IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 9, 2019, accepted May 10, 2019, date of publication May 17, 2019, date of current version May 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2917517

Blockchain Token Economics: A Mean-Field-Type Game Perspective

JULIAN BARREIRO-GOMEZ, (Senior Member, IEEE), AND HAMIDOU TEMBINE
Learning and Game Theory Laboratory, New York University at Abu Dhabi, Abu Dhabi, United Arab Emirates

Corresponding author: Hamidou Tembine (tembine@ieee.org)

This work was supported by the U.S. Air Force Office of Scientific Research under Grant FA9550-17-1-0259.

ABSTRACT This paper studies the blockchain cryptographic tokens by means of mean-field-type game theory. It introduces the variance-aware utility function per decision-maker to capture the risk of cryptographic tokens associated with the uncertainties of technology adoption, network security, regulatory legislation, and market volatility. We establish a relationship between the network characteristics, token price, number of token holders, and token supply. Both in-chain diversification and cross-chain diversification among tokens are examined by using a mean-variance approach. The results suggest that the number of tokens in circulation needs to be adjusted in order to capture risk-awareness and self-regulatory behavior in blockchain token economics. The Sharpe and Modigliani ratios for cryptographic tokens are revisited.

INDEX TERMS Blockchain, token, risk, network economics, game theory, mean-field.

I. INTRODUCTION

In basic game theory, a utility function of a decision-maker should capture its preferences and its satisfaction for using an action. The satisfaction drives the demand of the agent, which in turn drives the price together with the supply. Network economics applies a similar principle by including network characteristics. A blockchain is a peer-to-peer network. A blockchain is a distributed cryptographic ledger shared amongst all participating nodes, over which every data or transaction is recorded. The transactions are collected in blocks, which are found in a random process from the protocol. Some blockchains have cryptographic tokens and some others do not. In the context of cryptographic assets, a utility function of an agent would be dependent on the number of tokens in circulation in the blockchain, the demand, which is the aggregated drives of agents or entities, the network characteristics (security, vulnerability, delay), and incentives to verifiers (miners, validators, stakeholders, delegates, enough-token-holders etc). The game-theoretic incentives are key elements (i) for developers to deliver a high quality product, (ii) for users to adopt the platform, (iii) for the verifiers to engage in a desired set of behaviors, (iv) for all to enable a medium of exchange.

The associate editor coordinating the review of this manuscript and approving it for publication was Fatih Emre Boran.

A. RELATED WORKS

Earlier to the cryptographic tokens, token economics [1], [2] had similar issues and obstacles in community settings. These obstacles included identifying procedures to enhance program efficacy, to train staff, to overcome client resistance, to promote long-term maintenance and transfer of training, to the extension of the token economy to institutional settings, to integrate token economies within existing institutional constraints, and the disseminability of the procedures on a large scale. More than four decades later, most of these difficulties on adoption, utility, self-regulation apply to the current cryptographic token-based networks. Blockchain-based startups have embraced initial coin offerings, initial token offerings, pre-sale tokens, initial exchange offering, as a vehicle to raise early capital. The cryptographic tokens offered in these sales are intended to fill a widely large set of roles on different platforms. Moreover, cryptographic tokens pose new challenges in terms of distributed network security and distributed denial of service, which affects token's demand and price. As indicated in [3], designing a successful token must take into account certain aspects of computer science, monetary theory, financial economics, and game theory. The work in [4] examines blockchain economics by means of two approaches: innovation-centric and governance-centric. The authors discussed how the governance approach, based on new institutional economics and public choice economics, can create spontaneous organizations, i.e., new types of

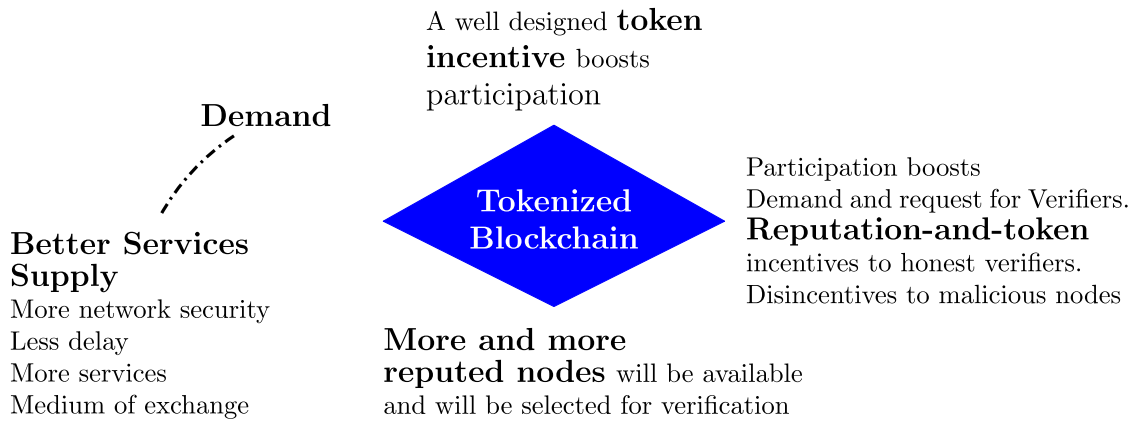

FIGURE 1. Blockchain-based cryptographic token economics examined in this paper.

economies. The authors in [5] examine how value can be created out from blockchain and how tokens, and indeed the entire blockchain economic system, operate as something like a vote of confidence. Blockchain-based cryptographic tokens provide online data and open sources, and hence the evolution of market prices can be analyzed. Based on a set of 143 cryptocurrencies for a sample spanning 2014-2018, the work in [6] shows that, there is no evidence of significant momentum payoffs, supporting the view that the cryptocurrency market is getting more efficient. The work in [7] examines 456 different cryptocurrencies, and show that return predictability diminishes in cryptocurrencies with high market liquidity. The authors in [9] proposed a simulation framework for blocking projects including offers and return on investment. At the time of writing this paper, 2154 cryptographic tokens are displayed at *coinmarketcap.com* and their (reported) prices evolution are available online. For more recent references on blockchain technologies we refer the reader to [10], [11].

B. CONTRIBUTION OF THIS PAPER

This article studies basic game theoretic token incentives in *risk-aware* blockchain technologies. We revisit basic principles of network economics using mean-field-type game theory [54], [57]. We examine risk-aware game-theoretic models that combine risk-awareness, prices, and the security of both the network and the number of active participants. Despite its simplicity, the setting yields insightful implications for the equilibrium relation between the fundamental notions of token economics: the demand and the supply sides of the blockchain-based cryptographic token market. As the variance appears in the payoff functional, one obtains a distribution-dependent payoff. Moreover, the payoff functional of each agent is non-linear with the respect the probability distribution of the state. This leads to a class of variance-aware mean-field-type games, which are games with non-linearly distribution-dependent payoffs. Our contribution can be summarized as follows (see Figure 1):

- Token-less Blockchain economy (Proposition 1): we show that the optimal investment of decision-maker i in the token-free blockchain shares the following interesting features:
  - increases with the total number of active participants to the token-free blockchain.
  - increases with the productivity
  - decreases with the probability of success of an attack of the blockchain by malicious nodes.
- Token-based Blockchain economy (Proposition 2): we show that the optimal number of tokens of a decision-maker has the following interesting features:
  - increases with the total number of active participants in the blockchain.
  - decreases with the probability of success of an attack.
  - decreases with the token price
  - increases with the productivity
  - increases with interest rate of the token price.
- Token adoption (Proposition 3): we provide sufficient conditions under which the token enables and improves the adoption of blockchain technology.
- Token diversification within the chain: We show how to diversity in-chain tokens under correlated prices.
- Token diversification cross-chains: The methodology extends to cross-chain tokens with different access costs.

C. STRUCTURE

The rest of this article is structured as follows. Section II presents a definition of a mathematical definition of a blockchain, and analyzes the token outcomes: adoption, demand, and supply. Section III focuses on token diversification and exchange cross-chain and within the chain.

II. MEAN-FIELD-TYPE GAME-THEORETIC SETUP

A. BLOCKTREE

A blocktree is a 2-tuple $(\mathcal{B}, \mathcal{E})$, where: $\mathcal{B} \subset \mathbb{B}$, is a non-empty set of valid blocks, including at least one element b_0 (the genesis block). Let $\mathcal{E} \subset \mathcal{B}^2$ such that it exists a unique path

TABLE 1. Some consensus algorithms implemented in blockchain: Part I.

Consensus Algorithms	Key Observations
Proof-of-Work [24]–[26]	Blockchain Platform: Bitcoin Programmed in C++ No smart contract Pros: Less opportunity for 51% attack Contras: Greater energy consumption Miners centralization
Proof-of-Stake [27]	Blockchain Platform: Peercoin, Nxt, BlackCoin Programmed in Java with smart contract Pros: Less energy consumption Pros: More decentralized Contras: nothing-at-stake problem double-spend attacks Miners centralization
Delegated Proof-of-Stake [28]	Blockchain Platform: Lisk, Steem, EOS, BitShares. Programmed in JavaScript No smart contract Pros: Less energy consumption Contras: required participation, double-spend attacks partial centralization of miners
Leased Proof-Of-Stake [29]	Blockchain Platform: Waves, Lunes Programmed in Scala with smart contract Pros: Fair usage, Lease coins Contras: decentralization problem
Pure Proof-of-Stake	Blockchain Platform: Vault, algorand Programmed in Testnet with smart contract Pros: scalability Contras: incentives issue

from the initial block b_0 to any other block. A total order $\succ$ over $\mathcal{B}$, preserving $\mathcal{E}$, i.e.

$$(b, b') \in \mathcal{E} \implies b' \succ b.$$

The blockchain is the unique path from the genesis block b_0 to the last block $\max_{\succ} \mathcal{B}$. A blockchain is built by a network of processes applying sequentially the expansion operation starting from the initial blocktree $\{b_0, \{\}\}$. In the distributed case, every processing node refers to its own view of the blocktree and strives to build a consensus with each other on the shared blockchain while increasing its depth. Regular nodes try to build valid blocks. When such valid block is found by a node, it expands its local blocktree from its last block (i.e. the last block of its own view of the blockchain) and broadcasts it to the others. When a regular node receives a new block from another one, it updates its local blocktree expanding it with the new block. During this updating phase, forks may actually be observed due to blocks broadcasting delay. Building a new valid block is an operation that may take many forms depending on the blockchain protocols. Several type of nodes are considered depending on the behaviors: empathy-altruism, regular, spiteful and malicious behaviors. There are several consensus algorithms implemented in the blockchain literature (see Tables 1 and 2 below). As of today, there is no chain-based protocol that outperforms all the others. Each protocol has pros and contras (network performance, end-to-end delay, security, cost) as well as the economic and game theoretic analysis (utility, gain, cost, adoption, medium of exchange) should be taken into consideration. The evolution of the protocols [51] may suggest co-existence and randomization among the class of better protocols. However, the randomization of better protocols will have a different cost and different outcome. Thus, the tradeoffs need to be designed and analyzed.

B. BLOCKCHAIN WITHOUT TOKENS

To proceed, let us consider a basic setup where risk-aware users can conduct businesses and enjoy the exchange surplus on the blockchain platform without holding tokens, but by using a base currency (e.g., dollar, euro, yuan), the numeraire, as a medium of exchange. Let us consider the following risk-aware best-response problem:

$$\begin{aligned} &\sup_{x_i} \mathbb{E}\{w_i(T) - \frac{\eta_i}{2\, w_i(0)} var[w_i(T)]\}, \quad \text{subject to} \\ &dw_i = [\{x_i^{\rho}(h(n)A\lambda_i)^{1-\rho}\}\mathbb{1}_{\{a=0\}} - \xi - x_i r]dt, \\ &dA = A(d_A dt + \sigma_A dB), \\ &A(0) > 0. \end{aligned} \tag{1}$$

where B is a Brownian motion, w_i is the flow of good achieved on the blockchain by transacting in its native cryptographic token by decision-maker i, x_i is the amount in dollar used in decision-maker i, n is the total number of decision-makers that decide to join the blockchain network (i.e., $x_i > 0$,). h is a positive one-to-one mapping. a is a binary random variable representing the state of the attack, $a = 1$ when the

TABLE 2. Some consensus algorithms implemented in blockchain: Part II.

Proof of Elapsed Time [30]	Blockchain Platform: Hyperledger Programmed in Python, C++, Java with smart contract Pros: cheap participation Contras: specialized hardware
Practical Byzantine Fault Tolerance [31]	Blockchain Platform: Hyperledger Programmed in Java with smart contract Pros: no need for confirmation Contras: communication issue Sybil attack
Delegated Byzantine Fault Tolerance [32]	Blockchain Platform: NEO Programmed in Python, Java, C++ with smart contract Pros: scalable, fast Contras: Greater energy consumption Miners centralization
Federated Byzantine Fault Tolerance [33]–[35]	Blockchain Platform: Stellar, Ripple Programmed in Java with smart contract Pros: low latency, scalable Contras: quorum slice choice
Directed Acyclic Graphs [36], [37]	Blockchain Platform: IOTA Programmed in JavaScript, C++ Pros: scalability Contras: double spending issues
Proof-of-Activity [38]	Blockchain Platform: Decred Programmed in Go with smart contract Pros: lower probability of the 51% attack Contras: double signature
Proof-of-Importance [39], [40] Proof-of-devotion (Nebulas) [41]	Blockchain Platform: NEM Programmed in C++, Java with smart contract Pros: partnership Contras: decentralization issue
Proof-of-Capacity [42], [43]	Blockchain Platform: Burstcoin Programmed in Java with smart contract Pros: cheap Contras: decentralization problem
Proof-of-Burn [44]	Blockchain Platform: Slimcoin Programmed in Java no smart contract Pros: cheap Contras: long-term investors Miners centralization
Proof-of-Weight [45]	Blockchain Platform: Filecoin, algorand Programmed in Snark with smart contract Pros: scalability Contras: incentives issue

attack is successful. $A\lambda_i$ is the productivity of i. The initial flow of good is positive $w_i(t_0) > 0$. Here, the interaction with other decision-makers occurs through the term $n(t) = \sum_i \mathbb{1}_{\{x_i(t)>0\}}$. The parameter η_i is a risk-awareness index of decision-maker i. The power parameter for the dollars amount in the dynamics (1) is given by $\rho \in (0, 1)$. The term ξ is the instant access cost, and it can be expressed as a function of waiting cost. An example of such a function was derived in [23] using queueing theory.

$$\xi(d_i) = \xi_0 + \left(\frac{\hat{\lambda}}{\hat{\mu}K}\right)\int_0^{d_i} F'(x)x\frac{D'_K(\frac{\hat{\lambda}(1-F(x))}{\hat{\mu}K})}{\hat{\mu}}dx,$$

Delays are costly to the users and the delay costs per unit time are distributed randomly with cumulative distribution F, where D_K is the expected waiting time measured in blocks of size K, $\hat{\lambda}$ is the arrival rate of request, and $\hat{\mu}$ is the service rate.

Note that, this game problem (1) is not a standard stochastic differential game problem because of the variance term. This is a variance-aware mean-field-type game problem [8], [54], [55], [58].

Proposition 1 (No tokens): The equilibrium strategy of i in the token-less blockchain technology is

$$x_i^* = \left(\frac{\rho}{r}\right)^{\frac{1}{1-\rho}} h(n)\tilde{A}\lambda_i,$$

where $\tilde{A} = A(1-\nu)^{\frac{1}{(1-\rho)}}$, ν *is the probability that an attack (by malicious node or a group of malicious nodes) succeeds under the blockchain protocol.*

The number of participants in the token-free blockchain technology $n_{nto} := \kappa_{nto}\bar{n}$ *solve the following fixed-point equation:*

$$\begin{aligned}\kappa_{nto} &:= \mathbb{P}[\lambda_i \geq \frac{\xi}{h(\kappa_{nto}\bar{n})\tilde{A}}\frac{\rho}{r(1-\rho)}(\frac{r}{\rho})^{\frac{1}{1-\rho}}] \\ &= 1 - F_{\lambda_i}\left[\frac{\xi}{h(\kappa_{nto}\bar{n})\tilde{A}}\frac{\rho}{r(1-\rho)}(\frac{r}{\rho})^{\frac{1}{1-\rho}}\right], \qquad (2)\end{aligned}$$

where F_{λ_i} *is the cumulative function of the productivity random variable.*

To prove this proposition we have used a dynamic programming principle for mean-field-type games. As the drift does not contain the state variable w_i and the reformulation do not have a running payoff, the equilibrium strategies are obtained by one-shot direct optimization for each decision-maker.

Notice that the optimal investment of decision-maker i in the token-free blockchain shares the following interesting features:

- increases with the total number of active participants to the token-free blockchain.
- increases with the productivity $A\lambda_i$ of the token-free blockchain.
- decreases with the probability of success ν of an attack of the blockchain by malicious nodes.

C. REDUCTION OF THE COST OF VERIFICATION

Settlement is the process of transferring an asset or information to another party. Reconciliation ensures that internal records pertaining to a particular transaction are consistent across the relevant parties. Transfers of cryptographic assets through a distributed digital ledger require verification because electronic objects files, unlike physical objects, can be easily duplicated or changed. For this, a blockchain network needs verifiers. In a centralized network, a specific node (a firm or an institution) is entrusted with the responsibility of verification. In exchange, it charges users with fees. In a distributed network, verification tasks are not delegated to a single node but to different members of the network. Trust does not rely on a node, but on the behavior of the network and its protocols. The verifiers contribute resources

that deliver a certain level of trust. A consensus protocol allow participants to agree on a common output that aggregates private inputs when some dishonest (who do not follow the process) participants may attack the process. This question, known as the byzantine agreement, was studied in [12], [13]. The cost of verification of the blockchain will be affected by the used protocol and the economic incentives to the verifiers [20]. If there is a significant reduction of cost of verification of the blockchain compared with the traditional operation, then part of this saving can be used to fund token at the beginning of the blockchain. Below, we examine the effect of tokens on the blockchain economy.

D. BLOCKCHAIN WITH A NATIVE TOKEN

In the current blockchain technology, token economics and legislation are important challenges to be addressed. Before issuing a token, it is important to define the goal, context and objectives of that token. Does it add value to the blockchain project? Does the token price have an economic demand-supply values fit?

Next, we evaluate a native token introduced in the blockchain from a non-zero price $p(0)$ and non-zero production $A(0)$.

$$\begin{aligned}\sup_{u_i} \mathbb{E}w_i(T) - \frac{\eta_i}{2\, w_i(0)} var[w_i(T)], \quad \text{subject to}\\ dw_i &= \{(pu_i)^{\rho}(h(n)A\lambda_i)^{1-\rho}dt + u_i p\mathbb{E}[\frac{dp}{p}]\}\mathbb{1}_{\{a=0\}}\\ &\quad - \xi dt - u_i p r dt,\\ dA &= A(d_A dt + \sigma_A dB_A),\\ A(0) &> 0,\\ dp &= p(d_p dt + \sigma_p dB_p),\\ p(0) &> 0. \end{aligned} \tag{3}$$

Now, n is the total number of decision-makers who decide to join the blockchain network (i.e., $u_i > 0$, to hold some tokens). $u_i p\mathbb{E}[\frac{dp}{p}]$ is the token appreciation and ξ is the access cost. We rename d_p to be $d_p(1-\nu)^{\frac{1}{(1-\rho)}}$. We provide the changes compared with the results of Proposition 1.

Proposition 2 (With tokens): The equilibrium strategy of i is

$$u_i^* = \frac{1}{p}(\frac{\rho}{r-d_p})^{\frac{1}{1-\rho}}[h(n)\tilde{A}\lambda_i],$$

The number of participants in the blockchain with tokens is

$$n_{to} := \kappa_{to}\bar{n},$$

which solves the following fixed-point equation-

$$\begin{aligned}\kappa_{to} &:= \mathbb{P}[\lambda_i \geq \frac{\xi}{h(\kappa_{to}\bar{n})\tilde{A}}\frac{\rho}{(1-\rho)[r-d_p]}(\frac{r-d_p}{\rho})^{\frac{1}{1-\rho}}]\\ &= 1 - F_{\lambda_i}\left[\frac{\xi}{h(\kappa_{to}\bar{n})\tilde{A}}\frac{\rho}{(1-\rho)[r-d_p]}(\frac{r-d_p}{\rho})^{\frac{1}{1-\rho}}\right], \end{aligned} \tag{4}$$

In order to prove this proposition, we have used again dynamic programming principle for mean-field-type games. Only the drift is modified and the new drift does not contain the state variable w_i. There is no running payoff. Thus, the equilibrium strategies are obtained by one-shot direct optimization for each decision-maker.

The optimal number of tokens of decision-maker i has the following interesting features:

- increases with the total number of active participants in the blockchain.
- decreases with the probability of success ν of an attack.
- decreases with the token price p
- increases with the productivity $A\lambda$
- increases with interest rate d_p of the token price

As observed in practice, the network security affects the price, the adoption and the sustainability of blockchain technologies. This simple model captures that behavior.

Proposition 3: If the network security level is identical $\nu_{to} = \nu_{nto} = \nu$, then the following inequality holds:

$$n_{to} > n_{nto}.$$

This means that the introduction of token can boost the adoption and participation to the blockchain technology.

Proof: The proof follows from the monotonicity of F and the fact that $\frac{\rho}{[r-d_p]}(\frac{r-d_p}{\rho})^{\frac{1}{1-\rho}}$ is monotone with d_p. ■

The demand is $D = \frac{1}{p}(\frac{\rho}{r-d_p})^{\frac{1}{1-\rho}}[h(\kappa_{to}\bar{n})\tilde{A}\kappa_{to}\bar{n}]$, and the supply of tokens is S_{to}. Hence, the following formula holds in equilibrium:

$$S_{to} = \frac{1}{p}(\frac{\rho}{r-d_p})^{\frac{1}{1-\rho}}[h(\kappa_{to}\bar{n})\tilde{A}\kappa_{to}\bar{n}]. \tag{5}$$

This determines a token price formula p_{to} of the tokenized blockchain technology as a function of the total population size $\bar{n}$, token user base κ_{to} and the supply of tokens S_{to}.

$$p_{to} = \frac{1}{S_{to}}(\frac{\rho}{r-d_p})^{\frac{1}{1-\rho}}[h(\kappa_{to}\bar{n})\tilde{A}\kappa_{to}\bar{n}]. \tag{6}$$

The velocity [52] of a token is the number of times (frequency) that the token is exchanged from one transaction to another over the period of time $[0, T]$, or in other words, how often token is turned over. The token velocity is a crucial parameter in influencing the value of the token. Based on (6), if the target is a big market size n with a scarce supply S, when the token has high velocity, then there will only be limited value appreciation potential to the token. Token velocity should be taken into consideration in the design of d_p.

Note that, if we modify the utility function by inserting $u_i dp$ instead of $u_i p\mathbb{E}[\frac{dp}{p}]$, the result would be completely different in terms of the nice properties mentioned above. This is because dp will bring the controlled diffusion term $u_i p\sigma_p dB$ which affects the optimization part with a term $\frac{1}{2}[u_i p\sigma_p]^2$. If we use $u_i\mathbb{E}[dp]$ instead of $u_i p\mathbb{E}[\frac{dp}{p}]$, one obtains a function of the ratio $d_p\frac{\mathbb{E}[p]}{p}$ instead of d_p.

Note that when the probability of attack of the tokenized blockchain ν_{to} is big compared with the probability of attack

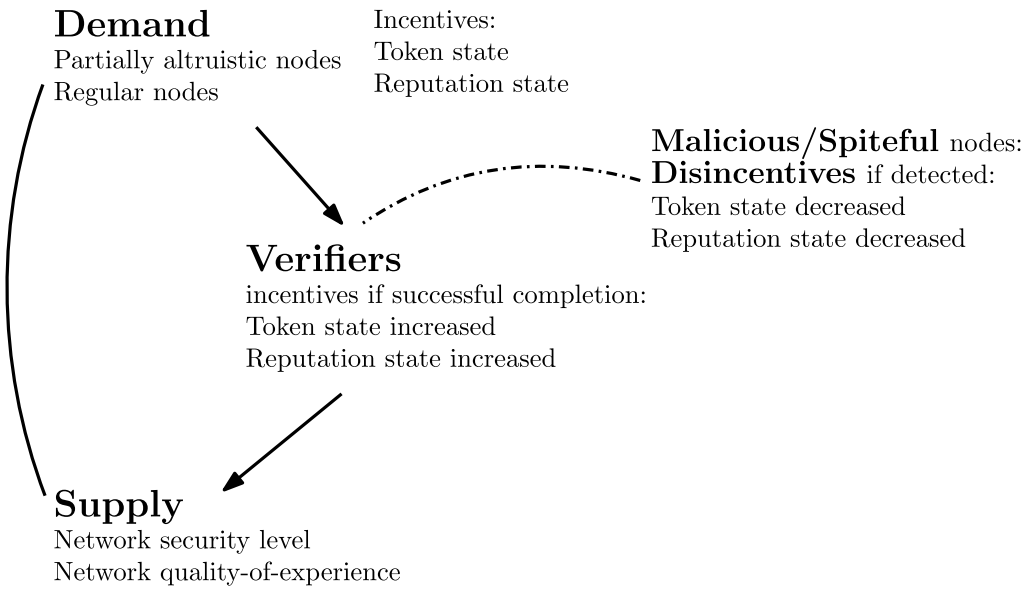

FIGURE 2. Incentives to users and verifiers with token and reputation.

of the token-less blockchain ν_{nto}, the token creates a negative effect and the number of active users will decrease. The ability of the token to create a positive value, to boost adoption or to be a medium of exchange depends the parameters mentioned above.

E. SPECIFIC CRYPTOGRAPHIC TOKEN

We apply the methodology to blockchain-based networks whose consensus algorithms rely on pure PoS and Algorand. The analysis of Bitcoin and PoW can be found in [14]–[19], [21], [22], Ethereum and lighting network incentives [50]. Algorand [46]–[48] is based on the cryptographic sortition mechanism [46], [49] i.e., for every round, it efficiently selects only few verifiers, this is made randomly from the set of all users, and in a way that it is unpredictable until the very last moment. The original protocol of Algorand does not specify an incentive to verifiers. As the temporary verifiers are among the token holders, they may have wanted to protect their own tokens. This makes a lower cost validation procedure if there is enough participation and if the number of regular nodes is high enough. How to get enough participation of honest nodes, to be connected online at any random time?

- Voluntary contributors from token holders and/or those with good reputations (above a certain threshold)
- Community or federation-based contributors who are token holders and with good reputation states
- Incentives for truly decentralized nodes who are token holders and good reputation states.

In order to encourage participation from more than a majority of randomly selected committee members, the nodes who honestly participate get an award (in tokens). If a malicious node is detected, then that node will not be rewarded and disincentive schemes are applied.

1) INCENTIVES FOR VERIFIERS

In order to consolidate the incentives to the verifiers, we propose to add a relatively small award (in token) to the randomly selected verifiers for their service. They consume energy to send and propagate messages whenever active. Thus, the production (supply) is not at free cost. One should consider the cost of delivering (end-to-end delay and timely) such a task. Each verifier will have a specific state depending on their reputation score. The verifier will be its reputation increased after a successful completion of a transaction. A detected malicious behavior will have its reputation state to be decreased if detected. After a certain time step in the evolution of protocol, the number of nodes with high reputation state is big enough. The probability of selection can now combine token and reputation or between two types of tokens as illustrated in Figure 2.

A typical example of committee selection is to choose a proportional probability to

$$[e^{(to_i-\bar{to})}]^{\lambda}[e^{(r_i-\bar{r})}]^{(1-\lambda)}, \text{ or}$$
$$\lambda[e^{(to_i-\bar{to})}]+(1-\lambda)e^{(r_i-\bar{r})},$$

where r_i is the current reputation of i and to_i is the number of tokens that i is holding in the system. If a malicious node is detected, then the user's reputation is set down to zero as well as its token state.

In a single interaction between a set of verifiers and an user, the verifiers have no incentive to provide services to the user. The mechanism we study for creating incentives to provide service involves the exchange of cryptographic tokens. Each agent can hold an arbitrary non-negative number of cryptographic tokens, but cannot hold a negative number of cryptographic tokens and cannot borrow.

The blockchain creates incentives for the verifiers and nodes to provide or share resources, by either providing a supply of tokens or by recommending strategies on their

TABLE 3. Empirical evidence on correlation between some cryptographic tokens in 2018. Symmetric matrix (except the average column). The numbers are computed from the formula $cov(X, Y)$. The source data is available at longhash.com.

2018	Bitcoin	Ethereum	Ripple	BTC Cash	EOS	Stellar	Litecoin	Tron	Cardano	IOTA	Monero	Average
BTC	1	0.815	0.668	0.759	0.687	0.667	0.885	0.556	0.736	0.748	0.829	0.73
ETH		1	0.738	0.753	0.698	0.697	0.827	0.531	0.784	0.780	0.790	0.741
Ripple			1	0.612	0.653	0.728	0.695	0.545	0.772	0.703	0.676	0.679
BTC Cash				1	0.632	0.583	0.746	0.451	0.653	0.720	0.733	0.664
EOS					1	0.610	0.686	0.501	0.711	0.637	0.656	0.647
Stellar						1	0.632	0.414	0.836	0.645	0.675	0.649
LTC							1	0.481	0.714	0.758	0.806	0.718
TRON								1	0.528	0.487	465	0.496
Cardano									1	0.738	0.727	0.721
IOTA										1	0.739	0.696
Monera											1	0.71

reputation. The best response strategies depend on the current token holdings and reputation.

For node i to send information to node k, a fully distributed and random number of nodes are selected to form a committee J. The committee J is selected based specific random process. A strategy profile is a collection $(s_i, s_k, \{s_j\}_{j\in J})$. s_j output maps to acceptance or rejection for j to participate to the vote as a honest node, or to attack or not if a malicious node. If requested service is provided, a portion of tokens is transferred to the committee members and to shared equally. The client's holding of tokens decreases by to_s and each verifier holding of tokens increases by $\frac{1}{|J|}to_s$. Let $\bar{u}$ is the per capita supply of tokens. The distribution of token holdings between verifiers should satisfy the following equalities:

$$\begin{aligned} \sum_{to} \mu(to) &= 1, \\ \sum_{to} to\ \mu(to) &= \bar{u}, \end{aligned} \tag{7}$$

2) ADOPTION-DEPENDENT PRICE

With a pure proof-of-stake the more tokens a user keeps in its accounts, the more chance of being selected at one of the voting rounds. However, its vote counts as one single vote and voter replaceability holds. We change $\tilde{d}_p = d_p + \tilde{\lambda}h(n)$ to capture the dependence of the price on the number nodes participating to the blockchain. Also, the productivity $\tilde{d}_A = d_A + \tilde{\lambda}h(n)$ changed because the random committee is drawn from the population sampling at each round. These changes do affect the above calculations. In particular, the fixed equation (4) is changed. Does a token-rich agent have an incentive to save tokens instead of spending them within the blockchain? There should be an incentive such that the token can enable as a kind of medium of exchange while avoiding rewarding to those who send back and forth.

III. MANAGING TOKENS: DIVERSIFICATION AND EXCHANGE

Once the native token is adopted in the system, one can diversify with several other projects and tokens. We consider two different tokens with price dynamics given by

$$\begin{aligned} dp_1 &= p_1(d_1dt + \sigma_1 dB_1), \\ p_1(0) &> 0, \\ dp_2 &= p_2(d_2dt + \sigma_2 dB_2), \\ p_2(0) &> 0, \end{aligned} \tag{8}$$

where B_1 and B_2 are two Brownian motions (possibly correlated such that $\mathbb{E}[dB_i dB_j] = \beta_{ij}dt$ with $\beta_{ii} = 1$.) Empirical observation from coin-market-cap shows a non-negligible positive correlation of some cryptographic tokens with the major tokens and some others have negative correlation. So correlation between the random variable is reasonable in the crypto networks. Tables 3 and 4 show the correlation between some major cryptographic tokens in 2018 and 2017. Daily prices of Bitcoin and ten other largest cryptocurrencies by market capitalization are used (Ethereum, XRP, Bitcoin Cash, EOS, Stellar, Litecoin, Tron, Cardano, IOTA, and Monero). The entries are obtained using

$$cov(X, Y) := \frac{\mathbb{E}[(X - \mathbb{E}(X))(Y - \mathbb{E}(Y))]}{\sqrt{\mathbb{E}[(X - \mathbb{E}(X))^2]\mathbb{E}[(Y - \mathbb{E}(Y))^2]}}.$$

By stochastic integration formula one gets

$$\begin{aligned} &d[(p_1 - \mathbb{E}p_1)(p_2 - \mathbb{E}p_2)] \\ &\quad = (p_1 - \mathbb{E}p_1)[(p_2 - \mathbb{E}p_2)d_2\ dt + p_2\sigma_2\ dB_2] \\ &\qquad + (p_2 - \mathbb{E}p_2)[(p_1 - \mathbb{E}p_1)d_1 dt + p_1\sigma_1 dB_1] \\ &\qquad + p_2\sigma_2 p_1\sigma_1\beta_{12}dt. \end{aligned} \tag{9}$$

Taking the expectation yields

$$\begin{aligned} d[cov(p_1, p_2)] &= d\mathbb{E}[(p_1 - \mathbb{E}p_1)(p_2 - \mathbb{E}p_2)] \\ &= [d_1 + d_2 + \sigma_1\sigma_2\beta_{12}]cov(p_1, p_2) \\ &\quad -\mathbb{E}[p_1]\mathbb{E}[p_2]\sigma_1\sigma_2\beta_{12}, \end{aligned} \tag{10}$$

By direct computation, one has

$$\mathbb{E}[p_1]\mathbb{E}[p_2] = \mathbb{E}[p_1(0)]\mathbb{E}[p_2(0)]e^{(d_1+d_2)t}.$$

Hence the covariance is

$$\begin{aligned} &cov(p_1, p_2) \\ &\quad = e^{[d_1+d_2+\sigma_1\sigma_2\beta_{12}]t}\ \{cov(p_1(0), p_2(0)) \\ &\qquad -\mathbb{E}[p_1(0)]\mathbb{E}[p_2(0)]\sigma_1\sigma_2\beta_{12}\int_0^t e^{-[\sigma_1\sigma_2\beta_{12}]t'}dt'\Big\} \\ &\quad = e^{[d_1+d_2+\sigma_1\sigma_2\beta_{12}]t}cov(p_1(0), p_2(0)) \\ &\qquad + e^{[d_1+d_2]t}\mathbb{E}[p_1(0)]\mathbb{E}[p_2(0)](e^{\sigma_1\sigma_2\beta_{12}t} - 1) \end{aligned} \tag{11}$$

This means that, even if B_1 and B_2 were uncorrelated, an initial correlation of the token prices will propagate and affect both tokens prices law later on. The total token value is $m = p_1\ u_{i1} + p_2\ u_{i2}$, where u_{ik} is the number of tokens

TABLE 4. Empirical evidence on correlation between some cryptographic tokens in 2018. The numbers are computed from the covariance formula *cov*(*X*, *Y*). The source data is available at longhash.com.

2017	Bitcoin	Ethereum	Ripple	Stellar	Litecoin	Monero	Average
BTC	1	0.355	0.107	0.22	0.369	0.412	0.293
ETH		1	0.111	0.194	0.343	0.461	0.292
Ripple			1	0.474	0.213	0.156	0.212
Stellar				1	0.273	0.356	0.304
Litecoin					1	0.348	0.309
Monero						1	0.346

of type $k \in \{1, 2\}$ held by decision-maker i. The token diversification problem for decision-maker i is the following risk-aware mean-field-type control problem (12) [56]:

$$\begin{aligned}
&\sup_{u_{i1}} \mathbb{E}m(T) - \frac{\eta_i}{2m(0)} var[m(T)], \text{ subject to}\\
&dm = [d_2 m + p_1 u_{i1}(d_1 - d_2)]dt\\
&\qquad + \sigma_1 p_1 u_{i1} dB_1 + \sigma_2 (m - p_1 u_{i1}) dB_2,\\
&m(0) > 0,\\
&0 \le p_1 u_{i1} \le m,
\end{aligned} \tag{12}$$

Note that, the control action u_{i1} is constrained. The correlation between the noises and constraint makes the problem more involved.

Proposition 4 (Diversification between two tokens): The interior (if any) optimal allocation strategy of i is

$$\begin{aligned}
u^*_{i1} &= \frac{1}{p_1}[\tau_i(m - \mathbb{E}m) + \bar{\tau}_i \mathbb{E}m + e_i],\\
u^*_{i2} &= \frac{1}{p_2}[m - \tau_i(m - \mathbb{E}m) - \bar{\tau}_i \mathbb{E}m - e_i],
\end{aligned} \tag{13}$$

with

$$\begin{aligned}
&d[\mathbb{E}m] = [d_2 + \bar{\tau}_i(d_1 - d_2)]\mathbb{E}[m] + e_i(d_1 - d_2)]dt,\\
&\mathbb{E}m(0) > 0,\\
&c\tau_i = (d_1 - d_2) + \sigma_2^2 - \frac{1}{2}\beta_{12}\sigma_1\sigma_2,\\
&c\bar{\tau}_i = [\frac{\bar{\alpha}_i}{\alpha_i}(d_1 - d_2) + \sigma_2^2 - \frac{1}{2}\beta_{12}\sigma_1\sigma_2],\\
&c = \sigma_1^2 + \sigma_2^2 - \beta_{12}\sigma_1\sigma_2,\\
&ce_i = m_0(d_1 - d_2)\frac{\gamma_i}{\alpha_i}.
\end{aligned} \tag{14}$$

Proof: Consider the following problem

$$\begin{aligned}
&\sup_{x_{i1}} \mathbb{E}m(T) - \frac{\eta_i}{2m(0)} var[m(T)], \text{ subject to}\\
&dm = [d_2 m + x_{i1}(d_1 - d_2)]dt\\
&\qquad + \sigma_1 x_{i1} dB_1 + \sigma_2 (m - x_{i1}) dB_2,\\
&m(0) > 0,\\
&0 \le x_{i1} \le m,
\end{aligned} \tag{15}$$

Using the decompositions: $X = (X - \mathbb{E}[X]) + \mathbb{E}[X]$, we rewrite the problem as follows:

$$\begin{aligned}
&\sup_{x_{i1}} \mathbb{E}m(T) - \frac{\eta_i}{2\,m(0)} var[m(T)], \text{ subject to}\\
&d[\mathbb{E}m] = [d_2 \mathbb{E}[m] + \mathbb{E}[x_{i1}](d_1 - d_2)]dt,\\
&\mathbb{E}m(0) > 0,\\
&d(m - \mathbb{E}m)\\
&\quad = [d_2(m - \mathbb{E}m) + (x_{i1} - \mathbb{E}x_{i1})(d_1 - d_2)]dt\\
&\qquad + [\sigma_1(x_{i1} - \mathbb{E}x_{i1}) + \sigma_1 \mathbb{E}x_{i1}]dB_1\\
&\qquad + \sigma_2(m - \mathbb{E}m + \mathbb{E}m - (x_{i1} - \mathbb{E}x_{i1}) - \mathbb{E}x_{i1})dB_2,\\
&\qquad m(0) - \mathbb{E}m(0),\\
&0 \le (x_{i1} - \mathbb{E}x_{i1}) \le (m - \mathbb{E}m),\\
&0 \le \mathbb{E}x_{i1} \le \mathbb{E}m,
\end{aligned} \tag{16}$$

Based on the structure of the terminal mean-variance utility, we consider the following guess functional:

$$f_i = \gamma_i \mathbb{E}m - \frac{\alpha_i}{2m_0}(m - \mathbb{E}m)^2 + \frac{\bar{\alpha}_i}{2m_0}(\mathbb{E}m)^2,$$

where $(\alpha_i, \bar{\alpha}_i, \gamma_i)$ are deterministic functions (of time) to be determined below. It follows that,

$$\begin{aligned}
&\mathbb{E}[R_i - f_i(0)]\\
&= \mathbb{E}[(1 - \gamma_i(T))\mathbb{E}m(T) + \frac{\alpha_i(T) - 1}{2m_0}(m - \mathbb{E}m)^2\\
&\quad - \frac{\bar{\alpha}_i(T)}{2m_0}(\mathbb{E}m)^2]\\
&\quad + \mathbb{E}\int_0^T (\dot{\gamma}_i + d_2\gamma_i)\mathbb{E}[m]\\
&\quad - [\dot{\alpha}_i + 2\alpha_i d_2 + \alpha_i \sigma_2^2]\frac{(m - \mathbb{E}m)^2}{2m_0}dt\\
&\quad - \frac{\alpha_i}{m_0}(d_1 - d_2)(m - \mathbb{E}m)(x_{i1} - \mathbb{E}x_{i1})dt\\
&\quad + 2\frac{\alpha_i}{2m_0}\sigma_2^2(m - \mathbb{E}m)(x_{i1} - \mathbb{E}x_{i1})dt\\
&\quad - \frac{\alpha_i}{2m_0}\beta_{12}\sigma_1\sigma_2(x_{i1} - \mathbb{E}x_{i1})(m - \mathbb{E}m)\\
&\quad - (\sigma_1^2 + \sigma_2^2 - \beta_{12}\sigma_1\sigma_2)\frac{\alpha_i}{2m_0}(x_{i1} - \mathbb{E}x_{i1})^2\\
&\quad + \mathbb{E}[x_{i1}](d_1 - d_2)\gamma_i dt\\
&\quad - \frac{\alpha_i}{2m_0}\beta_{12}\sigma_1\sigma_2[\mathbb{E}x_{i1}]\mathbb{E}m dt\\
&\quad + 2\frac{\alpha_i}{2m_0}\sigma_2^2[\mathbb{E}m]\mathbb{E}x_{i1}dt\\
&\quad + \frac{\bar{\alpha}_i}{m_0}(d_1 - d_2)(\mathbb{E}m)\mathbb{E}[x_{i1}]\\
&\quad - (\sigma_1^2 + \sigma_2^2 - \beta_{12}\sigma_1\sigma_2)\frac{\alpha_i}{2m_0}[\mathbb{E}x_{i1}]^2\,dt\\
&\quad + [\dot{\bar{\alpha}}_i + 2\bar{\alpha}_i d_2 - \alpha_i\sigma_2^2]\frac{(\mathbb{E}m)^2}{2m_0}dt.
\end{aligned} \tag{17}$$

TABLE 5. Sharpe ratio some cryptographic tokens.

2018	Ethereum	Ripple	Litecoin	EOS	Bitcoin Cash	Bifinance coin	Stellar	Tether	Tron	Cardano	Bitcoin Sv	Monero
Sharpe	0.0513	-0.024	0.209	0.1440	0.0725	0.325	0.258	-0.507	-0.132	0.124	0.00921	0.00671
2018	IOTA	Dash	Maker	NEO	Ontology	ETH classic	NEM	Chain	Zcash	Vechain	Waves	Tezos
Sharpe	0.0717	0.0552	0.145	0.0787	0.277	0.00593	0.109	0.342	-0.0322	0.1841	-0.289	0.0117

Assume that

$$m(0) := m_0 > 0, \quad \sigma_1^2 + \sigma_2^2 - \beta_{12}\sigma_1\sigma_2 > 0. \tag{18}$$

It follows that

$$\begin{aligned} x_{i1}(t) &= \tau_i(m(t) - \mathbb{E}m) + \bar{\tau}_i \mathbb{E}m + e_i, \\ c\tau_i &= (d_1 - d_2) + \sigma_2^2 - \frac{1}{2}\beta_{12}\sigma_1\sigma_2, \\ c\bar{\tau}_i &= [\frac{\bar{\alpha}_i}{\alpha_i}(d_1 - d_2) + \sigma_2^2 - \frac{1}{2}\beta_{12}\sigma_1\sigma_2], \\ c &= \sigma_1^2 + \sigma_2^2 - \beta_{12}\sigma_1\sigma_2, \\ ce_i &= m_0(d_1 - d_2)\frac{\gamma_i}{\alpha_i}. \end{aligned} \tag{19}$$

■

The risk-awareness index η_i of decision-maker i plays an important role in the optimal allocation strategy. From the terminal condition: $\alpha_i(T) = \eta_i > 0$. This means that η_i affects significantly the value of $(\bar{\tau}_i, e_i)$ which in turn affects the value of $\mathbb{E}[m]$

A. SHARPE AND MODIGLIANI RATIOS FOR CRYPTOGRAPHIC TOKENS

The Sharpe ratio [59], [60] was developed by Nobel laureate William F. Sharpe and it is used to help investors to understand the return of an investment compared to its risk (Table 5 shows a sample data of the Sharpe ratio from *longhash.com*). The classical Sharpe ratio is the average return earned in excess of the risk-free rate per unit of volatility or total risk. For cryptographic tokens, we do not recommend to use the risk-free model. We instead recommend a risk-reference model because of empirical volatility. We consider two cryptographic token assets with parameters (d_k, σ_k). The parameters $\tau_i, \bar{\tau}_i, e_i$ can be seen as functions of modified Sharpe ratios.

$$\begin{aligned} \tau_i &= \frac{(d_1 - d_2) + \sigma_2^2 - \frac{1}{2}\beta_{12}\sigma_1\sigma_2}{\sigma_1^2 + \sigma_2^2 - \beta_{12}\sigma_1\sigma_2}, \\ \bar{\tau}_i &= \frac{\frac{\bar{\alpha}_i}{\alpha_i}(d_1 - d_2) + \sigma_2^2 - \frac{1}{2}\beta_{12}\sigma_1\sigma_2}{\sigma_1^2 + \sigma_2^2 - \beta_{12}\sigma_1\sigma_2}, \\ e_i &= m_0\frac{\gamma_i}{\alpha_i}\frac{(d_1 - d_2)}{\sigma_1^2 + \sigma_2^2 - \beta_{12}\sigma_1\sigma_2}. \end{aligned}$$

As both cryptographic token prices are volatile, we modify the evaluation criteria. Mimicking Modigliani and Modigliani [61], [62] who proposed a slightly modified ratio, one can consider the ratio

$$M^2 := \mathbb{E}[r_k - r_{ref}]\frac{\sigma_{ref}}{\sigma_{r_k}} + \mathbb{E}[r_{ref}],$$

with r_k being the return on cryptographic token k, σ_{r_k} is the variance on cryptographic token k, r_{ref} is the return on the market reference, and σ_{ref} is the variance on the market reference. It is in units of percentage return, which is instantly interpretable by the crypto users and investors. Note that e_i can be rewritten as

$$e_i = \left(\frac{m_0\frac{\gamma_i}{\sigma_2^2\alpha_i}}{\frac{\sigma_1}{\sigma_2} + \frac{\sigma_2}{\sigma_1} - \beta_{12}}\right)\left((d_1 - d_2)\frac{\sigma_2}{\sigma_1}\right).$$

The last factor $\left((d_1 - d_2)\frac{\sigma_2}{\sigma_1}\right)$ can be seen as $M^2 - \mathbb{E}[r_{ref}]$, therefore it is related to the Modigliani ratio.

B. IN-CHAIN DIVERSIFICATION

Consider two tokens within the same blockchain technology. The network characteristics are similar. In terms of utility function, the token diversification problem between decision-makers is the following risk-aware mean-field-type game problem: [53], [57]:

$$\begin{aligned} &\sup_{u_{i1}} \mathbb{E}w_i(T) - \frac{\eta_i}{2\, w_i(0)} var[w_i(T)], \text{ subject to} \\ dw_i &= \{m^\rho (h(n)A\lambda_i)^{1-\rho}dt + [md_2 + u_{i1}p_1(d_1 - d_2)]dt \\ &\quad + [u_{i1}^\rho + \mathbb{E}u_{i1}^\rho]^{\frac{1}{2}} p_1^{\frac{\rho}{2}}\sigma_1\, dB_1 \\ &\quad + \sigma_2[(m - p_1\, u_{i1})^\rho + \mathbb{E}(m - p_1\, u_{i1})^\rho]^{\frac{1}{2}} dB_2\}\mathbb{1}_{\{a=0\}} \\ &\quad - \xi dt - [mr_2 + u_{i1}p_1(r_1 - r_2)]dt, \\ dm &= [d_2\, m + p_1 u_{i1}(d_1 - d_2)]dt \\ &\quad + \sigma_1\, p_1\, u_{i1} dB_1 + \sigma_2(m - p_1\, u_{i1})dB_2, \\ m(0) &> 0, \\ dA &= A(d_A dt + \sigma_A dB), \\ 0 &\le p_1 u_{i1} \le m, \\ n &= \sum_i \mathbb{1}_{\{u_{i1} > 0\}} + \mathbb{1}_{\{p_1 u_{i1} < m\}}, \end{aligned} \tag{20}$$

In the in-chain procedure, there is a need of token circulation at a later stage. To so do, one can incentivize users for spending tokens. However, sending back and forth between two accounts may be penalized.

C. CROSS-CHAIN DIVERSIFICATION

We now consider cross-chain diversification between two tokens from two different blockchains. The network characteristics: productivity and security level A_k, a_k, ν_k are different. The utility characteristics: $h_k, \lambda_{ik}, \rho_k, \xi_{kk'}, r_k$ are different. Likewise, the number of token adopters n_{to1} and n_{to2} are also different.

$$\begin{aligned} dw_i &= \{(p_1\, u_{i1})^{\rho_1}(h_1(n_{to1})A_1\lambda_{i1})^{1-\rho_1}dt \\ &\quad + u_{i1}p_1\mathbb{E}[\frac{dp_1}{p_1}]\}\mathbb{1}_{\{a_1=0\}} - \xi_{12}dt - u_{i1}p_1\, r_1\, dt \end{aligned}$$

$$+\{(m-p_1\,u_{i1})^{\rho_2}(h_2(n_{to2})A_1\lambda_{i2})^{1-\rho_2}dt$$
$$+(m-u_{i1}p_1)\mathbb{E}[\frac{dp_2}{p_2}]\}\mathbb{1}_{\{a_2=0\}}dt$$
$$-\xi_{21}dt-(m-u_{i1}p_1)r_2dt, \quad (21)$$

D. ARBITRARY NUMBER OF CRYPTOGRAPHIC TOKENS

We consider L different tokens, $L \geq 2$ being arbitrary and $\sum_{i=1}^{L} K_i$ correlated noises. The token dynamics is given by

$$\begin{aligned} dm &= [d_1 m + \sum_{i=2}^{L} p_i u_i (d_i - d_1)]dt \\ &\quad + (m - \sum_{i=2}^{L} p_i u_i) \sum_{j=1}^{K_1} \sigma_{1j} dB_{1j} \\ &\quad + \sum_{i=2}^{L} p_i u_i \sum_{j=1}^{K_i} \sigma_{ij} dB_{ij}, \\ m(0) &= m_0 > 0, \\ 0 &\leq \sum_{i=2}^{L} p_i u_i \leq m, \end{aligned} \quad (22)$$

with the correlation $\mathbb{E}[dB_{ij}dB_{kl}] = \beta_{ijkl}dt$, $\beta_{ijij} = 1$ for any (i, j). The unconstrained constraint problem can be explicitly solved by using the above methodology. However, the problem is constrained by the state m. Thus, a projection into the set $\{u \mid \sum_{i=1}^{L} p_i u_i = m,\ u_i \geq 0\}$, which is a weighted simplex may be required.

IV. CONCLUSION AND FUTURE WORK

In this paper we have studied basic cryptographic token on blockchain using variance-aware mean-field-type games. We have seen that incentives, network security, network delay (via the productivity) affect the behavior of the agents. The incentive proposed here exhibits the following features:

- A well-designed token can incentivize the agents and boost participation (Proposition 3)
- The participation boosts demand and requests for verifiers. Then reputation and token are designed to give incentives to verifiers and to disincentives malicious nodes. The reputation allows to select verifiers who are really known for their good work in the blockchain. They do not necessarily have to have a large amount of native tokens.
- As good works are completed, the quality-of-experience is calculated, and more and more reputed nodes will be available and those reputed agents will be selected for verification and validation.
- This enables better network security, less delay, better supply and a medium of exchange, which in turn enables for demand.

As a future work, it would be interesting to examine incentives for larger medium of exchange and possible extension of this study *beyond blockchains*. The structure of the used network and protocol play important roles in the verification and validation of new information, data or transaction to be added the network. Direct acyclic graph has been proposed as an alternative network. It removes blocks and work directly with Markov Chain Monte Carlo or Poisson Point Process.

REFERENCES

[1] R. C. Winkler, "A theory of equilibrium in token economics," *J. Abnormal Psychol.*, vol. 79, no. 2, pp. 169–173, 1972.
[2] A. E. Kazdin, "The token economy: A decade later," *J. Appl. Behav. Anal.*, vol. 15, no. 3, pp. 431–445, 1982.
[3] J. P. Conley, "Blockchain and the economics of crypto-tokens and initial coin offerings," Dept. Econ. Work. Papers, Vanderbilt Univ., Nashville, TN, USA, Working Paper 17-00008, 2017.
[4] S. Davidson, P. De Filippi, and J. Potts, "Economics of Blockchain," Tech. Rep., Mar. 2016, pp. 1–23. doi: 10.2139/ssrn.2744751.
[5] J. Hargrave, N. Sahdev, and O. Feldmeier, "How value is created in tokenized assets," in *Blockchain Economics: Implications Of Distributed Ledgers-Markets, Communications Networks, And Algorithmic Reality*. Singapore: World Scientific, 2018. doi: 10.2139/ssrn.3146191.
[6] K. Grobys and N. Sapkota, "Cryptocurrencies and momentum," *Econ. Lett.*, vol. 180, pp. 6–10, Jul. 2019.
[7] W. C. Wei, "Liquidity and market efficiency in cryptocurrencies," *Econ. Lett.*, vol. 168, pp. 21–24, Jul. 2018.
[8] T. Başar, B. Djehiche, and H. Tembine, *Mean-Field-Type Game Theory I: Foundations and New Directions*. Springer, to be published.
[9] A. Rasskazova and E. Koroleva, "Investment simulation model for estimating the future value of tokens," in *Proc. 11th Int. Conf. Manage. Large-Scale Syst. Develop. (MLSD)*, Moscow, Russia, 2018, pp. 1–5. doi: 10.1109/MLSD.2018.8551770.
[10] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published. doi: 10.1109/TSMC.2019.2895123.
[11] N. A. Popova and N. G. Butakova, "Research of a possibility of using blockchain technology without tokens to protect banking transactions," in *Proc. IEEE Conf. Russian Young Res. Elect. Electron. Eng. (EIConRus)*, Moscow, Russia, Jan. 2019, pp. 1764–1768. doi: 10.1109/EIConRus.2019.8657279.
[12] M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults," *J. ACM*, vol. 27, no. 2, pp. 228–234, 1980.
[13] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.
[14] M. Rajcaniova, P. Ciaian, and d'A. Kancs, " The economics of BitCoin price formation," *Appl. Econ.*, vol. 48, no. 19, pp. 1799–1815, 2016.
[15] C. Burniske, *Cryptoasset Valuations*. 2017.
[16] T. Peterson, "Metcalfe's law as a model for BitCoin's value," *Alternative Investment Analyst Rev.*, vol. 7, no. 2, pp. 9–18, 2018.
[17] B. Van Vliet, "An alternative model of Metcalfe's Law for valuing BitCoin," *Econ. Lett.*, vol. 165, pp. 70–72, Apr. 2018.
[18] L. W. Cong, Y. Li, and N. Wang, "Tokenomics: Dynamic adoption and valuation," School Bus., Univ. Chicago, Chicago, IL, USA, Working Paper 18-46, 2018.
[19] B. Biais, C. Bisière, M. Bouvard, and C. Casamatta, "The blockchain folk theorem," Toulouse School Econ., Univ. Toulouse Capitole, Toulouse, France, Working Paper 17-817, 2018, pp. 1–71.
[20] C. Catalini and J. S. Gans, "Some simple economics of the blockchain," Nat. Bureau Econ. Res., NBER Working Paper 22952, 2016, pp. 1–29.
[21] Y. Kawase and S. Kasahara, "Transaction-confirmation time for Bitcoin: A queueing analytical approach to blockchain mechanism," in *Proc. Int. Conf. Queueing Theory Netw. Appl.* Cham, Switzerland: Springer, 2017, pp. 75–88.
[22] Q.-L. Li, J.-Y. Ma, and Y.-X. Chang, "Blockchain queueing theory," in *Proc. Int. Conf. Comput. Social Netw., Comput. Data Social Netw. (CSoNet)*, 2018, pp. 25–40.
[23] G. Huberman, J. Leshno C. C. Moallemi, "An economic analysis of the Bitcoin payment system," Tech. Rep., 2019.
[24] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 740. Berlin, Germany: Springer, 1993, pp. 139–147.
[25] M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols (extended abstract)," *Communications and Multimedia Security*. Norwell, MA, USA: Kluwer, 1999, pp. 258–272.

[26] S. Nakamoto, "BitCoin: A peer-to-peer electronic cash system," Bitcoin.org, Tech. Rep., 2008.
[27] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," Peercoin.net, Tech. Rep., 2013.
[28] D. Larimer, "Delegated proof-of-stake," BitShares, Tech. Rep., 2013.
[29] T. B. R. Le Page, T. Tran, and T. Do, "Leased proof-of-stake," White Paper, 2017.
[30] B. Bollen, "Introduce a start for Burrow EVM as sawtooth transaction processor," Github.com, Tech. Rep., 2016.
[31] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Oper. Syst. Design Implement. (OSDI)*. Berkeley, CA, USA: USENIX Association, 1999, pp. 173–186.
[32] (2017). *Delegated Byzantine Fault Tolerant, NEO White Paper*. [Online]. Available: https://docs.neo.org/en-us/whitepaper.html
[33] D. Mazières, "The stellar consensus protocol: A federated model for Internet-level consensus," Stellar Develop. Found., Tech. Rep., 2016.
[34] I. Abraham, G. Chockler, I. Keidar, and D. Malkhi, "Byzantine disk paxos: Optimal resilience with Byzantine shared memory," *Distrib. Comput.*, vol. 185, pp. 387–408, Apr. 2006.
[35] G. Bracha, "Asynchronous Byzantine agreement protocols," *Inf. Comput.*, vol. 752, pp. 130–143, Nov. 1987.
[36] (2017). *The Tangle: Serguei Popov, Version 1.3*. [Online]. Available: http://untangled.world/iota-whitepaper-tangle/
[37] (2017). *IOTA: A Cryptocurrency for Internet-of-Things*. [Online]. Available: https://www.iota.org
[38] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending Bitcoin's proof of work via proof of stake," NetEcon, Tech. Rep., 2014.
[39] J. Risberg, "What is NEM Cryptocurrency?" CoinCentral, Tech. Rep., 2017.
[40] A. Beikverdi, "Proof-of-Importance: How NEM is Going to Add Reputations to the Blockchain," Coin Telegraph, Tech. Rep., 2015.
[41] *Nebulas Technical White Paper, Proof-of-Devotion, The Value-Based Blockchain Operating System and Search Engine*, Apr. 2018.
[42] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Proc. IACR-CRYPTO*, vol. 9216, 2015, pp. 585–605.
[43] G. Ateniese, I. Bonacina, A. Faonio, and N. Galesi, "Proofs of space: When space is of the essence," in *Security and Cryptography for Networks*, vol. 8642. Cham, Switzerland: Springer, 2014, pp. 538–557.
[44] *Slimcoin: A Peer-to-Peer Crypto-Currency With Proof-of-Burn: Mining Without Powerful Hardware*, P4Titan, Tolar, TX, USA, 2014.
[45] Protocol Labs. (2017). *Proof-of-Weight. Filecoin: A Decentralized Storage Network, Filecoin White Paper*. [Online]. Available: https://filecoin.io/filecoin.pdf
[46] S. Micali, "Algorand: The efficient and democratic ledger," Tech. Rep., 2016.
[47] S. Micali, "Very simple and efficient Byzantine agreement," in *Proc. ITCS*, 2017, p. 6.
[48] J. Chen, S. Gorbunov, S. Micali, and G. Vlachos, "ALGORAND AGREEMENT: Super Fast and Partition Resilient Byzantine Agreement," IACR Cryptol. ePrint Arch., Tech. Rep., 2018, p. 377.
[49] S. Micali, M. Rabin, and S. Vadhan, "Verifiable random functions," in *Proc. 40th Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, New York, NY, USA, Oct. 1999, pp. 120–130.
[50] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," Tech. Rep., 2016.
[51] E. Altman, R. El-Azouzi, Y. Hayel, and H. Tembine, "The evolution of transport protocols: An evolutionary game perspective," *Comput. Netw.*, vol. 53, no. 10, pp. 1751–1759 2009.
[52] F. S. Mishkin, *The Economics of Money, Banking and Financial Markets*, 7th ed. Reading, MA, USA: Addison-Wesley, 2004, p. 520.
[53] J. Gao and H. Tembine, "Distributed mean-field-type filters for traffic networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 507–521 Feb. 2019.
[54] T. Duncan and H. Tembine, "Linear–quadratic mean-field-type games: A direct method," *Games*, vol. 9, no. 1, p. 7, 2018.
[55] B. Djehiche, J. Barreiro-Gomez, and H. Tembine, "Price dynamics for electricity in smart grid via mean-field-type games," in *Dynamic Games and Applications*. 2019.
[56] A. Bensoussan, B. Djehiche, H. Tembine, and P. Yam, "Risk-sensitive mean-field-type control," in *Proc. CDC*, 2017, pp. 33–38.
[57] A. Bensoussan, B. Djehiche, H. Tembine, and P. Yam, "Mean-field-type games with jump and regime switching," in *Dynamic Games and Applications*, to be published.
[58] J. Barreiro-Gomez, T. E. Duncan, and H. Tembine, "Linear-quadratic mean-field-type games: Jump-diffusion process with regime switching," *IEEE Trans. Autom. Control*, to be published. doi: 10.1109/TAC.2019.2895295.
[59] W. F. Sharpe, "Mutual fund performance," *J. Bus.*, vol. 39, pp. 119–138, Jan. 1966. doi: 10.1086/294846.
[60] W. F. Sharpe, "The Sharpe ratio," *J. Portfolio Manage.*, vol. 21, no. 1, pp. 49–58, 1994.
[61] F. F. Modigliani and L. Modigliani, "Risk-adjusted performance," *J. Portfolio Manage.*, vol. 23, no. 2, pp. 45–54, 1997.
[62] L. Modigliani, "Yes, You can eat risk-adjusted returns," Morgan Stanley U.S. Investment Res., New York, NY, USA, Tech. Rep. 17, 1997, pp. 1–4.

JULIAN BARREIRO-GOMEZ received the B.S. degree *(cum laude)* in electronics engineering from Universidad Santo Tomás (USTA), Bogotá, Colombia, in 2011, the M.Sc. degree in electrical engineering and the Ph.D. degree in engineering from the Universidad de Los Andes (UAndes), Bogotá, in 2013 and 2017, respectively, and the Ph.D. degree *(cum laude)* in automatic, robotics and computer vision from the Technical University of Catalonia (UPC), Barcelona, Spain, in 2017. He is currently a Postdoctoral Associate with the Learning and Game Theory Laboratory, New York University Abu Dhabi (NYUAD), United Arab Emirates. His main research interests include mean-field-type games, risk-aware engineering, constrained evolutionary game dynamics, distributed optimization, and distributed predictive control. He received the Best Ph.D. Thesis in Control Engineering 2017 Award from the Spanish National Committee of Automatic Control (CEA) and Springer, the EECI Ph.D. Award from the European Embedded Control Institute in recognition to the best Ph.D. thesis in Europe in the field of control for complex and heterogeneous systems, in 2017, and the ISA Transactions Best Paper Award 2018 in Recognition to the best paper published in the previous year.

HAMIDOU TEMBINE received the M.S. degree in applied mathematics from the École Polytechnique, Palaiseau, France, the master's degree in game theory and economics, and the Ph.D. degree in computer science from INRIA and the University of Avignon, France. He has been a Visiting Researcher with the University of California at Berkeley, USA, McGill University, Montreal, QC, Canada, the University of Illinois at Urbana–Champaign (UIUC), USA, the École Polytechnique Fédérale de Lausanne (EPFL), Switzerland, and the University of Wisconsin–Madison, USA. He holds over 150 scientific publications, including magazines, letters, journals, and conferences. He is the author of the book on distributed strategic learning for engineers (published at CRC Press, Taylor & Francis, 2012), which received the Book Award, in 2014, and the coauthor of the book: *Game Theory and Learning for Wireless Networks* (Elsevier Academic Press). His main research interests include learning, evolution, and games. He is a Next Einstein Fellow. He has been a TPC Member and a Reviewer for several international journals and conferences. He received the IEEE ComSoc Outstanding Young Researcher Award for his promising research activities for the benefit of the society, in 2014. He was the recipient of over ten best paper awards in the applications of game theory. He has been a Co-Organizer of several scientific meetings on game theory in networking, wireless communications, and smart energy systems.