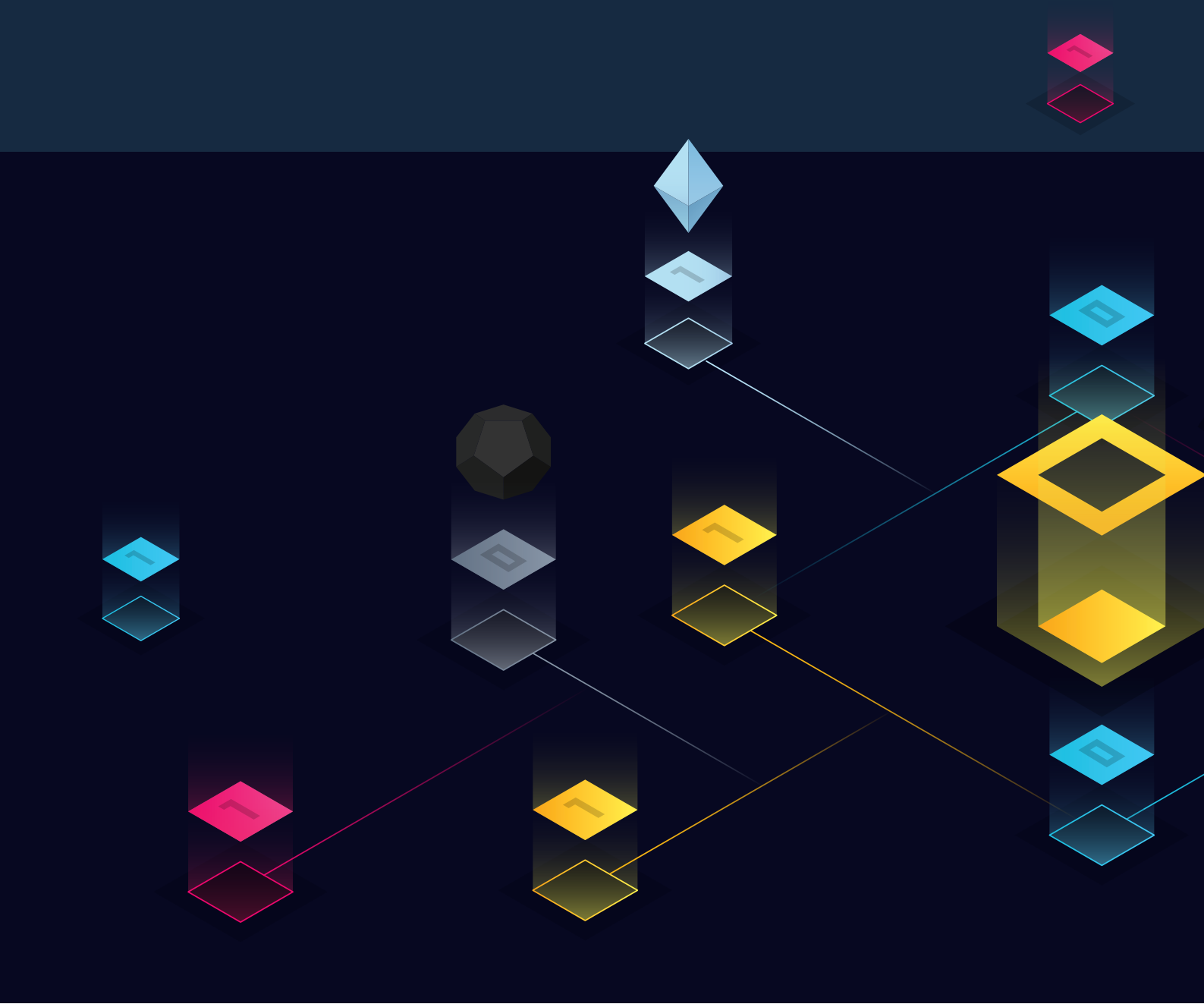
PlatON

A Blockchain-based Infrastructure for Privacy Computation and Distributed Economies

Blue Paper on Economics



Transvaluation of values

Umwertung aller Werte

-Nietzsche

PlatON is a future-oriented infrastructure for privacy computation and distributed economies built on blockchain and cryptographic technologies. The goal of PlatON is to enable and facilitate trades in data usage while protecting data ownership and privacy, thereby eventually establishing a viable market for data and computing power. PlatON, in its capacity as a data and computation marketplace, differentiates from other public blockchains with many added features, which creates new value proposition for its native token and requires unique governance structure.

This *Blue Paper on Economics* provides a comprehensive introduction of PlatON's economic design. It consists of three parts. Part Ⅰ summarizes the principles of economic design of major public blockchains from the perspective of distributed economies. Part Ⅱ describes PlatON's economic design in details, including economic activities within PlatON's public blockchain and those supported by it (i.e. the PlatON market for data and computing power). Part Ⅲ discusses how PlatON's economic design impacts its governance structure.

PlatON

CONTENTS

Part Ⅰ: The Principles of Economic Design of Major Public Blockchains

It is necessary to review designs of existing blockchains and contemplate the principles as we finalize the economic details of PlatON.

Ⅰ. Infrastructure Financing in a Distributed Economy

A distributed economy is an economy where scarce resources are produced and exchanged by the market mechanism rather than central planning and coordination. A distributed economy is autonomous. Its members jointly build and own its infrastructures. Blockchain is one of the most important technologies in a distributed economy.

There are two layers of distributed economic activities associated with a public blockchain: Those within the blockchain (i.e. the 1st layer) and those supported by it (i.e. the 2nd layer).

Participants in the 1st layer mainly include initiators of token transactions, miners[1], and network nodes. Transaction initiators broadcast their transactions onto the peer-to-peer network. Miners package token transactions, produce blocks, and run a consensus algorithm. Network nodes, especially full nodes, synchronize and store the distributed ledger. The efficiency of the 1st layer is manifested in the blockchain's throughput.

The 2nd layer includes decentralized applications (DApps), layer 2 solutions, and decentralized finance (DeFi). Participants in the 2nd layer are more diverse.

In both layers, participants form the division of labor based on their resources and preferences. They trade with each other via the market mechanism.

The most important infrastructure underpinning distributed economies is the distributed ledger, from which the trust in economic activities is derived. If the security and efficiency of the distributed ledger are compromised, distributed economies will be plagued by backlog and delay, or even fall into chaos.

Miners play an indispensable role by maintaining the distributed ledger. They incur costs and take risks in their work. For example, PoW miners need to invest in mining hardware and consume a lot of electricity. PoW mining has become a capital-intensive business. PoS miners need much less capital investment on physical equipment and electricity consumption. This, however, doesn't mean PoS mining is cheap and riskless. PoS miners are usually required to own and lock up tokens in a smart contract (thereafter referred to as "stake tokens"). By doing so, they not only temporarily give up the liquidity of those tokens, but also are vulnerable to price volatility and higher risks in hot wallets.

[1]In many public blockchains, especially those of the PoS type, miners are also referred to as validators. Part Ⅱ also uses "validators" in introducing PlatON's consensus algorithm.

Miners must be adequately compensated for their costs and risks in maintaining the distributed ledger. This is the infrastructure financing problem in the distributed economy.

A common solution is "**usage-based payment**". For example, Bitcoin and Ethereum, by design, limit the number of transactions per second that can be recorded in their distributed ledgers. Initiators of Bitcoin or Ethereum transactions must offer fees to miners to incentivize miners to prioritize their transactions. In terms of economics, they essentially raise transaction fees to bid for limited spaces in the distributed ledgers. That is an important mechanism to generate revenues for miners but at the cost of scalability. EOS adopts a different approach and offers better scalability. EOS miners, when processing EOS transactions and the calling of smart contracts, need to create an operating environment (i.e. RAM) and consume computing power (i.e. CPU). They also need to use network bandwidth (i.e. NET) in synchronizing new blocks with other miners. EOS doesn't have hard-wired limits on RAM, CPU, or NET. EOS holders can obtain those resources with their EOS holdings, rather than through a bidding process. Specifically, they can get CPU and NET by staking EOS or renting from others. They can buy RAM from a special smart contract with EOS.

However, it isn't clear whether "usage-based payment" is a sustainable and effective solution to the infrastructure financing problem. Firstly, the size of transaction fees depends on the activeness of on-chain transactions. Those revenues are therefore unstable and to some extent unpredictable for miners. Secondly, there is no guarantee that transaction fees can cover miners' costs and risks in the long run. In fact, this problem has troubled the Bitcoin community for quite some time. Thirdly, the issue of fairness. Many long-term token holders rarely conduct token transactions and don't pay much to miners. However, the value of their token holdings depends on the security of the distributed ledger. Are they free riding on miners' work?

Block reward is another solution to the infrastructure financing problem. It can solve the problems faced by "usage-based payment", especially in the early development period of public blockchains.

Ⅱ. Token Value, Block Reward, and Inflation Tax

Block reward is different from "usage-based payment" in many aspects. For example, "usage-based payment" redistributes existing tokens from transaction initiators to miners, while block reward means new token issuance. In most literature, the block reward is referred as inflation. However, this is inaccurate.

For fiat money, inflation doesn't mean the growth of the money supply. Rather, inflation means the rise of the general price level, which is measured by the fiat-money-denominated price of a basket of goods and services. There exists a close relationship between money supply and inflation. Milton Friedman, a world-renowned economist and Nobel laureate, once famously pointed out that inflation is always and everywhere a monetary phenomenon. Inflation rises whenever too much fiat money chases a limited amount of goods and services. However, token-denominated economies are still too immature to define a general price index, let alone token-denominated inflation.

To better understand the economic mechanism of the block reward, we must first understand the relationship between token value and token supply.

For most public blockchains, their native tokens have dual functions[2]. Firstly, a payment tool. Tokens are used to settle obligations in blockchain related economic activities. Secondly, tokens represent the right of access to distributed economies. Although some tokens give their holders certain rights in blockchain governance, tokens, in general, don't represent a claim on any asset or future cash flow. This is a key difference between tokens and financial securities such as stocks and bonds. Particularly, tokens don't convey any meaning of ownership, because nobody can own distributed economies.

In addition, token issuance generally follows the rules below: 1. Tokens are not endorsed by any trusted entity or backed by any assets in the real world. 2. Token issuance is solely decided on the supply side and has nothing to do with the demand side. That is to say, people's token demands usually don't impact the amount or speed of token issuance. 3. Token issuance is an algorithm-determined function of time. How active mining is or how much energy mining consumes has little impact on token issuance. Some blockchains limit the total number of token supply (i.e. "hard cap") while others don't (i.e. "soft cap"). If a hard cap exists, new token issuance falls with time.

For tokens with the above features, there is no widely accepted valuation method. Firstly, token value isn't linked to the trustworthiness of any entity or the value of any asset in the real world. Secondly, without any future cash flow, it is impossible to evaluate tokens with mainstream models such as discounted cash flow and no-arbitrage pricing[3]. Finally, since token supply is independent from mining's energy consumption, it is difficult to apply cost-plus pricing. In fact, for PoW-type blockchains, token price determines mining cost through miners' income maximization behaviors, rather than the other way around. Section Ⅲ will further discuss this point.

[2] It should be pointed out that this section's analysis doesn't apply to stable coins, tokenization of off-chain assets, and tokens with "buy back and burn" features (i.e. those issued by some cryptocurrency exchanges).

[3] At any given point of time, token supply in a PoW-type blockchain is pre-specified by its consensus algorithm and has nothing to do with mining's energy consumption. If token price rises, more computing power will be attracted into mining, but token supply won't rise correspondingly. Therefore, token price won't be held back. Since more computing power competes for a given number of new tokens, mining cost will rise. Similarly, if token price falls, there will be less computing power in mining, but token supply won't be reduced. Therefore, token price won't be boosted. With less computing power competing for a given number of tokens, mining cost will fall.

Nevertheless, our study shows that **token value is driven by fundamentals factors in the long run and by liquidity factors in the short run.**

On the one hand, tokens represent the right of access rather than ownership of distributed economies. Using a method similar to the purchasing power parity, we prove that token value is linked to the development of distributed economies. Given other conditions unchanged, the larger distributed economies become, the higher token value is. Intuitively speaking, the right of access to growing distributed economies become more valuable. Token value is linked not only to the aggregate size of the two layers of distributed economic activities but also to the economic coupling relationship between them. Part Ⅲ will discuss this point in greater details.

On the other hand, token price tends to rise when more fiat money chases a given number of tokens, and vice versa. Token price fluctuation caused by liquidity factors is also related to the characteristics of the secondary market for tokens. In particular, if a number of tokens goes out of circulation, such as being staked or used as collateral, the effective token supply will fall, thereby pushing up the token price.

At the moment of new token issuance, it is reasonable to assume that neither fundamental nor liquidity factors change significantly. Under this assumption, the new tokens will dilute the value of existing tokens. This effect is similar to the case when economic fundamentals remain unchanged, the new money supply will dilute the purchasing power of existing money and cause inflation. Similarly, we call the dilution of existing tokens by new token issuance "**inflation tax**". The inflation tax is proportional to the speed of new token issuance. It is shared by existing token holders proportional to the size of their token holdings. Meanwhile, via block reward, inflation tax redistributes wealth from existing token holders to miners. It is interesting to see how this mechanism works without central coordination. By comparison, in a sovereign state, it is the government that collects tax and makes fiscal transfers and redistribution.

Compared with "usage-based payment", the inflation tax offers a more stable source of revenues for miners. Long-term token holders pay miners through their share of inflation tax. The free rider problem is thus greatly alleviated. Although inflation tax redistributes wealth in the short term, long-term interests of both existing token holders and miners are tied together to the rise of token value.

Ⅲ. Basis of Trust, Consensus Algorithm, and Cost of Consensus

Consensus algorithms lie at the heart of public blockchains. They mainly serve two purposes. The first is to reward miners for maintaining the distributed ledger. The second is to assign the book-keeping right of the distributed ledger and protect it from malicious miners. This section will study the basis of trust in consensus algorithms and the cost of consensus.

1.PoW: Technology-based Trust

PoW-type blockchains don't require miners to hold tokens. Miners only need to invest in mining hardware and use electricity. In theory, miners can sell tokens soon after they receive the block reward. Their risk exposures to blockchains mainly result from their mining hardware, whose value depends on token value. Some mining hardware such as GPU is general-purpose. If token price falls, miners can switch GPU to other purposes such as video games, thus limiting their risk exposures. However, if mining hardware is built upon ASIC chips, miners can't switch it to other purposes. Their interests are more aligned with blockchains.

PoW mining is to find a random number, the so-called nonce, that satisfies a cryptographic problem. Currently there exists no better solution to this problem than brute-force search or exhaustive search. The process to find a nonce has nothing to do with miners' off-chain identities or reputation. It only depends on miners' computing power. The more computing power a miner controls, the more likely it finds a nonce earlier than other miners. PoW mining is also memoryless. For the same amount of computing power, its future performance in mining is almost independent of its past performance.

In PoW-type blockchains, miners compete with each other to find a nonce. There is little or no interactive communication or cooperation among them. Whoever finds a nonce first gets the book-keeping right and block reward, while the other miners' work since the previous block becomes worthless. It is a winner-takes-all arrangement. Sometimes, a group of miners form a mining pool to smooth out uncertainties and share profits in mining. However, the relationship among different mining pools is strictly non-cooperative.

PoW mining is open to anyone who can afford mining hardware and electricity. However, this fact, combined with the competition among miners, causes a serious side effect. When token price rises, mining cost rises too. On the one hand, as long as token price makes mining profitable, new computing power will be attracted into mining, which lowers mining profitability until mining becomes just a break-even business. Because more computing power competes for a given number of new tokens, mining cost rises accordingly. On the other hand, whenever a miner invests in mining hardware, it raises its probability of success in mining but lowers that of others. Therefore, its investment generates negative externalities to others. Faced with this situation, other miners have to make more investment too. Miners are trapped in a "prisoner's dilemma" and have to engage in an "arms race" of mining hardware.

In short, PoW represents technology-based trust. With cryptographic technologies, PoW creates a mining environment that doesn't rely on miners' off-chain identities or reputation. However, the "arms race" of mining hardware makes PoW-type blockchains far from energy efficient.

2.PoS: Mechanism-based Trust

PoS-type blockchains require miners to hold tokens. Although PoS miners are subject to much weaker hardware requirements, they have direct risk exposures to blockchains through their token holdings. The size of their risk exposures also depends on whether they need to stake tokens.

Section Ⅰ has pointed out that staking tokens mean temporarily giving up tokens' liquidity, or the right to sell tokens freely according to market conditions. Its cost is positively correlated with how many and how long tokens are staked. Its cost also depends on token holders' liquidity preferences. Long-term token holders have no intention to sell tokens in the near future. They incur little cost in staking tokens. But for ordinary investors, staking tokens when token price is volatile can be very costly. By comparing the cost of staking tokens with the potential reward in participating in consensus algorithms, only token holders with a lower liquidity preference have enough incentive to become PoS miners. Those token holders also have a deeper commitment to blockchains.

In some blockchains, miners don't need to stake tokens. Although mining is more open, the alignment of interests between miners and blockchains become weaker.

In order to improve the efficiency of consensus algorithms, PoS-type blockchains usually use voting mechanisms to choose a small group of miners. Token holders are first assigned a number of votes according to the size of their token holdings. The assignment of votes can be linear, for example, one token one vote, or non-linear such as quadrative voting. Token holders may only vote for themselves or could vote for others with all or a part of their votes. Those receive the most votes are more likely to be chosen as miners. For example, in EOS, one staked EOS can be exchanged for 30 votes, which can then be voted for at most 30 block producer candidates. The 21 candidates receiving the most votes become block producers. Algorand uses a verifiable random function (VRF) to select miners. Each token holder's probability of being selected is proportional to the size of its token holding. The selection of miners is similar to political elections. Different selection mechanisms represent different philosophic considerations and have different implications for blockchain governance.

PoS miners have three notable features. Firstly, when miners need to win other token holders' votes, their off-chain identities and reputation matter a lot. Under this circumstance, miners and their supporters engage in a repeated game. Miners' reputation is built upon past performance, such as their rates of success in producing blocks and their generosity in sharing block reward with supports. Their reputation then determines how many votes they can win in the future. If malicious miners are identified, they can be voted out. Secondly, there is a certain level of cooperation among miners. Once selected, PoS miners don't need to compete with each other to produce blocks. For example, in EOS, block producers take turns to produce blocks. Algorand uses a VRF to choose block proposers. After a candidate block is produced, PoS miners usually run Byzantine agreements to reach consensus. Thirdly, in PoS mining, investment in mining hardware doesn't necessarily lead to higher block reward. Therefore, there will be no "arms race" of mining hardware.

When delegated voting is allowed, staking pools will form around PoS-type blockchains. Ordinary token holders may not have adequate knowledge, time, or hardware to participate in consensus algorithms. By joining forces to support a miner and sharing its block reward, ordinary token holders can earn more profits than on a standalone basis. That's the logic behind staking pools.

To sum up, PoS represents mechanism-based trust. Mechanisms are behavioral rules that incentivize participants in distributed economies to cooperate effectively. In the context of PoS, mechanisms include miners' off-chain identities and reputation, miners' selection procedures, and their cooperation in producing blocks and reaching consensus.

3.Cost of Consensus

Whether PoW or PoS, consensus algorithms aim to ensure that nodes in the peer-to-peer network share the same copy of the distributed ledger in the face of malicious attacks and asynchronous network communication, and without central coordination. To achieve this alignment of the distributed ledger isn't free. We call its cost the **cost of consensus**.

In PoW, the cost of consensus mainly consists of capital expenditure in mining hardware and energy consumption, which we call **the technological cost of consensus**. Section Ⅰ has pointed out that PoW mining has no requirements on miners' off-chain identities or reputation, or cooperation among them. However, the "arms race" of mining hardware and its energy consumption drive up the technological cost of consensus.

PoS's cost of consensus is less explicit and more complicated. The building blocks of PoS are mechanisms. However, many conditions need to be met for mechanisms to function sustainably, effectively, and stable. Firstly, miners and token holders must respond to incentives and constraints embedded in mechanisms. This requires individual rationality. However, irrational or opportunistic behaviors are very common in the real world. That is why off-chain identities and reputation matter so much. Secondly, to improve group interaction and cooperation without central coordination, mechanisms usually include procedural arrangements such as voting schedules and miners' order in producing blocks. Many procedural arrangements have deep backgrounds in game theory.

POS's reliance on off-chain identities and reputation plus procedural arrangements have complicated impacts on its cost of consensus, which we call the **mechanism cost of consensus**.

Firstly, off-chain identities and reputation are built in repeated games and therefore costly. As a matter of fact, the much-rumored activities of bribery in EOS demonstrate the "shadow" cost in building off-chain identities and reputation.

Secondly, off-chain reputation tends to reinforce itself. PoS miners with a better reputation are more likely to be selected again. With more block reward, they have more resources to win supporters and maintain their reputation. As a result, in many PoS-type blockchains, the list of miners become more or less fixed. Some miners even become "permanent". Although in theory consensus algorithms are open to all token holders, in reality, a highly selective group of miners enjoy monopolist power. This tendency of centralization has serious implications for blockchain security.

Thirdly, procedural arrangements in miner selection, block production, and consensus building make collusion easier to be planned and implemented. This will compromise the fairness, effectiveness, and credibility of mechanisms. Besides, if information asymmetry is pervasive, miners and token holders can have hidden information and motivation. Consequently, procedural arrangements may not have their intended effects.

In addition, there are two key differences between technology-based trust and mechanism-based trust. On the one hand, compared with the technological cost of consensus, the mechanism cost of consensus is more implicit and more difficult to be measured accurately. Most people only realize the mechanism cost of consensus when mechanisms fail, or the same mechanisms are transplanted into different environments.

On the other hand, technologies can produce conditional certainties. For example, with current technologies, it is impossible to crack the Elliptic Curve Digital Signature Algorithm (ECDSA) within a meaningful time frame. By comparison, are there any mechanisms that can withstand the test of human nature for a long period of time? We don't believe there are perfect mechanisms either in the real world or in the blockchain field.

In summary,every consensus algorithm relies on a combination of technology-based and mechanism-based trust. It thus incurs technological and mechanism costs of consensus, respectively. **The total cost of consensus is the sum of the technological and mechanism costs**. The more it relies on technology-based trust, the higher its technological cost is, and vice versa. This relationship also applies to mechanism-based trust and the mechanism cost of consensus. Solely relying on technology-based trust, or mechanism-based trust, will result in a very high cost of consensus. We believe there is an optimal combination of technology-based trust and mechanism-based trust, which minimizes the cost of consensus (Figure 1).

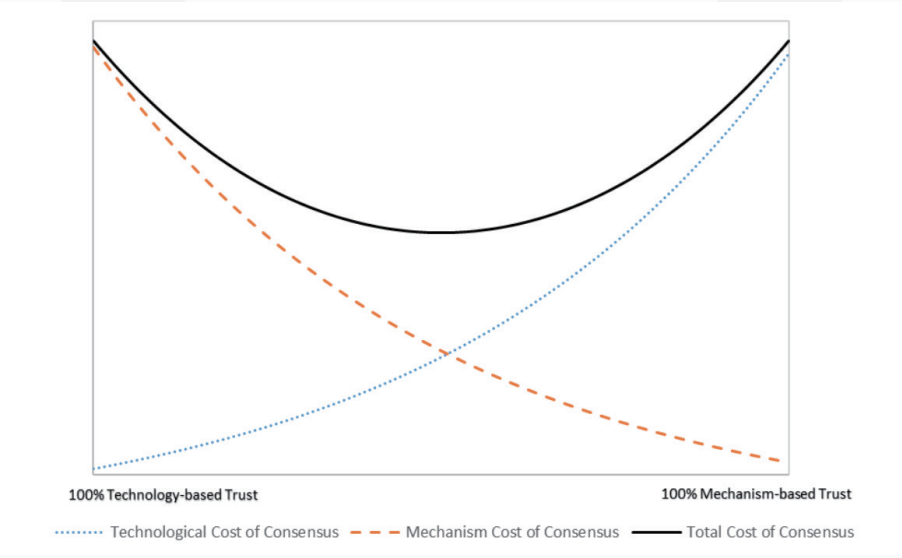


Figure 1: The Cost of Consensus

Part Ⅱ: PlatON's Economic Design

Ⅰ. Major Goals in PlatON's Economic Design

Based on the analysis of Part Ⅰ, we have three major goals in PlatON's economic design.

Goal 1: To lower the cost of consensus as much as possible. Considering PoW's energy consumption and the constraints it faces in the real world, we believe its share in the blockchain field can't grow indefinitely. The PlatON public blockchain is of the PoS-type. We call its consensus algorithm PlatON PoS, or PPoS. Although PPoS uses off-chain identities and reputation plus procedural arrangements, it limits its reliance on them through the introduction of randomness by a VRF. PPoS can effectively prevent collusion and bribery.

Goal 2: To strengthen the economic coupling relationship between the two layers of distributed economic activities. We want the value of Energon, PlatON's native token, to have solid supports.

Goal 3: To endogenously curb the expansion of staking pools around PlatON and ensure the decentralization and security of the PlatON public blockchain.

The following sections will elaborate on the economic design of the two layers of distributed economic activities. Namely, those within the PlatON public blockchain and those supported by it (i.e. the PlatON market for data and computing power).

Ⅱ. Economic Design Inside the PlatON Public Blockchain

1.Initial Allocation and New Issuance of Energon

There is no "hard cap" on the total number of Energon. The initial allocation of Energon is shared among the PlatON founding team, the PlatON foundation, the academic fund, the ecosystem fund, and early investors who participate in the private placement. Participants in the initial allocation are subject to lock-up requirements.

Afterwards, new Energons are issued in each round of PPoS. New Energon issuance is shared according to a pre-specified schedule. The majority of new Energon issuance is given to validators in the form of the block reward. A smaller part of new Energon issuance is given to alternative validators. We refer to their reward as staking reward. The remaining part of new Energon issuance is reserved in a trust fund to reward the PlatON developer community. The trust fund is managed by the PlatON foundation.

Every year, the number of new Energon issuance is a pre-specified portion of the number of Energon supply as of the end of last year. During the first years post the launch of the PlatON main net, the PlatON foundation will use its share of the initial allocation to subsidize validators, alternative validators, and the PlatON developer community. This subsidy will phase out gradually. So, during this period, validators and alternative validators are expected to have a higher income.

2.Three Stages of PPoS

Each round of PPoS consists of 3 stages: First, the election of alternative validators; Second, the selection of validators by the VRF; Third, validators take turns to produce blocks and run a Byzantine agreement, CBFT, to reach consensus. For technical details of PPoS, we will publish the *PlatON Yellow Paper on Consensus*. This section will focus on PPoS' economic problems.

Stage 1: The Election of Alternative Validators

In PlatON, every Energon holder can participate in PPoS.

For an Energon holder who wants to become a validator, it must stake more than a pre-specified minimum number of Energons to first become an alternative validator candidate. One staked Energon means one vote, which must be voted for himself and no one else. In other words, alternative validator candidates aren't allowed to vote for each other.

Other Energon holders who want to participate in the election of alternative validators must stake Energons too. They can stake as many Energons as they wish, also with one staked Energon equaling one vote. They can vote for any alternative validator candidates they choose.

After all the votes are cast, alternative validator candidates are ranked according to how many votes they receive. A pre-specified number of candidates receiving the most votes become alternative validators. The Energons staked by alternative validators and their supporters remain staked until the end of a pre-specified lock-up period. For other candidates and their supporters, their staked Energons can be un-staked immediately after the election. They won't participate in current round of PPoS anymore and won't get any compensation, either.

Stage 2: The Selection of Validators by the VRF

The VRF is used to select a pre-specified number of validators within all the alternative validators. The details of the VRF are very complicated. But it is equivalent to the following experiment.

Firstly, imagine every vote received by each alternative validator as a ball. Mark different alternative validators by different colors, and mix all the balls together. Secondly, randomly draw a ball from the pool, record its color, and put it back. Repeat this step for many times. Thirdly, count the color distribution of the balls drawn from the pool. Those alternative validators corresponding to the colors with the most occurrences become validators.

It can be proved that the more votes an alternative validator receives, the more likely it will be selected by the VRF as a validator. However, the VRF introduces a considerable level of randomness. The validators selected may not correspond to the alternative validators with the most votes.

Stage 3: Validators Run CBFT

In CBFT, every validator is assigned a time window, during which it produces a pre-specified number of blocks consecutively. All the validators then run CBFT to reach consensus on the candidate blocks.

After receiving block reward and staking reward, validators and alternative validators share their income with supporters according to agreements between them. Validators' income also includes transaction fees.

3.Analysis of Economic Design within the PlatON Public Blockchain

Firstly, **a reasonable combination technology-based trust and mechanism-based trust.** Like EOS, the election of alternative validators in PPoS depends on their off-chain identities and reputation. The better reputation an alternative validator candidate has, the more votes it will receive, and the more likely it will be selected by the VRF to be a validator. However, the VRF introduces randomness into the selection of validators. It reduces the reliance on off-chain identities and reputation, and thereby lowers the chance of collusion. If a validator turns out to be malicious, its performance in future elections will be negatively affected. It may even be voted out. That's exactly how off-chain identities and reputation works. In addition, the restriction that alternative validator candidates can't vote for each other helps to curb collusion.

Secondly, **the fairness and openness of the consensus process**. In many PoS-type blockchains, it is feasible to ex ante estimate the probability of becoming a validator given the number of votes a candidate receives. There exist many strategies that help a candidate be elected with a high probability of success. That means it is possible to manipulate the election of validators. Does PPoS also suffer from this problem? We don't think so. It can be proved that the probability for an alternative validator to become a validator depends not only on how many votes it receives, but also on how many votes other alternative validators receive, which is beyond its control. Therefore, the VRF brings many uncontrollable factors and makes the selection of validators unmanipulable.

As will be pointed out below, Energon holders will vote in a balanced manner and avoid concentrating their votes on one or several alternative validator candidates. Consequently, compared with many PoS-type blockchains, the list of validators in PPoS will show greater variability and openness. PPoS will avoid both "tyranny of the majority" and oligarchy.

Thirdly, **endogenously preventing the expansion of staking pools**. Similar to other PoS-type blockchains, staking pools will inevitably form around the PlatON public blockchain. As a mitigating measure, during each round of PPoS, PlatON sets block reward per block to be independent from the number of Energons staked by a validator and its supporters. Essentially, this reflects diseconomies of scale. When electing alternative validators, Energon holders face the following problem: Do they want to support a certain candidate to become an alternative validator first and then a validator with a high probability, but have to share the same reward with more Energon holders?

In this game, the most profitable Energon holders are those who vote for the alternative validators that don't win the most votes but are lucky enough to be selected by the VRF. However, due to the random nature of the VRF, it is hard to predict which alternative validators will have this kind of luck. So, Energon holders have the incentive to diversify their votes. Meanwhile, professional operators of staking pools, constrained by the randomness of the VRF, are less willing to build large staking pools.

Fourthly, **lowering the cost of consensus**. We have compared PlatON with EOS in previous discussion. Now we will compare PlatON with Algorand, a leading public blockchain that also uses a VRF. We believe there are two key differences between PlatON and Algorand.

Algorand uses a VRF to select token holders to participate in its Byzantine agreement, BA★. Token holders are not required to stake tokens. Nor can they vote for each other. The probability of a token holder to be selected by the VRF is proportional to the size of its token holding. Under those arrangements, the alignment of interests between token holders and Algorand is weaker. Token holders with a good off-chain reputation but only owning few tokens have little chance to be selected by the VRF. If we consider the chance to participate in BA★ as power, this power is concentrated among large token holders ("the rich ones"). To the contrary, Energon holders need to stake Energons to participate in PPoS and bind their interests more tightly with PlatON. Any Energon holder, no matter how many Energons it owns, can win votes with its off-chain reputation. With a good enough reputation, a small token holder can become a validator too. In other words, PlatON isn't "ruled by the rich" but is "ruled by the respected".

Algorand uses the VRF at every step of every round of BA★ to independently select a new group of validators. Algorand proves that BA★ can achieve consensus with this feature of player-replaceability. This, of course, is a unique strength of Algorand. Although it makes Algorand more secure, it raises the cost of consensus. Obviously, it is costly to run the VRF among all token holders at every step of every round of BA★. By comparison, in PlatON, once a group of validators are selected by the VRF, they run a full round of CBFT. Considering validators' off-chain reputation, we believe it is unnecessary to replace them in the middle of CBFT. This shows how PlatON uses off-chain identities and reputation to lower the cost of consensus.

Ⅲ. Economic Design of the PlatON Market for Data and Computing Power

1.Overview of the PlatON Market for Data and Computing Power

PlatON is committed to building a high-performing network for computation and facilitating trades in data usage and computing power. With the help of cryptographic technologies such as homomorphic encryption and secure multi-party computation, PlatON can trade in data usage while protecting data privacy.

The PlatON public blockchain is the backbone of the PlatON market for data and computing power. The distribution of computing tasks, the matching between computing tasks and computing power, and the recording of transactions all take place on the PlatON public blockchain. The PlatON public blockchain decouples on-chain consensus from off-chain computing. Key computing work is conducted off-chain. Through verifiable computation, nodes on the PlatON public blockchain can verify transactions without repeating the computing work. Therefore, computation isn't constrained by on-chain resource limits. Trades in data usage and computing power are settled in Energons.

Major participants in the PlatON market for data and computing power include coordinators, data providers, and computing power providers. They are all nodes on the PlatON public blockchain.

Data providers provide input data according to the data format specified by related algorithms but store all input data in their local databases. Nodes participating in PPoS, as the providers of on-chain data, are a special group of data providers.

Coordinators are usually data providers at the same time. After obtaining input data, they first identify suitable providers of computing power. They then package input data and parameters in verifiable computation into multiple sub-tasks. Next, they distribute those sub-tasks to computing power providers. Coordinators ensure computation is conducted in a collaborative and decentralized approach. When distributing computing tasks, they also introduce a certain level of redundancy to enhance fault tolerance.

Computing power providers receive and conduct computing tasks. When a computing power provider joins the PlatON computation network, it automatically evaluates and publishes its computing capacity. After receiving and conducting computing tasks, they use verifiable computation to generate a short proof of the correctness of its computation. They then return both the computation result and the proof to coordinators.

2.Pricing of Computing Power

Compared with trades in data usage, trades in computing power are more standardized or commoditized, verifiable, and measurable. Trades in computing power are also more efficient and transparent. Besides, verifiable computation helps identify malicious or dysfunctional providers of computing power. Therefore, it is possible to objectively evaluate the performance of computing power providers and compensate them accordingly.

It is rather straightforward to price computing power in PlatON. Computing power can be priced based on its energy consumption. The amount of correctly performed computing tasks is recorded in the contribution scores of computing power providers. Those scores represent the reputation of computing power providers in PlatON.

3.Pricing of Data Usage

Trades in data usage are less standardized. Firstly, data are becoming increasingly diverse both in their categories and sources. For example, data covered by PlatON could include information related to people's identities, creditworthy and health records. Data could come from social networks, the Internet of things, and the industrial Internet. Many data are unstructured by nature. Secondly, with the rise of AI, there are increasingly more methods for data analytics. PlatON will support a wide variety of algorithms. Thirdly, the uniqueness of data as a commodity. It is difficult to define and protect data ownership. Data can easily be collected, stored, copied, transferred, and used without appropriate authorization. Data are non-rivalry. The same data can be used repeatedly, which doesn't reduce data's quantity or quality. Data are non-exclusive. Different people can use the same data at the same time. Those unique features of data cause market failure problems in traditional markets for data ownership.

Cryptographic technologies such as homomorphic encryption and secure multi-party computation used by PlatON help enforce data ownership. They make it possible to trade in data usage without exchanging data ownership. In PlatON, trades in data usage follow three principles: 1. Respecting data sovereignty; 2. Orderly trading in data usage while protecting data ownership and privacy; 3. Data users must pay data owners fairly. Therefore, PlatON greatly alleviates market failure problems.

There are two methods to price data usage. The first is absolute pricing. For data users, the value of data is reflected in how data improve their cognitive abilities, decision making, and welfare. The magnitude of improvement determines how much users are willing to pay for data usage. The second is relative pricing. Given a data set and a common task, relative pricing aims to evaluate the contribution of each member of the data set to the common task. Relative pricing can be the basis of absolute pricing. Shapley value is a powerful tool in relative pricing. It is an important concept in cooperative games introduced by Lloyd Shapley, a Nobel Laureate in Economics in 2012, in 1953.

Part Ⅲ: Impacts of PlatON's Economic Design on its Governance Structure

Part Ⅰ has mentioned that token value depends not only on the aggregate size of the two layers of distributed economic activities associated with a blockchain, but also on the economic coupling relationship between them.

Economic coupling is an important yet underappreciated concept in the blockchain field. For example, in many public blockchains that support DApps, DApps can run on their own tokens. On many occasions, DApp users have very low demands for the native tokens of the blockchains. They also rarely engage in transactions in native tokens. This situation can easily cause two problems. Firstly, DApp users don't care much about the development of the blockchains, although the value of their DApp token holdings depend on the security of the blockchains. Secondly, miners of the blockchains provide the security foundation for DApps but are unable to benefit from the development of DApps. Without strong economic coupling, the native tokens of the blockchains couldn't capture values effectively from the 2nd layer of economic activities. There will also be a misalignment of interests between participants of the two layers of economic activities.

We propose two indicators to measure the level of economic coupling. Firstly, to what extent will the 2nd layer of economic activities boost demands for the native tokens? For example, if DApps and Layer 2 solutions have their own tokens, and their users can use those tokens to pay miners, the boost effect will be very weak. If users of DApps and Layer 2 solutions are required to own or even stake the native tokens, the boost effect will be much stronger.

Secondly, to what extent do participants of the two layers of economic activities overlap with each other? For most PoW-type blockchains, there exists a clear division of labor and the two groups of participants rarely overlap. Many PoS-type blockchains have professional operators of staking pools. They have expertise in token custody, community engagement, and supporter relationship management. They may not be active in the DApp level but could be very active in DeFi.

Compared with most public blockchains, PlatON has stronger economic coupling. Firstly, Energons are used to settle trades in the PlatON market for data and computing power. The development of this market will boost demands for Energons and support its value.

Secondly, Participants in the PlatON computation network earn Energons by providing data usage, computing power, and algorithms. As Energon holders, they can also participate in PPoS. Leading participants in the PlatON computation network can accumulate more Energons and therefore have greater influences in PPoS. In other words, participants with more commitment and larger exposures to the PlatON computation network also play a more important role in PPoS. This reflects a deep alignment of interests. It also shows how off-chain identities and reputation can transmit into the blockchain.

We think this arrangement demonstrates the true meaning of "stake" in PoS . Stakeholders are different from shareholders because no one owns the blockchain. Stakeholders have risk exposures to the blockchain. If anything happens to the blockchain or the two layers of distributed economic activities, their interests are directly at stake. Among all stakeholders, validators are the most important ones.

Thirdly, PlatON will support the development of DApps and DeFi and introduce economic coupling designs for DApps and DeFi. For example, DApps on the PlatON public blockchain can issue their own tokens. But DApp tokens must be backed by Energon reserves. The sub-communities of DApps decide the strength of the coupling relationship between DApps tokens and Energon reserves. Once this coupling relationship is agreed upon, it is binding and enforced by smart contracts. If a DApp sub-community wants to issue more tokens, it must put asides more Energon reserves into a smart contract. If it wants to redeem some tokens, the smart contract will refund it with Energons. Therefore, as the DApp develops, its users must acquire more Energons and stake them as reserves. This will help Energon better capture value from the development of DApps and support its value. To encourage this economic coupling relationship, the PlatON foundation will donate a part of initial Energon reserves to DApp sub-communities as their "kick start funding". The stronger the relationship between DApp tokens and Energon reserves chosen by DApp sub-communities, the larger the donation from the PlatON foundation.

PlatON will also support the development of stable coins collateralized by Energon. Some participants in trades in data usage and computing power may prefer to settle obligations in stable coins rather than Energons. PlatON will offer this flexibility. More trades settled in stable coins mean more demands for stable coins, which will lead to more Energons being collateralized. This is another mechanism for Energon to capture value from the development of the PlatON market for data and computing power.

Thus far, this *Blue Paper on Economics* has briefly discussed how PlatON's economic design impacts its governance structure. It has the features of "built by the community, shared by the community, and governed by the community". The *PlatON Red Paper on Governance* will introduce PlatON's governance structure in greater details.

PlatON

platon.network