pi(i)}(s_1, \dots, s_m) = u_i\big(s_{\pi(1)}, \dots, s_{\pi(m)}\big).$$

In this case, u_i is a symmetric function of all its arguments except for the i^{th}.

Note that replacement of the left action of the symmetric group by the right action leads to a stronger notion of *fully symmetric game* [12].

Definition 3. If the sets of strategies are equipped with a topology, one can consider the corresponding Borel σ-algebra.

A *mixed (randomized) strategy* μ_i is a Borel probability measure on the set of strategies S_i.

The utility for mixed strategy μ_i on the jth place is the expectation calculated via Lebesgue integral:

$$u_i(\dots, \mu_j, \dots) = \int_{S_j} u_i(\dots, s_j, \dots)\, d\mu(s_j).$$

Definition 4. A *pure strategy Nash equilibrium* is a strategy profile $(s_i)_{i\in P} \in \prod_{i\in P} S_i$, where for each $i \in P$,

$$u_i(s_1 \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_m) \geq u_i(s_1 \dots, s_{i-1}, s_i', s_{i+1}, \dots, s_m) \text{ for all } s_i' \in S_i.$$

A *mixed strategy Nash equilibrium* is a mixed strategy profile $(\mu_i)_{i\in P}$, where for each $i \in P$

$$u_i(\mu_1 \dots, \mu_{i-1}, \mu_i, \mu_{i+1}, \dots, \mu_m) \geq u_i(\mu_1 \dots, \mu_{i-1}, \mu_i', \mu_{i+1}, \dots, \mu_m)$$

for all mixed strategies μ_i' on S_i.

In this paper, we consider a symmetric game and are looking for a symmetric Nash equilibrium given by the same probability measure μ^* repeated m times. In this case, we can formulate an equivalent Nash equilibrium criterion by making comparisons only with pure strategies:

Lemma 1. *For any symmetric game, a symmetric Nash equilibrium is given by a probability measure μ^* iff the utility*

$$u_1(s_1, \mu^*, \dots, \mu^*) = \int_{S^{m-1}} u_1(s_1, \dots, s_m) \prod_{j=2}^{m} d\mu^*(s_j)\,. \tag{1}$$

satisfies the condition

$$supp\ \mu^* \subseteq \underset{s_1\in S}{argmax}\, u_1(s_1, \mu^* \dots, \mu^*). \tag{2}$$

where supp μ^* *is the support of the measure μ^*.*

In this case, the game price is

$$u^* = \max_{s_1\in S} u_1(s_1, \mu^* \dots, \mu^*).$$

3. The Case of One-Step Game of Distributed Proof Generations

3.1 Description of the Game

In what follows, under a one-step game, we will mean a symmetric strategic game corresponding to one step of provers' work for a distributed proof generation.

Definition 5. (One-step game).

Each i^{th} prover (≡ player), i ∈ {1,2, … , m}, randomly selects and builds one of n proofs according to the function g: {1,2, … , m} → {1,2, … , n} and quote a price (≡strategy) $s_i \in S \subset \mathbb{R}_{>0}$ for his work.

Let $I \subseteq \{1,2, \dots, m\}$, $I \neq \emptyset$. For the function $I \ni i \mapsto s_i$, consider the set

$$\underset{i'\in I}{\text{argmin}}(s_{i'}) \coloneqq \{i'' \in I \mid s_{i''} = \min_{i'\in I} s_{i'}\}. \tag{3}$$

A block-forger, for every built j-th proof, allocates a subset $\underset{i'\in g^{-1}(j)}{\text{argmin}}(s_{i'})$ of provers, who asked the minimal price $s_{i'}$, among the set $g^{-1}(j)$ of all provers who built it, randomly selects a prover from the allocated subset and pays him the declared price.

For the subset (3) in {1,2, … , m}, consider the corresponding δ-function

$$\delta_{\underset{i'\in I}{\text{argmin}}(s_{i'})}\colon \{1,2, \dots, m\} \to \mathbb{R}, i \to \begin{cases} \dfrac{1}{\#\underset{i'\in I}{\text{argmin}}(s_{i'})}, \text{if } i \in \underset{i'\in I}{\text{argmin}}(s_{i'})\,; \\ 0, \text{otherwise.} \end{cases}$$

For a fixed i^{th} prover and for a fixed set $g^{-1}(g(i))$ of other provers that select the same proof after averaging overall selections of the block-forger, the payment for this prover will be $s_i \cdot \delta_{\underset{i' \in g^{-1}(g(i))}{\operatorname{argmin}(s_{i'})}}(i)$. Each subset $I \subseteq \{1,2,\dots,m\}$ with $i \in I$ appeared as $g^{-1}(g(i))$ with probability $\left(\frac{1}{n}\right)^{|I|-1}\left(\frac{n-1}{n}\right)^{m-|I|}$. The number κ_i of other provers, which select the same proof as to the i^{th} prover, has the binomial distribution (as a sum of independent Bernoulli random variables):

$$\mathbf{Pr}(\kappa_i = k) = \binom{m-1}{k}\left(\frac{1}{n}\right)^k\left(\frac{n-1}{n}\right)^{m-k-1} = \binom{m-1}{k}\frac{(n-1)^{m-k-1}}{n^{m-1}}.$$

Then the utility of the i-th prover is

$$u_i(s_1,\dots,s_m) = \sum_{\substack{I\subseteq\{1,2,\dots,m\}\\ i\in I}} \frac{(n-1)^{m-|I|}}{n^{m-1}} \cdot s_i \cdot \delta_{\underset{i' \in g^{-1}(g(i))}{\operatorname{argmin}(s_{i'})}}(i) \cdot \tag{4}$$

For example, in the case of two provers

$$u_1(s_1,s_2) = \frac{n-1}{n}s_1 + \frac{1}{n}\begin{cases} s_1, \text{if } s_1 < s_2, \\ s_1/2\,, \text{if } s_1 = s_2, \\ 0, \text{if } s_1 > s_2. \end{cases} \tag{5}$$

The general formula (4) or its particular cases will be used in all following statements

3.2 The Utility in Mixed Strategies. Auxiliary Results

Below we formulate and prove some auxiliary results that were helpful in obtaining the main results.

The following Lemma adopts the general case of the utility function for the Nash equilibrium for the one-step game from Definition 5.

Lemma 2. *The utility (1) for a one-step game admits the expression*

$$u_1(s_1,\mu^*\dots,\mu^*) = \frac{s_1}{mn^{m-1}}\sum_{k=0}^{m-1}\left(\mu^*(S_{\geq s_1})+n-1\right)^k\left(\mu^*(S_{\geq s_1})+n-1\right)^{m-k-1}, \tag{6}$$

where $S_{\geq s_1} = \{s \in S \mid s \geq s_1\}$ *and* $S_{>s_1} = \{s \in S \mid s > s_1\}$.

In particular, when $\mu^*(s_1) = 0$

$$u_1(s_1,\mu^*\dots,\mu^*) = \frac{s_1}{n^{m-1}}\left(\mu^*(S_{\geq s_1})+n-1\right)^{m-1}. \tag{7}$$

Proof. Substitution of (4) into (1) and then grouping together of the summands with the same cardinality of I yields

$$\begin{aligned} u_1(s_1,\mu^*\dots,\mu^*) &= \frac{s_1}{n^{m-1}}\sum_{\substack{I\subseteq\{1,2,\dots,m\}\\ i\in I}}(n-1)^{m-|I|}\int_{S_{\geq s_1}^{|I|-1}}\frac{1}{\#\operatorname{argmin}_{j\in I}(s_j)}\prod_{j\in I\setminus\{1\}}d\mu^*(s_j) = \\ &= \frac{s_1}{n^{m-1}}\sum_{k=0}^{m-1}\binom{m-1}{k}(n-1)^{m-k-1}\int_{S_{\geq s_1}^{k}}\frac{1}{\#\operatorname{argmin}_{1\leq j\leq k+1}(s_j)}\prod_{j=2}^{k+1}d\mu^*(s_j). \end{aligned} \tag{8}$$

If $\mu^*(s_1) = 0$, one can ignore in (8) the set of zero measure, where $s_1 = s_i$ for some $i \neq 1$, then use of the Fubini's theorem and the binomial identity to get (7)

$$u_1(s_1, \mu^* \dots, \mu^*) = \frac{s_1}{n^{m-1}} \sum_{k=0}^{m-1} \binom{m-1}{k} (n-1)^{m-k-1} \mu^*(S_{\geq s_1})^k$$
$$= \frac{s_1}{n^{m-1}} \left(\mu^*(S_{\geq s_1}) + n - 1\right)^{m-1}$$

Then we need the identity

$$\sum_{k=0}^{n} \binom{n}{k} \frac{p^k q^{n-k}}{k+1} = \frac{1}{p(n+1)} \sum_{k=0}^{n} \binom{n+1}{k+1} p^{k+1} q^{n-k} = \frac{(p+q)^{n+1} - q^{n+1}}{p(n+1)}. \quad (9)$$

In the case $p + q = 1$, this is the expectation of $1/(k+1)$ with respect to the binomial distribution.

If $\mu^*(s_1) > 0$, one can rewrite (8) using (9) three times:

$$u_1(s_1, \mu^* \dots, \mu^*) = \frac{s_1}{n^{m-1}} \sum_{k=0}^{m-1} \binom{m-1}{k} (n-1)^{m-k-1} \sum_{l=0}^{k} \binom{k}{l} \frac{\mu^*(s_1)^l \mu^*\left(S_{\geq s_1}\right)^{k-l}}{l+1} =$$
$$= \frac{s_1}{n^{m-1}} \sum_{k=0}^{m-1} \binom{m-1}{k} (n-1)^{m-k-1} \frac{\mu^*\left(S_{\geq s_1}\right)^{k+1} - \mu^*\left(S_{>s_1}\right)^{k+l}}{(k+1)\mu^*(s_1)} =$$
$$\frac{s_1}{n^{m-1}} \frac{(\mu^*\left(S_{\geq s_1}\right) + n - 1)^m - (\mu^*\left(S_{>s_1}\right) + n - 1)^m}{m\mu^*(s_1)} =$$
$$= \frac{s_1}{mn^{m-1}} \sum_{k=0}^{m-1} (\mu^*\left(S_{\geq s_1}\right) + n - 1)^k (\mu^*\left(S_{>s_1}\right) + n - 1)^{m-k-1}$$

For $m \in \mathbb{Z}_{>0}$, consider the following homogeneous polynomials

$$p_m(x, y) = \frac{x^m - y^m}{x - y} = \sum_{k=0}^{m-1} x^k y^{m-k},$$
$$q_m(x, y, z) \coloneqq p_m(x, y) p_m(x, z) - p_m(x, x) p_m(y, z) =$$
$$= p_m(x, y) p_m(x, z) - m x^{m-1} p_m(y, z).$$

Lemma 3.

1. The following polynomial identity is true

$$q_m(x, y, z) = \sum_{k=1}^{m-1} x^{m-1-k} p_{m-k}(y, z)\left(x^k - y^k\right)\left(x^k - z^k\right) =$$
$$= q_2(x, y, z) = \sum_{k=1}^{m-1} x^{m-1-k} p_{m-k}(y, z) p_k(x, y) p_k(x, z), \quad (10)$$

2. For positive x, y, z, if $q_2(x, y, z) = (x - y)(x - z) > 0$ then $q_m(x, y, z) > 0$ for all $m \geq 2$.

Proof. Parts of (10) equals to

$$\sum_{k=1}^{m-1} \sum_{\substack{i,j \geq 0 \\ i+j=m-1-k}} \left(x^{m-1+k} y^i z^j + x^{m-1-k} y^{i+k} z^{j+k} - x^{m-1} y^i z^{j+k} - x^{m-1} y^{i+k} z^j\right)$$

The expression ν_{mn} and the interval from the following lemma appears in the description of Nash equilibriums.

Lemma 4.

1. *The utility on the symmetric profile of pure strategies has the form*

$$u_i(s,\dots,s) = s\upsilon_{mn},\ \upsilon_{mn} \coloneqq \frac{n^m-(n-1)^m}{mn^{\{m-1\}}}. \tag{11}$$

2. *For $m,n \geq 2$ the following interval is nonempty*

$$\left(\upsilon_{mn}^{-1}\ \frac{(n-1)^{m-1}}{n^{m-1}}, \upsilon_{mn}\right) = \left(\frac{m(n-1)^{m-1}}{n^m-(n-1)^m}, \frac{n^m-(n-1)^m}{mn^{m-1}}\right). \tag{12}$$

3. *The endpoints and length of the above interval admit the asymptotics*

$$\lim_{\substack{m,n\to\infty \\ n/m\to z}} \upsilon_{mn} = z\left(1-e^{-1/z}\right) \underset{z\to+\infty}{=} 1-\frac{1}{2z}+O\left(\frac{1}{z^2}\right),$$

$$\lim_{\substack{m,n\to\infty \\ n/m\to z}} \left(\upsilon_{mn}-\upsilon_{mn}^{-1}\ \frac{(n-1)^{m-1}}{n^{m-1}}\right) = z\left(1-e^{-1/z}\right)-\frac{e^{-1/z}}{z(1-e^{-1/z})} \underset{z\to+\infty}{=} \frac{1}{12z^2}+O\left(\frac{1}{z^3}\right)$$

Proof. The identity (11) can be obtained directly or as the special case of (6).

The inequality $\upsilon_{mn}^{-1}\ \frac{(n-1)^{m-1}}{n} < \upsilon_{mn}$ between endpoints of (12) is equivalent to the positivity of $q_m(n,n-1,n-1)$ from Lemma 3.

Asymptotic formulas come from easy calculation with the Maclaurin series.

3.3 Pure Strategy Nash Equilibrium

Here we obtain the main results are obtained on the Nash equilibrium for a game from Definition 5 in pure strategies for the general case (Proposition 1) and a particular case (Corollary 1) with only two strategies. We also provide numerical examples are given, built using these statements.

Proposition 1. *Let S be the set of pure strategies and $s^* \in S$. The profile $(s_i = s^*)_{1\leq i\leq m}$ is a symmetric Nash equilibrium iff for all $s \in S$ the following two conditions hold*

1. *If $s < s^*$ then $s \leq \upsilon_{mn}s^*$. (I.e. $S \cap (\upsilon_{mn}\ s^*, s^*) = \emptyset$.)*
2. *If $s > s^*$ then $s\left(\frac{n-1}{n}\right)^{m-1} \leq \upsilon_{mn}s^*$.*

Proof. Note that

$$u_1(s,s^*,\dots,s^*) = \begin{cases} s, \text{if } s_1 < s^*, \\ \upsilon_{mn}\ s, \text{if } s_1 = s^*, \\ \left(\frac{n-1}{n}\right)^{m-1}, \text{if } s_1 > s^*. \end{cases}$$

Then $u_1(s^*,s^*,\dots,s^*) \geq u_1(s,s^*,\dots,s^*)$ yields the conditions 1 and 2 from the proposition.

Example 1 (Numerical).

1. Let $\mathrm{m} = 50, \mathrm{n} = 10\ \mathrm{S} = \{1,2,\dots,10\}$. Then only one Nash equilibrium exists in pure symmetric strategies with $\mathrm{s}^* = 1$.
2. Let $\mathrm{m} = 100, \mathrm{n} = 10000\ \mathrm{S} = \{1,2,\dots,10\}$. Then only one Nash equilibrium exists in pure symmetric strategies with $\mathrm{s}^* = 10$.
3. Let $\mathrm{m} = \mathrm{n} = 200\ \mathrm{S} = \{1,2,3,4,5,9,9.1,9.2,9.3,\dots,10\}$. Then only one Nash equilibrium exists in pure symmetric strategies with $\mathrm{s}^* = 9$.

Corollary 1. *Suppose that S consists of two strategies $\{s_{min} < s_{max}\}$.*

1. *The profile $(s_i = s_{max})_{1\leq i\leq m}$ is a symmetric Nash equilibrium iff $\frac{s_{min}}{s_{max}} \leq \upsilon_{mn}$.*
2. *The profile $(s_i = s_{min})_{1\leq i\leq m}$ is a symmetric Nash equilibrium iff $\frac{s_{min}}{s_{max}} \geq \upsilon_{mn}^{-1}\ \left(\frac{n-1}{n}\right)^{m-1}$.*
3. *Both profiles $(s_i = s_{max})_{1\leq i\leq m}$ and $(s_i = s_{min})_{1\leq i\leq m}$ are symmetric Nash equilibria iff $\frac{s_{min}}{s_{max}}$ lies in the interval $\left[\frac{m(n-1)^{m-1}}{n^m-(n-1)^m}, \frac{n^m-(n-1)^m}{mn^{m-1}}\right]$ from (12).*

Example 2 (Numerical).

Let $S = \{s_{\min}, s_{\max}\}$,

$m \in \{2, 10, 50, 100, 200, 500\}$,

$n \in \{2, 10, 50, 100, 200, 500, 10^3, 2 \cdot 10^3, 5 \cdot 10^3, 10^4\}$.

Define $b = \frac{s_{\min}}{s_{\max}}$. Then if $b = 0.1$ and $n \geq m$, the Nash equilibrium exists in pure symmetric strategies with $s^* = s_{\max}$.

If $m = 10$ and $n = 2$, or $m = 50$ and $n = 10$, or $m = 200$ and $n = 50$, or $m = 500$ and $n = 100$, two Nash equilibria exist in pure symmetric strategies with $s^* = s_{\min}$ and $s^* = s_{\max}$.

For all other values of m, n from the set ranges, Nash equilibrium exists in pure symmetric strategies with $s^* = s_{\min}$.

3.4 Mixed Strategies Absolutely Continuous in an Interval

Here we obtain the main results on the Nash equilibrium for the game from Definition 5 in mixed strategies that are considered as absolutely continuous measures on some intervals. Numerical examples are provided to illustrate the results obtained.

Proposition 2. *Suppose that the set of strategies is an interval* $S = [s_{min}, s_{max}]$.

A symmetric Nash equilibrium is given by the probability measure μ^* *absolutely continuous with respect to the Lebesgue measure exists iff* $\frac{s_{min}}{s_{max}} \leq \left(\frac{n-1}{n}\right)^{m-1}$. *In this case, the game price and the support of the measure are*

$$u^* = s_{max} \frac{(n-1)^{m-1}}{n^{m-1}}, supp\ \mu^* = [u^*,\ s_{max}] \tag{13}$$

and the density of the measure μ^* *is*

$$\frac{d\mu^*(s)}{ds} = \frac{n-1}{m-1} \frac{s_{max}^{1/(m-1)}}{s^{m/(m-1)}}. \tag{14}$$

Proof. The support of the measure μ^* should be a subinterval $\text{supp}\ \mu^* = [s'_{min},\ s_{max}]$, $s'_{min} \in [s_{min},\ s_{max})$ and the formula (7) for the game price u^* is

$$\frac{s_1}{n^{m-1}} \left(\mu^*\left(S_{\geq s_1}\right) + n - 1\right)^{m-1} = u^*,\ s'_{min} \leq s_1 \leq s_{max}. \tag{15}$$

Substitutions of $s_1 = s_{max}$ and $s_1 = s'_{min}$ in (15) yield $s'_{min} = u^* = s_{max} \left(\frac{n-1}{n}\right)^{m-1}$

Then (15) can be rewritten as

$$\mu^*\left(S_{\{\geq s_1\}}\right) = \int_{s_1}^{s_{max}} d\mu^*(s) = (n-1) s_{max}^{1/m-1} s_1^{-1/m-1} - n + 1.$$

Taking derivative in $s \in \text{supp}\ \mu^* = [s'_{min}, s_{max}]$, we obtain the formula for the density.

Remark 1. Note that in the previous proposition

$$\lim_{\substack{m,n\to\infty \\ n/m\to z}} \frac{min \frac{d\mu^*(s)}{ds}}{max \frac{d\mu^*(s)}{ds}} = \lim_{\substack{m,n\to\infty \\ n/m\to z}} \left(1 - \frac{1}{n}\right)^m = e^{-\frac{1}{z}} \underset{z\to+\infty}{=} 1 - \frac{1}{z} + O\left(\frac{1}{z^2}\right).$$

So, for large n/m the measure μ^* is closed to uniform.

Example 3 (Numerical).

Let parameters m, n take the same values as in Numerical example 2, $S = [s_{min}, s_{max}]$, $b = \frac{s_{min}}{s_{max}} = 0.1$. Then the existence of the Nash equilibrium in mixed strategy (20), (21) is described by the following Table 1, where "+" stands for the existence of the Nash equilibrium for given parameters, "-" stands for its absence.

Table 1
Existence of Nash equilibrium in mixed strategy (20), (21)

m n	2	10	50	100	200	500
2	+	-	-	-	-	-
10	+	+	-	-	-	-
50	+	+	+	+	-	-
100	+	+	+	+	+	-
200	+	+	+	+	+	-
500	+	+	+	+	+	+
1000	+	+	+	+	+	+
2000	+	+	+	+	+	+
5000	+	+	+	+	+	+
10000	+	+	+	+	+	+

From Table 1 we can conclude that Nash equilibrium in mixed strategies always exists when the number of proofs is bigger than the number of provers.

It also should be noted that, though the case of a continuous set of strategies seems unreal, we may use some approximations of these results in the case when prices may change in very small steps.

3.5 The Cases of Discreet Measures

Here we obtain conditions of the Nash equilibrium for the game from Definition 5 in mixed strategies that are considered as discrete measures on some intervals, for various sets of strategies and other parameters.

Proposition 3. *Suppose that the set of strategies $S = \{s_{min} < s_{max}\}$ consists of two elements. Then the symmetric Nash equilibrium in mixed strategies μ^* exists iff the value $\frac{s_{min}}{s_{max}}$ lies on the interval from (12):*

$$\frac{s_{min}}{s_{max}} \in \left(\frac{m(n-1)^{m-1}}{n^m - (n-1)^m}, \frac{n^m - (n-1)^m}{mn^{m-1}} \right) \tag{16}$$

In this case, $n - \mu^*(s_{min})$ is the a root of the polynomial

$$h(x) = \sum_{k=0}^{m-1} \left(s_{min} n^k - s_{max}(n-1)^k \right) x^{m-k-1}; \tag{17}$$

and the game price is

$$\begin{aligned} u^* &= \frac{s_{max}}{mn^{m-1}} \sum_{k=0}^{m-1} (n-1)^k \left(n - 1 + \mu^*(s_{max}) \right)^{m-k-1} \\ &= \frac{s_{min}}{mn^{m-1}} \sum_{k=0}^{m-1} n^k \left(n - \mu^*(s_{max}) \right)^{m-k-1}. \end{aligned} \tag{18}$$

Proof. As special cases of (6), we get

$$\begin{aligned} u_1(s_{max}, \mu^*, \dots, \mu^*) &= \frac{s_{max}}{mn^{m-1}} \sum_{k=0}^{m-1} (n-1)^k \left(n - \mu^*(s_{min}) \right)^{m-k-1}, \\ u_1(s_{max}, \mu^*, \dots, \mu^*) &= \frac{s_{min}}{mn^{m-1}} \sum_{k=0}^{m-1} n^k \left(n - \mu^*(s_{min}) \right)^{m-k-1}. \end{aligned} \tag{19}$$

The equality between two expressions from (19) takes the form $h\left(n - 1 + \mu^*(s_{min})\right) = 0$ for the polynomial $h(x)$ from (17).

Note that $h(n-1) = s_{min}(n^m - (n-1)^m) - s_{max}m(n-1)^{m-1} > 0$ iff $\frac{s_{min}}{s_{max}} > \left(\frac{n-1}{n}\right)^{m-1} v_{mn}^{-1}$ and $h(n) = s_{min}\, mn^{m-1} - s_{max}(n^m - (n-1)^m) < 0$ iff $\frac{s_{min}}{s_{max}} < v_{mn}$.

So for $\frac{s_{min}}{s_{max}} \in \left(v_{mn}^{-1}\frac{(n-1)^{m-1}}{n^{m-1}}, v_{mn}\right)$ the Bolzano's theorem implies the existence of $x \in (n-1,n)$ which is a root of $h(t)$, and the corresponding probability $p = x - n + 1 = \mu^*(s_{max})$ of mixed strategy μ^*.

Let $x \in (n-1,n)$. By Lemma 3 we have $q_m(n, n-1, x) > 0$ and $q_m(n-1, n, x) > 0$. The first inequality implies $h(x) > 0$ when $\frac{s_{min}}{s_{max}} < v_{mn}$. The second inequality implies $h(x) < 0$ when $\frac{s_{min}}{s_{max}} < v_{mn}^{-1}\frac{(n-1)^{m-1}}{n}$.

Remark 2. In the case of a two-element set $S = \{s_{min} < s_{max}\}$ the condition that s_{min}/s_{max} belongs to the interval from (12) appeared in both Corollary 1. about pure strategies and in Proposition 3 on mixed strategies. The first is the limit case of the second.

Example 4 ($S = \{s_{min} < s_{max}\}$). Note that the degree of the polynomial $h(x)$ from (17) equals to $m-1$. So for small m one can calculate the equilibrium measure μ^* and the game price u^* explicitly.

In the case of two provers, $m = 2$, for $\frac{s_{min}}{s_{max}} \in \left(\frac{2n-2}{2n-1}, \frac{2n-1}{2n}\right)$:

$$\mu^*(s_{max}) = \frac{(2n-1)s_{min} - (2n-2)s_{max}}{s_{max} - s_{min}}, u^* = \frac{s_{max}s_{min}}{2n(s_{max} - s_{min})}.$$

In the case of three provers, $m = 3$, for $\frac{s_{min}}{s_{max}} \in \left(\frac{3(n-1)^2}{3n^2-3n+1}, \frac{3n^2-3n+1}{3n^2}\right)$:

$$\mu^*(s_{max}) = \frac{(3n-2)s_{min} - (3n-3)s_{max} + \sqrt{D}}{2(s_{max} - s_{min})},$$
$$D = -3n^2 s_{min}^2 + (6n^2 - 6n + 4)s_{min}s_{max} - 3(n-1)^2 s_{max}^2.$$

This expression comes from the largest root of the square polynomial (17) (the smallest root is always outside the interval $(n-1,n)$).

Substitution of $\mu^*(s_{max})$ into (18) yields the game price.

Proposition 4. Suppose that there are two provers $m = 2$ and the set of strategies is $S = \{s_{(0)} > s_{(1)} > \cdots > s_{(k)}\}$.

1. *Denote* $\sigma_l := \sum_{l'=0}^{l} \frac{(-1)^{l'}}{s(l-l')}$ *for* $l = 0,1,\dots,k$; *and for convenience put* $\sigma_{-1} = 0$. *Then* $s_{(l)}$ *are restored as* $1/(\sigma_l + \sigma_{-1})$. *In this case, a one-to-one correspondence is obtained between* $(k+1)$*-tuples* $s_{(0)} > s_{(1)} > \cdots > s_{(k)} > 0$ *and* $(k+1)$*-tuples of* $(\sigma_i)_{0\le i\le k}$ *such that*
$$0 < \sigma_0 < \sigma_2 < \sigma_4 < \cdots, 0 < \sigma_1 < \sigma_3 < \sigma_5 < \cdots. \quad (20)$$
2. *If the symmetric Nash equilibrium is given by a probability measure* μ^* *with supp* $\mu^* = S$, *then the game price and probabilities are*
$$u^* = \frac{a}{2n\sigma_k}, a = 1 + \left(1 + (-1)^k\right)(n-1).$$
$$\mu^*\left(s_{(\ell)}\right) = 2nu^*(\sigma_l - \sigma_{l-1}) - (-1)^\ell(2n-2) = a\frac{\sigma_l - \sigma_{l-1}}{\sigma_k} - (-1)^\ell(2n-2), 0 \le l \le k. \quad (21)$$
3. *Such Nash equilibrium exists iff* $(\sigma_i)_{0\le i\le k}$ *satisfy the inequalities (20) and (22)*
$$a\sigma_l > a\sigma_{l-1} + (-1)^l(2n-2)\sigma_k, 0 \le l \le k, \quad (22)$$
The set of all such $(\sigma_i)_{0\le i\le k}$ *is a nonempty interior of convex* $(k+1)$ *is dimensional polytope.*

Proof. The formula (6) for the game price $u^* = u_1(s_1, \mu^*)$ takes the form

$$\mu^*(s_1) = 2n\frac{u^*}{s_1} - 2n + 2 - 2\mu^*\left(S_{>s_1}\right).$$

Then we prove simultaneously by induction in $l = 0,1, \dots, k$ the formulas for probabilities (21) and

$$\mu^*\left(S_{\geq s_{(l)}}\right) = 2n\sigma_l - (1 + (-1)^l)(n-1).$$

The equation $\mu^*\left(S_{\geq s_{(k)}}\right) = 1$ yields the formula for the game price u^*.

For $(\sigma_l)_{0\leq l\leq k}$ satisfying (20), an above Nash equilibrium exists iff all values of probabilities in (21) are positive, that is equivalent to (22).

Suitable $(\sigma_l)_{0\leq l\leq k}$ can be obtained algorithmically depending on the parity of k: In the case when k is odd, one can select arbitrarily σ_l with odd l satisfying $0 < \sigma_1 < \sigma_3 < \cdots < \sigma_k$ and then select $\sigma_l \in ((2n-2)\sigma_k + \sigma_{l-1}, (2n-2)\sigma_k + \sigma_{l+1})$ for all even l. In the case when k is even, one can select arbitrarily σ_l with even l satisfying $0 < \sigma_0 < \sigma_2 < \cdots < \sigma_k$ and additional condition $\frac{\sigma_0}{\sigma_k} > \frac{2n-2}{2n-1}$ and then select $\sigma_l \in (\sigma_{l-1} - \frac{2n-2}{2n-1}\sigma_k, \sigma_{l+1} - \frac{2n-2}{2n-1}\sigma_k)$ for all odd l.

Proposition 5. *Suppose that there are two provers $m = 2$. Then each symmetric Nash equilibrium is given by a probability measure μ^* with $supp\,\mu^* = S$ on the countable set of strategies is $S = \{s_{(0)} > s_{(1)} > \cdots\}$ [bounded below by a positive constant] is described as follows: Consider an arbitrary sequence $\sigma_{-1} < \sigma_0 < \sigma_1, \dots$, where the subsequence of elements with odd indexes $0 = \sigma_{-1} < \sigma_1 < \sigma_3 < \cdots$ is strongly increasing and bounded and for each even $l \geq 0$*

$$\sigma_l \in \left((2n-2)\lim_{i\to\infty}\sigma_{2i+1} + \sigma_{l-1}, (2n-2)\lim_{i\to\infty}\sigma_{2i+1} + \sigma_{l+1}\right).$$

In this case the subsequence of elements with even indices is strongly increasing $\sigma_0 < \sigma_2 < \cdots$ and $\lim_{i\to\infty}\sigma_{2i} = (2n-1)\lim_{i\to\infty}\sigma_{2i+1}$; the game price is

$$u^* = \frac{1}{2n\lim_{i\to\infty}\sigma_{2i}} = \frac{2n-1}{2n\lim_{i\to\infty}\sigma_{2i+1}}.$$

strategies and probabilities are

$$s_{(\ell)} = \frac{1}{\sigma_l + \sigma_{l-1}}, \mu^*\left(s_{(\ell)}\right) = 2nu^*(\sigma_l - \sigma_{l-1}) - (-1)^\ell(2n-2), \ell = 0,1, \dots$$

Proof. This Proposition can be proved similarly to the previous one.

Example 5. According to the previous proposition, one can select $\sigma_l = \frac{l+1}{l+2}$ for odd $l = -1,1,3, \dots$ and $\sigma_l = 2n - 2 + \frac{\sigma_{l-1}+\sigma_{l+1}}{2} = 2n - 2 + \frac{\ell^2+3\ell+1}{(\ell+1)(\ell+3)}$ for even $\ell = 0,2,4, \cdots$

Then

$$s_{(\ell)} = \begin{cases} \dfrac{1}{2n - \dfrac{2\ell+1}{\ell(\ell+2)}}, \text{if } \ell = 1,3,5, \cdots \\ \dfrac{1}{2n - \dfrac{2\ell+5}{(\ell+1)(\ell+3)}}, \text{if } \ell = 0,2,4, \dots \end{cases}$$

$$\mu(s_{(\ell)}\}) = \begin{cases} \dfrac{1}{\ell(\ell+2)}, \text{if } \ell = 1,3,5, \cdots \\ \dfrac{1}{(\ell+1)(\ell+3)}, \text{if } \ell = 0,2,4, \dots \end{cases} \qquad u^* = \frac{1}{2n}.$$

Note that though the results of this paragraph were obtained under some artificial restrictions on the set of strategies and number of provers, they also help to understand the equilibrium existence for some exotic and extreme cases.

3.6 Measures with Discreet and Continuous Parts

Here we obtain conditions of the Nash equilibrium for the game from Definition 5 in mixed strategies, which are considered as measures with discrete and continuous parts, on suitable sets of strategies.

Proposition 6. *Suppose that* $= \{s_{min}\} \cup [s', s_{max}]$, $s_{min} < s' < s_{max}$ *Then there exists a symmetric Nash equilibrium given by the probability measure* μ^* *absolutely continuous with respect to the Lebesgue measure on* $[s', s_{max}]$ *iff*

$$\frac{s_{min}}{s_{max}} \in \left(\frac{(n-1)^{m-1}}{n^{m-1}}, \frac{m(n-1)^{m-1}}{n^m - (n-1)^m} \right).$$

In this case, the game price u^*, *the discrete part* $\mu^*(s_{min})$ *and the density* $\frac{d\mu^*(s)}{ds}$ *of the measure is given by the formulas*

$$u^* = s_{max} \frac{(n-1)^{m-1}}{n^{m-1}}, \frac{\left(n - \mu^*(s_{min})\right)^{m-1}}{(n-1)^{m-1}} = \frac{s_{max}}{s'}. \tag{23}$$

$$\frac{d\mu^*(s)}{ds} = \frac{n-1}{m-1} \frac{s_{max}^{1/m-1}}{s^{m/m-1}}, s \in [s', s_{max}] \tag{24}$$

Proof. Substitution of s_{max} and s' into the formula for the game price (6) yields (29). Derivation of (7) yields (24).

Substitution of the expression for game price into (6) for $s_1 = s_{min}$ yields

$$h_1(\mu^*(s_{min})) = s_{min} \sum_{k=0}^{m-1} n^k \left(n - \mu^*(s_{min})\right)^{m-k-1} - s_{max} m (n-1)^{m-1} = 0., \tag{25}$$

Note that $h_1(0) \geq 0$ iff $\frac{s_{min}}{s_{max}} \geq \frac{(n-1)^{m-1}}{n^{m-1}}$ and $h_1(0) \leq 0$ iff $\frac{s_{min}}{s_{max}} \leq \frac{m(n-1)^{m-1}}{n^m - (n-1)^m}$. If $\frac{s_{min}}{s_{max}} \in \left[\frac{(n-1)^{m-1}}{n^{m-1}}, \frac{m(n-1)^{m-1}}{n^m - (n-1)^m} \right]$ we have a symmetric Nash equilibrium with $\mu^*(s_{min})$ given by a solution of equation (25).

Proposition 7. *Suppose that supp* $\mu^* = [s_{min}, s'] \cup \{s_{max}\}$, $s_{min} < s' < s_{max}$. *Then there exists symmetric Nash equilibrium given by probability measure* μ^* *absolutely continuous with respect to Lebesgue measure on* $[s_{min}, s']$ *iff*

$$\frac{s_{min}}{s_{max}} \in \left(\frac{(n-1)^{m-1}}{n^{m-1}}, \frac{n^m - (n-1)^m}{mn^{m-1}} \right).$$

In this case, the game price u^*, *the continuous part* $\mu^*([s_{min}, s'])$ *and the density* $\frac{d\mu^*(s)}{ds}$ *of the measure are given by the formulas*

$$u^* = s_{min}, s' \frac{\left(n - \mu^*([s_{min}, s'])\right)^{m-1}}{n^{m-1}} = s_{min}. \tag{26}$$

$$\frac{d\mu^*(s)}{ds} = \frac{n}{m-1} \frac{s_{min}^{1/(m-1)}}{s^{m/(m-1)}}, s \in [s_{min}, s'] \tag{27}$$

Proof. Substitution of s_{min} and s' yields

$$u^* = s_{min} = s' \frac{(n - \mu^*([s_{min}, s',]))^{m-1}}{n^{m-1}}.$$

The formula for density coincides with (14).

Substitution of the expression for game price in (6) for $s_1 = s_{max}$ yields

$$h_2(\mu^*([s_{min}, s',])) = s_{max} \sum_{k=0}^{m-1} (n-1)^k (n - \mu^*([s_{min}, s',]))^{m-1} - s_{min} m n^{m-1} = 0. \quad (28)$$

Note that $h_2(0) \geq 0$ iff $\frac{s_{min}}{s_{max}} \leq \frac{n^m - (n-1)^{m-1}}{m n^{m-1}}$ and $h_2(1) \leq 0$ iff $\frac{s_{min}}{s_{max}} \geq \frac{(n-1)^{m-1}}{n^{m-1}}$. If $\frac{s_{min}}{s_{max}} \in \left[\frac{(n-1)^{m-1}}{n^{m-1}}, \frac{n^m - (n-1)^m}{m n^{m-1}}\right]$ we have symmetric Nash equilibrium with $\mu^*([s_{min}, s',])$ given by the solution of equation (28).

4. Prover Migration Game

Here we are going to study another game describing the behavior of provers when choosing proofs for the next step from different blocks. This game may be considered as some further development and generalization of the game from Definition 5.

Definition 6. One-step game. We have m provers (= players) and k blocks under construction with n_i accessible proof-candidates in ith block for $1 \leq i \leq k$. The strategy of ith prover is the block number $1 \leq s_i \leq k$ he selects for the next step. In this case, the utility is defined as

$$u_i(s_1, \dots, s_m) = \left(1 - \frac{1}{n_{s_i}}\right)^{\#\{1 \leq i' \leq m | i' \neq i \wedge s_{i'} = s_i\}}. \quad (29)$$

Remark 3. The utility given by (29) comes as the price of the game on the interval described by (13).

Proposition 8. *The symmetric Nash equilibrium for the game from Definition 6 is given by the measure*

$$\mu^*(i) = \frac{n_i}{n_1 + n_2 \cdots + n_k}, i = 1,2, \dots, k. \quad (30)$$

Proof. The utility $u_1(s_1, \mu^*, \dots, \mu^*)$ from (1) for (29) is given by the binomial formula

$$\sum_{m'=0}^{m-1} \binom{m-1}{m'} \mu^*(i)^{m'} (1 - \mu^*(s_1))^{m-m'-1} \left(1 - \frac{1}{n_{s_i}}\right)^{m'} = \left(1 - \frac{\mu^*(s_1)}{n_{s_i}}\right)^{m-1}.$$

Then the condition (2) for Nash equilibrium yields (30).

The formula (30) means that the "best" strategy for provers to choose the block is to choose randomly one of the proofs-candidates among all proposed ones from different blocks. After that, proof selection completely defines the corresponding block selection.

5. Conclusions

We described necessary and sufficient conditions of Nash equilibrium existence for two one-step games, which describe provers' behavior in the process of distributed proof generation in sidechains. All results proposed are strictly formulated and proved using game-theoretical apparatus. Though we used rather complicated theoretical constructions, all results obtained are of significant practical value. They are expected to be used when building price policy in Latus Consensus in sidechains.

The direction for our further research, related to Latus Consensus and decentralized proof generation, is an investigation of sidechain functioning as a whole, taking into account both multilevel distributed proof generation in each block and provers' simultaneous work with proofs from few different blocks.

6. Acknowledgments

This work was supported in part by the National Research Foundation of Ukraine under Grant 2020.01/0351.

7. References

[1] Rootstock: smart contracts on bitcoin network, 2018. URL: https://www.rsk.co.
[2] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, P. Wuille, Enabling blockchain innovations with pegged sidechains, 2014. URL: https://blockstream.com/sidechains.pdf.
[3] A. Garoffolo, R. Viglione, Sidechains: Decoupled consensus between chains, 2018. URL: https://arxiv.org/abs/1812.05441.pdf.
[4] A. Kiayias, D. Zindros, Proof-of-work sidechains, Cryptology ePrint Archive, Report 2018/1048, 2018. URL: https://eprint.iacr.org/2018/1048.pdf
[5] A. Garoffolo, D. Kaidalov, R. Oliynykov, Zendoo: a zk-SNARK Verifiable Cross-Chain Transfer Protocol Enabling Decoupled and Decentralized Sidechains. 2020. URL: https://arxiv.org/pdf/2002.01847.pdf
[6] A. Kiayias, A. Russell, B. David, R. Oliynykov, Ouroboros: A provably secure proof-of-stake blockchain protocol, CRYPTO 2017, Part I, volume 10401 of Lecture Notes in Computer Science, Springer, Heidelberg, 2017, pp. 357–388.
[7] J. Garay, A. Kiayias, N. Leonardos, The bitcoin backbone protocol: Analysis and applications, Advances in Cryptology - EURO-CRYPT 2015, Part II, volume 9057 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2015, pp. 281–310.
[8] E. Ben-Sasson, A. Chiesa, E.Trómer, M. Virza, Succinct non-interactive zero knowledge for a von Neumann architecture, Cryptology ePrint Archive, Report 2013/879, 2013. URL: https://eprint.iacr.org/2013/879.pdf
[9] S. Bowe, A.Gabizon. Making Groth's zk-SNARK simulation extractable in the random oracle model, Cryptology ePrint Archive, Report 2018/187, 2018. URL: https://eprint.iacr.org/2018/187.pdf.
[10] Y. Bespalov, A. Garofolo, L. Kovalchuk, H. Nelasa, R.Oliynykov, Models of distributed proof generation for zk-SNARK-based blockchains, Theoretical and Applied Cryptography, Belarusian State University, Minsk, Belarus, 2020, pp. 112–120. URL: http://conf.bsu.by/data/theoreticalandappliedcrypto/doc/TAC_2020_Proceedings.pdf,
[11] R. B. Myerson, Game theory: Analysis of conflict, Harvard University Press, 1997.
[12] N. Ham, Notions of symmetry for finite strategic-form games, 2013. URL: https://arxiv.org/abs/1311.4766.pdf