TOKAMAK NETWORK

Building Protocol for Plasma Blockchain
With Perfect Turing Completeness and High Scalability

Onther PTE. LTD.

March, 2020

Contents

Abstract

Ethereum, created by Vitalik Buterin in 2015, considered blockchain as a state transition system[5] and expanded the areas of blockchain application via smart contracts. However, as the Ethereum network grows, it has reached its performance limit and the burden of increasing data capacity is also growing. These problems have accelerated the emergence of various scalability solutions such as sharding, state channels, and plasma. Ethereum has introduced new features to support such scalability solutions through multiple hard forks; however, it is hard to introduce experimental features in the main chain because the size is increasing and more stakeholders are onboarding.[7].

In 2017, Joseph Poon and Vitalik Buterin proposed Plasma[29] as a framework to handle millions of state transitions per second while enforcing the execution of smart contracts. Based on the research, various implementations were proposed, and such proposals achieved meaningful results in a specific area of blockchain application known as "state transition system for tokens(ERC20, ERC721)". However, as was the case with the early blockchain, most plasma implementations are used only as a "turing-incomplete state transition system".

Tokamak Network aims to provide a protocol allowing easy deployment of diverse turing-complete plasma chains. Tokamak Network sets the "correct state transition" criterion in the plasma chain by separately defining the rules for changing the "arbitrary state" in the root chain. It expands the use of plasma chain as general state transition system(layer2). Therefore, Tokamak Network will not only resolve the scalability problems of decentralized applications (DApps) in Ethereum, but also provide an environment that can allow easy deployment of applications that was not implemented in the past due to Ethereum's performance and functional limitations.

Disclaimer

This whitepaper and other documents distributed in relation hereto are used for the development and application of the Tokamak Network, and the material contained herein is for informational purposes only and may change in the future.

Accordingly, please read this entire section carefully. If you are in any doubt as to the action you should take, please consult your legal, financial, tax or other professional advisor(s).

1.1 Legal Statement

(a) This Whitepaper ("Whitepaper"), in its current form, is circulated for general information purposes only in relation to the protocol and applications described in the Whitepaper ("Protocol") as presently conceived and is subject to review and revision. Please note that this Whitepaper is a work in progress and the information in this Whitepaper is current only as of the date on the cover hereof. Thereafter, the information, including information concerning Onther Pte Ltd's (the "Company") intentions, business operations and financial condition (if applicable) may have changed. We reserve the right to change, modify, add or delete parts of this Whitepaper or website without notice for any reason or at any time.

(b) No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of the tokens native to the Protocol ("TON Token" or "Token") (as defined below) and no payment is to be accepted on the basis of this Whitepaper. Any sale and purchase of the Token will be governed by a legally binding agreement, the details of which will be made available separately from this Whitepaper. In the event of any inconsistencies between the abovementioned agreement and this Whitepaper, the former shall prevail.

(c) This Whitepaper does not constitute or form part of any opinion on any advice to sell, or any solicitation of any offer by the issuer/distributor/vendor of the Token to purchase any Token nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision.

(d) The Tokens are not intended to constitute securities, units in a business trust, or units in a collective investment scheme, each as defined under the Securities and Futures Act (Cap. 289) of Singapore, or its equivalent in any other jurisdiction. Accordingly, this Whitepaper therefore, does not, and is not intended to, constitute a prospectus, profile statement, or offer document of any sort, and should not be construed as an offer of securities of any form, units in a business trust, units in a collective investment scheme or any other form of investment, or a solicitation for any form of

investment in any jurisdiction.

(e) No Token should be construed, interpreted, classified or treated as enabling, or according any opportunity to, purchasers to participate in or receive profits, income, or other payments or returns arising from or in connection with the Protocol or the Token, or to receive sums paid out of such profits, income, or other payments or returns.

(f) This Whitepaper or any part hereof may not be reproduced, distributed or otherwise disseminated in any jurisdiction where the offer/distribution of digital tokens in the manner set out this Whitepaper is regulated or prohibited. Receipt of the Whitepaper does not guarantee or indicate any eligibility or guarantee of participation in the project described in the Whitepaper.

(g) No regulatory authority has reviewed, examined or approved of any of the information set out in this Whitepaper. No such action has been or will be taken in any jurisdiction.

(h) This Whitepaper contains the perspective and view of the Company which does not reflect the policies or positions of public authorities such as governments, quasi-governments, authorities or regulators in any jurisdiction. The information contained in the Whitepaper is based on information obtained from reliable sources, and the Company does not guarantee its accuracy or completeness.

(i) References to specific companies and platforms in the Whitepaper are for general reference and/or comparison purposes only. The use of the name of the enterprise or platforms and registered trademarks does not signify affiliation or endorsement of the party concerned.

(j) Where you wish to or have purchased any Token, the Tokens are not to be construed, interpreted, classified or treated as: (a) any kind of currency other than cryptocurrency; (b) debentures, stocks or shares issued by any entity; (c) rights, options or derivatives in respect of such debentures, stocks or shares; (d) rights under a contract for differences or under any other contract with the purpose or pretended purpose to secure a profit or avoid a loss; or (e) units or derivatives in a collective investment scheme or business trust, or any other type of securities.

1.2 Restrictions on Distribution and Dissemination

(a) The distribution or dissemination of this Whitepaper or any part thereof may be prohibited or restricted by the laws or regulatory requirements of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, to obtain legal and other relevant advice on, and to observe, any restrictions which are applicable to your possession of this Whitepaper or such part thereof (as the case may be) at your own expense and without liability to the Company or its representatives, agents, and related companies ("Affiliates").

(b) Persons to whom a copy of this Whitepaper has been distributed or disseminated, provided access to or who otherwise have the Whitepaper in their possession shall not circulate it to any other persons, reproduce or otherwise distribute this Whitepaper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

1.3 Disclaimer of Liability

(a) The Token, the Protocol and related services provided by the Company and its affiliates are provided on an "as is" and "as available" basis. The Company and its Affiliates do not grant any warranties or make any representation, express or implied or otherwise, as to the accessibility, quality, suitability, accuracy, adequacy, or completeness of the Token, the Protocol or any related services provided by the Company and its Affiliates, and expressly disclaim any liability for errors, delays, or omissions in, or for any action taken in reliance on, the Token, the Protocol and related services provided by the Company and its Affiliates.

(b) The Company, its Affiliates and its directors, officials and employees do not make or purport to make, and hereby disclaim, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in this Whitepaper.

(c) To the maximum extent permitted by the applicable laws and regulations, the Company and its Affiliates shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this Whitepaper or any part thereof by you.

1.4 Cautionary Note on Forward-Looking Statements

(a) Certain information set forth in this Whitepaper includes forward-looking information regarding the future of the project, future events and projections. These statements are not statements of historical fact and may be identified by but not limited to words and phrases such as "will", "estimate", "believe", "expect", project", "anticipate", or words of similar meaning. Such forward-looking statements are also included in other publicly available materials such as presentations, interviews, videos etc., information contained in this Whitepaper constitutes forward-looking statements including but not limited to future results, performance, or achievements of the Company or its Affiliates.

(b) The forward-looking statements involve a variety of risks and uncertainties. These statements are not guarantees of future performance and no undue reliance should be placed on them. Should any of these risks or uncertainties materialize, the actual performance and progress of the Company or its Affiliates might differ from expectations set by the forward-looking statements. The Company or its Affiliates undertake no obligation to update forward-looking statements should there be any change in circumstances. By acting upon forward-looking information received from this Whitepaper, the Company or its Affiliates' website and other materials produced by the Company or its Affiliates, you personally bear full responsibility in the event where the forward-looking statements do not materialize.

(c) As of the date of this Whitepaper, the Protocol has not been completed and is not fully operational. Any description pertaining to and regarding the Protocol is made on the basis that the Protocol will be completed and be fully operational. However, this paragraph shall in no way

be construed as providing any form of guarantee or assurance that the Protocol will eventually be completed or be fully operational.

1.5 Potential Risks

By purchasing, holding and using the Tokens, you expressly acknowledge and assume the risks set out in this section if any of these risks and uncertainties develops into actual events, the business, financial condition, results of operations and prospects of the Company or its Affiliates may be materially and adversely affected. In such cases, you may lose all or part of the value of the Token. Such risks include but are not limited to the following:

https://www.overleaf.com/project/5e4f057d8d12ae00017ba788

Risks Relating to the Tokens

(a) There may not be a public or secondary market available for the Tokens

I. The Tokens are intended to be native tokens to be used on the Protocol, and the Company and its Affiliates have not and may not actively facilitate any secondary trading or external trading of Tokens. In addition, there is and has been no public market for the Tokens and the Tokens are not traded, whether on any cryptocurrency exchange or otherwise. In the event that the Tokens are traded on a cryptocurrency exchange, there is no assurance that an active or liquid trading market for the Tokens will develop or if developed, be sustained. There is also no assurance that the market price of the Tokens will not decline below the purchase amount paid for the Tokens, which is not indicative of such market price.

II. A TON Token is not a currency issued by any central bank or national, supra-national or quasi-national organisation, nor is it backed by any hard assets or other credit. The Company and its Affiliates are not responsible for nor do they pursue the circulation and trading of the Tokens on the market. Trading of the Tokens merely depends on the consensus on its value between the relevant market participants, and no one is obliged to acquire any Token from any holder of the Token, including the purchasers of the Tokens, nor does anyone guarantee the liquidity or market price of the Tokens to any extent at any time. Accordingly, the Company and its Affiliates cannot ensure that there will be any demand or market for the Tokens, or that the price upon which the Tokens were purchased is indicative of the market price of the Tokens if they are made available for trading on a cryptocurrency exchange.

Risks Relating to the Company, its Affiliates and the Protocol

(a) Limited availability of sufficient information

The Protocol is still at an early development phase as of the date of this Whitepaper. Its governance structure, purpose, consensus mechanism, algorithm, code, infrastructure design and other technical specifications and parameters may be updated and changed frequently without notice. While this

Whitepaper contains the key information currently available in relation to the Protocol, it is subject to adjustments and updates from time to time, as announced on the Company's website at Tokamak Network Official Twitter. Users of the Protocol will not have full access to all the information relevant to the Tokens and/or the Protocol. Nevertheless, it is anticipated that significant milestones and progress reports will be announced on the Company's website at Tokamak Network Official Twitter.

(b) The digital assets raised in the sale of the Tokens are exposed to the risks of theft.

Whilst the Company and its Affiliates will make every effort to ensure that any cryptocurrencies received from the sale of Tokens are securely held through the implementation of security measures, there is no assurance that there will be no theft of the cryptocurrencies as a result of hacks, mining attacks, sophisticated cyber-attacks, distributed denials of service or errors, vulnerabilities or defects on such blockchain addresses, or any other blockchain, or otherwise. Such events may include, for example, flaws in programming or source code leading to exploitation or abuse thereof. In such event, even if the sale of Tokens is completed, the Company and its Affiliates may not be able to receive the cryptocurrencies raised and the Company and its Affiliates may not be able to utilize such funds for the development of the Protocol, and the launch of the Protocol might be temporarily or permanently curtailed. As such, the issued Tokens may hold little worth or value. The Tokens are uninsured, unless you specifically obtain private insurance to insure them. In the event of any loss or loss of value of the Tokens, you may have no recourse.

(c) The blockchain address(es) may be compromised and the digital assets may not be able to be retrieved.

Blockchain address(es) are designed to be secured. However, in the event that the blockchain address(es) for the receipt of purchase amounts or otherwise are, for any reason, compromised (including but not limited to scenarios of the loss of keys to such blockchain address(es), the funds held at such blockchain address(es) may not be able to be retrieved and disbursed, and may be permanently unrecoverable. In such event, even if the sale of the Tokens is successful, the Company and its Affiliates will not be able to receive the funds raised and the Company and its Affiliates will not be able to utilize such funds for the development of the Protocol, and the implementation of the Protocol might be temporarily or permanently curtailed. As such, distributed Tokens may hold little worth or value.

(d) There is no assurance of any success of the Protocol and the Company and its Affiliates may cease the development, launch and operation of the Protocol.

I. The value of, and demand for, the Tokens hinges heavily on the performance of the Protocol. There is no assurance that the Protocol will gain traction after its launch and achieve any commercial success. The Protocol has not been fully developed, finalized and integrated and is subject to further changes, updates and adjustments prior to its launch. Such changes may result in unexpected and

unforeseen effects on its projected appeal to users, and hence impact its success. There are no guarantees that the process for creating the Tokens will be uninterrupted or error-free.

II. While the Company has made every effort to provide a realistic estimate, there is also no assurance that the any cryptocurrencies raised in the sale of Tokens will be sufficient for the development and integration of the Protocol. For the foregoing or any other reason, the development and integration of the Protocol may not be completed and there is no assurance that its systems, protocols or products will be launched at all. As such, distributed Tokens may hold little or no worth or value.

III. Additional reasons which may result in the termination of the development, launch or operation of the Protocol includes, but is not limited to, (aa) an unfavorable fluctuation in the value of cryptographic and fiat currencies, (bb) the inability of the Company and its Affiliates to establish the Protocol or the Tokens' utility or to resolve technical problems and issues faced in relation to the development or operation of the Protocol or the Token, the failure of commercial relationships, (cc) intellectual property disputes during development or operation, and (dd) changes in the future capital needs of the Company or its Affiliates and the availability of financing and capital to fund such needs. For the aforesaid and other reasons, the Protocol may no longer be a viable project and may be dissolved or not launched, negatively impacting the Protocol and the potential utility and value of issued TON Tokens.

(e) There may be lack of demand for the Protocol and the services provided, which would impact the value of the Tokens.

I. There is a risk that upon launching of the Protocol, there is a lack of interest from consumers, merchants, advertisers, and other key participants for the Protocol and the services, and that there may be limited interest and therefore use of the Protocol and the Tokens. Such a lack of interest could impact the operation of the Protocol and the uses or potential value of the Tokens.

II. There is a risk of competition from alternative platforms/protocols that may have been established, or even from existing businesses which would target any segment of the potential users of the Protocol fulfilling similar demands, e.g. corporations targeting advertisers seeking purchase consumer data and market analysis. Therefore, in the event that the competition results in a lack of interest and demand for the Protocol, the services and the Tokens, the operation of the Protocol and Token value may be negatively impacted. r specialist as necessary before deciding whether to purchase TON tokens or participate in the Tokamak Network project.

(f) The Company and its Affiliates may experience system failures, unplanned interruptions in its network or services, hardware or software defects, security breaches or other causes that could adversely affect the Company or its Affiliates' infrastructure network, or the Protocol.

I. The Company and its Affiliates are unable to anticipate or detect when there would be occurrences of hacks, cyber-attacks, mining attacks (including but not limited to double-spend attacks,

majority mining power attacks and "selfish-mining" attacks), distributed denials of service or errors, vulnerabilities or defects in the Protocol, the Tokens, or any technology (including but not limited to smart contract technology) on which the Company, its Affiliates, the Protocol, the Tokens, rely on or the Ethereum Blockchain or any other blockchain. Such events may include, for example, flaws in programming or source code leading to exploitation or abuse thereof. The Company and its Affiliates may not be able to detect such issues in a timely manner, and may not have sufficient resources to efficiently cope with multiple service incidents happening simultaneously or in rapid succession.

II. Although the Company and its Affiliates will be taking steps against malicious attacks on its appliances or its infrastructure, which are critical for the maintenance of the Protocol and its other services, there can be no assurance that cyber-attacks, such as distributed denials of service, will not be attempted in the future, and that any of such security measures will be effective. Any significant breach of security measures or other disruptions resulting in a compromise of the usability, stability and security of the Company and its Affiliates' network or services, including the Protocol.

Risks Relating to the Participation in the Sale of Tokens

(a) You may not be able to recover the purchase amount paid for the Tokens.

Except as provided under any applicable terms of sale or prescribed by applicable laws and regulations, the Company is not obliged to provide you with a refund of any purchase amount. No promises of future performance or price are or will be made in respect to the Tokens, including promises of inherent value or continuing payments, and there is no guarantee that the Tokens will hold any particular value. Therefore, the recovery of the purchase amount may be impossible or may be subject to applicable laws and regulations.

(b) You may be subject to adverse legal and/or tax implications as a result of the purchase, distribution and use of the Tokens.

I. The legal character of cryptocurrency and cryptographic assets remain uncertain. There is a risk that the Tokens may be considered securities in certain jurisdictions, or may be considered to be securities in certain jurisdictions in the future. The Company and its Affiliates does not provide any warranty or guarantee as to how the Tokens will be classified, and each purchaser will bear all consequences of the Tokens being considered securities in their respective jurisdictions, and bear the responsibility of the legality, use and transfer of the Tokens in the relevant jurisdictions.

II. Further, the tax treatment of the acquisition or disposal of such cryptocurrency or cryptographic assets might depend on whether they are classified as securities, assets, currency or otherwise. As the tax characterization of the Tokens remains indeterminate, you must seek your own tax advice in connection with the purchase, acquisition or disposal of the Tokens, which may result in adverse tax consequences or tax reporting requirements for you.

(c) The loss or compromise of information relating to the purchaser wallet and your method of accessing the Protocol may affect your access to and possession of the Tokens.

There is a risk that you may lose access to and possession of the Tokens permanently due to loss of unique personal ID used to access the Protocol, and other identification information, loss of requisite private key(s) associated with the purchaser wallet or vault storing the Tokens or any other kind of custodial or purchaser errors.

(d) Blockchains may face congestion and transactions may be delayed or lost.

Most blockchains used for cryptocurrency transactions (e.g. Ethereum) are prone to periodic congestion during which transactions can be delayed or lost. Individuals may also intentionally spam the network in an attempt to gain an advantage in purchasing cryptographic tokens. This may result in a situation where block producers may not include your purchase of the Tokens when you intend to transact, or your transaction may not be included at all.

Privacy and data retention issues.

As part of any Token sales, the verification processes and the subsequent operation of the Protocol, the Company may collect personal information from you. The collection of such information is subject to applicable laws and regulations. All information collected will be used for purposes of the Token sales and operations of the Protocol, thus it may be transferred to contractors, service providers and consultants worldwide as appointed by the Company. Apart from external compromises, the Company and its appointed entities may also suffer from internal security breaches whereby their employees may misappropriate, misplace or lose personal information of purchasers. The Company may be required to expend significant financial resources to alleviate problems caused by any breaches or losses, settle fines and resolve inquiries from regulatory or government authorities. Any information breaches or losses will also damage the Company's reputations, thereby harming its long-term prospects.

Macro Risks

(a) General global market and economic conditions may have an adverse impact on the Company and its Affiliates' operations and the use of the Protocol.

I. The Company and its Affiliates could be affected by general global economic and market conditions. Challenging economic conditions worldwide have from time to time, contributed, and may continue to contribute, to slowdowns in the information technology industry at large. Weakness in the economy may have a negative effect on the Company and its Affiliates' business strategies, results of operations and prospects.

II. Suppliers on which the Protocol relies for servers, bandwidth, location and other services could also be negatively impacted by economic conditions that, in turn, could have a negative impact on the Company and its Affiliates' operations or expenses.

III. There can be no assurance, therefore, that current economic conditions or worsening economic conditions or a prolonged or recurring recession will not have a significant adverse impact on the Company and its Affiliates' business strategies, results of operations and prospects and hence the Protocol, which may in turn impact the value of the Tokens.

(b) The regulatory regime governing blockchain technologies, cryptocurrencies, Tokens, offering of Tokens, and the Protocol remain uncertain, and any changes, regulations or policies may materially adversely affect the development of the Protocol and the utility of the Tokens

I. Regulation of the Tokens, the offer and sale of Tokens, cryptocurrencies, blockchain technologies, and cryptocurrency exchanges is currently undeveloped or underdeveloped and likely to rapidly evolve. Such regulation also varies significantly among different jurisdictions, and is hence subject to significant uncertainty. The various legislative and executive bodies in different jurisdictions may in the future adopt laws, regulations, guidance, or other actions, which may severely impact the development and growth of the Protocol, the adoption and utility of the Tokens or the issue, offer, and sale of the Tokens by the Company. Failure by the Company and its Affiliates or users of the Protocol to comply with any laws, rules and regulations, some of which may not exist yet or are subject to interpretation and may be subject to change, could result in a variety of adverse consequences against the Company and its Affiliates, including civil penalties and fines.

II. Blockchain networks also face an uncertain regulatory landscape in many foreign jurisdictions. Various jurisdictions may, in the near future, adopt laws, regulations or directives that affect the Protocol, and therefore, the value of the Tokens. Such laws, regulations or directives may directly and negatively impact the operations of the Company and its Affiliates. The effect of any future regulatory change is impossible to predict, but such change could be substantial and could materially adverse to the development and growth of the Protocol and the adoption and utility of the Tokens.

III. To the extent that the Company and its Affiliates may be required to obtain licenses, permits and/or approvals (collectively, the "Regulatory Approvals") to carry out its business, including that of the creation of the Tokens and the development and operation of the Protocol, but are unable to obtain such Regulatory Approvals or if such Regulatory Approvals are not renewed or revoked for whatever reason by the relevant authorities, the business of the Company and its Affiliates may be adversely affected.

IV. There is no assurance that more stringent requirements will not be imposed upon the Company and its Affiliates by the relevant authorities in the future, or that the Company and its Affiliates will be able to adapt in a timely manner to changing regulatory requirements. These additional or more stringent regulations may restrict the Company and its Affiliates' ability to operate its business and the Company and its Affiliates may face actions for non-compliance if it

fails to comply with any of such requirements.

V. Further, should the costs (financial or otherwise) of complying with such newly implemented regulations exceed a certain threshold, maintaining the Protocol may no longer be commercially viable and the Company and its Affiliates may opt to discontinue the Protocol and/or the Tokens. Further, it is difficult to predict how or whether governments or regulatory authorities may implement any changes to laws and regulations affecting distributed ledger technology and its applications, including the Protocol and the Tokens. The Company and its Affiliates may also have to cease operations in a jurisdiction that makes it illegal to operate in such jurisdiction, or make it commercially unviable or undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction. In scenarios such as the foregoing, the distributed Tokens may hold little or no worth or value.

(c) There may be risks relating to acts of God, natural disasters, epidemics, pandemics, wars, terrorist attacks, riots, civil commotions widespread communicable diseases and other events beyond the control of the Company and its Affiliates

Any sale of the Tokens and the performance of the Company, its Affiliates and/or the Protocol's activities may be interrupted, suspended or delayed due to acts of God, natural disasters, wars, terrorist attacks, riots, civil commotions, widespread communicable diseases, epidemics, pandemics and other events beyond the control of the Company and its Affiliates. Such events could also lead to uncertainty in the economic outlook of global markets and there is no assurance that such markets will not be affected, or that recovery from the global financial crisis would continue. In such events, the Company and its Affiliates' business strategies, results of operations and outlook may be materially and adversely affected, and the demand for and use of the Tokens and the Protocol may be materially affected. Further, if an outbreak of such infectious or communicable diseases occurs in any of the countries in which the Company, its Affiliates, and the participants of the Protocol have operations in the future, market sentiment could be adversely affected and this may have a negative impact on the Protocol and its community.

(d) Blockchain and cryptocurrencies, including the Tokens are a relatively new and dynamic technology. In addition to the risks highlighted herein, there are other risks associated with the purchase of, holding and use of the Tokens, including those that we cannot anticipate. Such risks may further materialize as unanticipated variations or combinations of the risks discussed herein.

1.6 No Further Information or Update

No person has been or is authorized to give any information or representation not contained in this Whitepaper in connection with the Tokens, the Protocol, the Company or its Affiliates and their respective businesses and operations, and, if given, such information or representation must not be relied upon as having been authorized by or on behalf of the Company or its Affiliates.

1.7 Language

This Whitepaper may be translated into other languages. If any disagreement should arise due to different language translations, the version in English will prevail.

1.8 Advice

No information in this Whitepaper should be considered to be business, legal, financial or tax advice regarding the Token, the Protocol, the Company or its Affiliates. You should consult your own legal, financial, tax or other professional advisor(s) regarding the Token, the Company or its Affiliates and their respective businesses and operations. You should be aware that you may be required to bear the financial risk of any purchase of the Tokens for an indefinite period of time.

1. INTRODUCTION

The success of Crypto Kitties, the first crypto collectible using ERC721[1], has opened up possibilities of using smart contracts in a variety of non-financial areas other than tokens. However, transaction overload in transferring ownership, auctioning, and mating of kitties has caused severe congestion in the Ethereum Network[14] and raised concerns regarding limited capacity of public blockchains.

In addition, Ethereum developers have developed browser extensions such as MetaMask, MyEther-Wallet, and MyCrypto as well as mobile-based DApp Browser and DApp Messenger to improve accessibility and usability of decentralized applications for users. In terms of user experience, however, users have to pay fees for every transaction that can only be paid with Ether, which is a factor[20] that significantly reduces the usability of decentralized applications.

Tokamak Network aims to solve the problems mentioned above in the following ways. First, Tokamak Network can achieve high performance since Ethereum Virtual Machine is operating on the plasma chain run by only few nodes. Second, Tokamak Network alleviates centralization of the plasma chain through chain staking and plasma contract. Third, in order to build a platform for user-friendly applications, we make an alternative Ethereum Virtual Machine (EVM) that reduces the burden of transaction fees.

Tokamak Network addresses low performance and usability issues, which have been pointed out as weaknesses in the public chain. Furthermore, it can also keep the advantages of the public chain, such as decentralization, digital permanence, and reliability. It can also protect against DoS attacks. In addition, as the plasma chain uses Ethereum Virtual Machine, smart contracts of many DApps that have already been deployed can be ported directly.

[1]Non-Fungible Token, https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md

2. RELATED RESEARCH

2.1 Plasma

Plasma proposed by Joseph Poon and Vitalik Buterin of Ethereum Foundation is a layer-2 solution to address the scalability problem of Ethereum. In Plasma, merklized commitments(reduced block) are submitted periodically to Ethereum and based on this merklized data, verifies plasma blocks when problems occur. Initial plasma researches such as MVP and Cash proposed by Vitalik Buterin focused on simple transfer and verification; and further research expanded to deal with general states such as Plasma leap, and EVM.

2.1.1 Simple Transfer

2.1.1.1 Plasma MVP

This is the first plasma model presented since the publication of the Plasma whitepaper. Plasma MVP uses a UTXO-based binary merkle tree structure. It has a challenge system to prevent exits based on invalid states and additional confirmation and exit priority to solve data unavailability issues[8]. However, the confirmation procedure which requires a double signature to transfer severely undermined user experience. However, MVP served as a good starting point presenting direction for various future research tasks such as mass exit.

2.1.1.2 Plasma Cash

In Plasma cash, Sparse Merkle Tree (SMT) is used so that it can assign a unique ID and denomination to each coin[15]. The index of each node of the tree is defined as a token ID, and when the corresponding token is used, the related transaction is recorded as a value[9]. If a token is not used in the block, the value is null because there is no transaction for the corresponding token. Since it is possible to check whether the token is used in a specific block or not through the proof of inclusion and non-inclusion of SMT, anyone can verify the usage history of the token.

However, some issues remain to be solved in the future, such as not being able to spend tokens partially and the heavy task of verifying the history of each coin[28].

2.1.1.3 Plasma Group

Plasma Group is a framework based on Plasma Cash that is designed to enable anyone to easily deploy plasma chains. It also introduces several improvements to solve the issues of existing Plasma Cash. First, to solve fixed denomination[1], a large range of coins can be transferred in a single transaction. To prevent verification process from becoming too heavy, it uses Merkle Sum Tree[2]. This has improved the issues pointed out in the existing Plasma Cash.

2.1.2 General State Transition

2.1.2.1 Plasma Leap

Plasma Leap has implemented a general computation model as a type of small program called Spending Condition similar to bitcoin's pay-to-script hash (P2SH), and proposed Non-fungible Storage Token(NST) to manage the storage root hash for using the state model[3]. Through NST, it has resolved the data unavailability via exit mechanism used in the More Viable Plasma[25].

2.1.2.2 Plasma EVM

Plasma EVM is a model that can run EVM in a plasma chain. It uses Truebit-like verification game as a method to verify state transition and proposes requestable contracts to define exit authority and method of the contract account[12]. It also designed continuous rebase to resolve data unavailability. Plasma EVM is used as the core of Tokamak Network.

2.1.3 Plasma State Verification

2.1.3.1 TrueBit Protocol

TrueBit solved the verifier's dilemma by reducing on-chain transaction fees through separate verification procedures[34]. It executes complex operations off-chain, and only puts the results on the main chain. The method used at this process is called 'Verification Game.'

2.2 Transaction fee model for public blockchain

2.2.1 Ethereum

Ethereum imposes fees on all operations to prevent fraudulent use of Ethereum resources[38]. In other words, every operation in Ethereum pays time-space costs by means of "gas"[22]. All Ethereum transactions have a gas limit and gas price field. Gas Limit is a limit on how many computations of the transaction can be executed. Gas Price is the bids which are paid to the miners to include the transaction in a block.

[1]Fixed Denomination: In Plasma Cash, each coin can be used only as a fixed face denomination, like cash.

[2]It is not a simple hash tree like an ordinary merkle tree but a data structure that hashes and stores the sum of the balances of each node.

If the gas used in transaction execution is higher than Gas Limit of the transaction, it results in 'out of gas' error. In addition, if the Gas Price is not high enough (relative to other pending transactions), the miners are more likely not to include that transaction in blocks.

The bottom line is that the account that sends the transaction (sender, transactor) has to pay the Gas Used * Gas Price every time when sending a transaction, and for this, the account has to always maintain a certain balance level. Ethereum avoids denial-of-service (DoS) attacks through this type of fee model and solves the distribution problem of limited resource which is "the right to change the state of the blockchain." However, the cost of paying every transaction execution has greatly harmed the usability of decentralized applications (DApps) of Ethereum. Blockchain developers who were bothered by this demanded a chain without fees, and in this context, Steem and EOS emerged.

2.2.2 Steem

While most blockchains impose fees per transaction to prevent DoS attacks, Steem allocates bandwidth to accounts to prevent indiscriminate transactions[33].

Depending on the network congestion of Steem, the transaction bandwidth allowed per user is controlled flexibly. Each Steem account has a separate token called Steem Power to determine the weight contribution to Steem and the bandwidth that can be allocated to each account depending on the Steem Power reserve. However, since users must have tokens to be allocated the bandwidth, it does not support various functions such as delegation of bandwidth to other users.

2.2.3 EOS

In EOS, users can use the blockchain by with three computing resources, bandwidth, CPU, and RAM, from the 21 BPs that manage the blockchain network and allocates the resources[4]. Bandwidth and CPU are resources that are required to send transactions in the EOS. They are determined by the account's deposited EOS balance. And it also supports renting these resources to other accounts. RAM is an asset that can be traded in the market and used for storing data in the blockchain.

The advantage of the EOS transaction fee model is that users can generate a certain amount of transactions continuously within the resource limit (network, CPU, RAM) staked instead of simply paying. This allows EOS applications to allows user experience in which transaction fees do not burden users. In other words, once EOS is staked, it can be freely used within the range of the blockchain resources allocated to the account.

However, in order to make an account in the EOS, users need to have a certain level of RAM. This can be a good way to prevent Sybil Attacks, because it imposes costs on users. But it is a factor that hinders new entry of users and the price volatility of RAM[35] can undermine user experience.

3. SYSTEM CONFIGURATION

Chapter 3 describes the core of various technologies such as Plasma EVM[12] and the transaction fee delegation model[23] used in Tokamak Plasma. Plasma EVM, like existing plasma chains, have operators that commit the state of the plasma chain(child chain) periodically to Ethereum. In this process, if the plasma chain operator submits an invalid block, others can verify this through a verification game[1]. By giving a penalty to the operator or challenger depending on the result of verification game, the game improves the security of the plasma chain. In addition, when an operator attempts to withhold blocks, the data unavailability issue can be resolved via Continuous Rebase.

Plasma EVM adopted in Tokamak uses Ethereum Virtual Machine, which allows many existing decentralized applications (DApps) deployed on Ethereum to be moved to the plasma chain to improve performance [32]. In addition, users who send transactions in Tokamak Plasma can delegate fees to a third-party account[23]. Based on this, the DAO operating the initial DApp can create a single or multiple fee delegation account to provide users with a "no-fee user experience".

3.1 Generalized State Transition Enforcement

3.1.1 Concept of Generalized State and State Transition Enforcement

A state is a description of system status that is waiting for a transition. A transition is a set of actions to be executed when a condition is fulfilled or when an event is received[19]. Blockchain is a state transition system[5], and if it can define an infinite set of actions and the resulting state of those actions, it is considered close to Turing Complete. General state refers to the (infinite) set of states of a system that is close to Turing Complete.

A Turing Complete system can model another turing machine or state transition system. For example, if System B itself is programmed in System A and System B is evaluated based on the inputs and outputs of the program, it is possible to determine whether the specific state transition function performed by System B is correct or not[2].

[1] Truebit-Like Verification Game

[2] Note that if the system being modeled is Turing Complete, and data is unavailable at the time of the evaluation of System B, it is not feasible to verify state transition of B. Johann Barbie's Why Smart Contracts are NOT feasible on Plasma[**why-smart-contract-not-feasible-on-plasma**] describes this situation well.

3.1.2 Requestable Contracts: Defining Entering and Exiting Rules

In Ethereum, smart contract handles the generalized state. For example, the most commonly used token(ERC20) contract on Ethereum can be viewed as i) several accounts, ii) balances of each account, and iii) a program (object) that defines the rules for changing balances. The transfer function of ERC20 is defined as the balance state of the sender reduced and the balance state of the receiver increased.

'Enter' means to move the variable from the root chain to the plasma chain correctly and 'Exit' means the opposite. In order to reflect state variables and its requests between Ethereum and plasma chain, you must define enter/exit rule according to the target variable. For example, the rules for enter to move the balance state of a token from Ethereum to the plasma chain are as follows.

1. In Ethereum, the location of target variable(balance) to be reflected in the Plasma chain and number of tokens to enter are determined.
2. The corresponding number of tokens of the target variable are burned.
3. The corresponding number of tokens are minted in the plasma chain.

Enter rules can be defined in various ways. For example, Rule 2 may be implemented as freezing instead of burning. The contract implementation that shares the common specifications of these enter and exit rules is called a requestable contract.

The following number counters and tokens are very simple forms of smart contracts that will broaden your understanding of enter and exit rules.

3.1.2.1 Number Counter

A number counter is a program that counts numbers, and the number recorded increases by 1 starting from 0. The first number counter can be operated in Ethereum and then moved to the plasma chain based on a specific period, and vice versa. It is important that although the two chains are structurally separated in the process of exchanging states, the global value of the numeric state managed by this number counter should be logically correct.

The following BaseCounter contract code is the implementation of the basic counter. The simple counter and the freezable counter that follow can be implemented by inheriting the following contracts and being modulated into requestable counters in various ways.

```
contract BaseCounter {
  uint n;
  function count() external {
    n++;
  }
  function getCount() external view returns (uint) {
    return n;
```

```
    }
}
```

The user can increase the value of the counter by 1 calling the count() function. If you want to know the counter value at a specific time, you can check the current value by calling the getCount() function.

3.1.2.1.1 Simple Counter When there is a counter contract that allows anyone to increase the number, the most intuitive enter rule is to reduce the number in Ethereum and increase the value by the amount in the plasma chain. The exit rule, on the contrary, reduces the value first in the plasma chain and increases the value in Ethereum. The execution process of the Simple Counter that implements this is shown as follows:

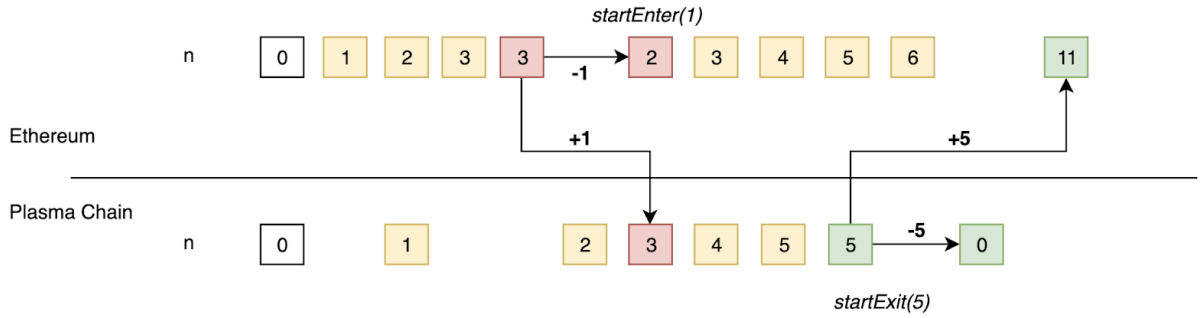

Figure 3.1: Simple Counter

The above figure describes the change of the contract variable n in each chain. The yellow squares mean that the count() function is called, red means enter, and the green means that it has changed due to exit. The core code of the applyRequeastlnRootChain() function that specifies the state transition rule of the counter value in Ethereum is as follows:

```
function applyRequeastInRootChain(...) {
    ...
    if (isExit) {
      n = n.add(trieValue.toUint());
    } else {
      n = n.sub(trieValue.toUint());
    }
    ...
}
```

When entering the plasma chain from Ethereum, the value of Ethereum counter decreases, and when exiting from the plasma chain to Ethereum, the value increases.

However, because the variable n can be reduced due to entry and exit, the Simple Counter must read the states of both Ethereum and Tokamak Plasma chain to determine how much the user has

counted in a certain state, and then the values are added separately. On the other hand, there is an advantage in that counters of both chains can be used at the same time regardless of whether the count value enters or exits.

3.1.2.1.2 Freezable Counter Another way is to freeze the number of counter contracts in each chain just before enter and exit. The Freezable Counter can be avoided if the number is reduced via request after freezing.

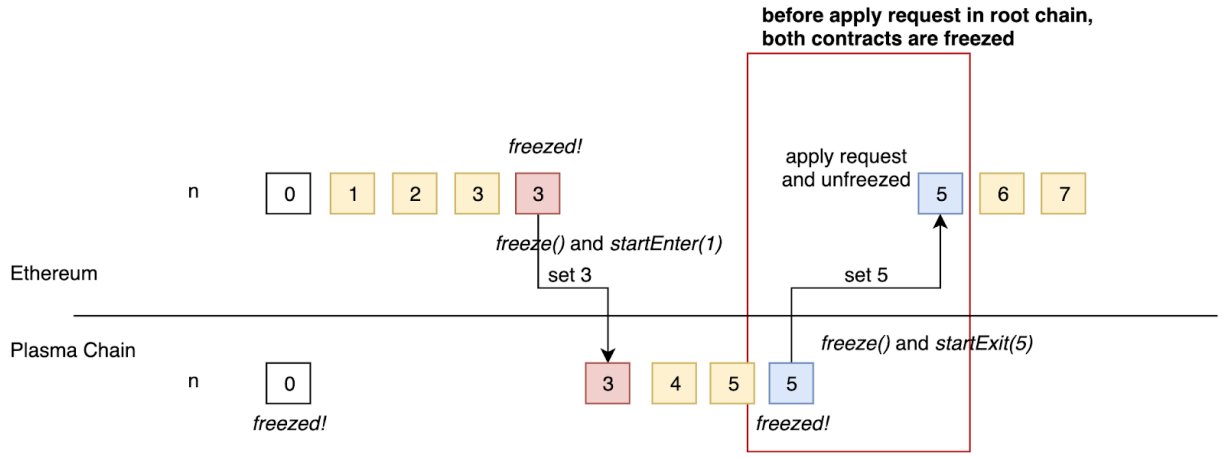

Figure 3.2: Freezable Counter

The state transition rules for Ethereum are as follows: (the key implementation code for the applyRequeastlnRootChain function is as follows.)

```
function applyRequeastInRootChain(...) {
    ...
    require(frozen)
    if (isExit) {
      frozen = false;
      n = trieValue.toUint();
    } else {
      require(n == trieValue.toUint());
    }
    ...
}
```

Once enter function is processed into the Tokamak Plasma chain from Ethereum, the corresponding state in Ethereum is frozen. The state value is unfrozen after processing exit from the Tokamak Plasma chain to Ethereum. In the process of freezing and unfreezing, both chains exchange counter state values with each other. The advantage of this implementation is that the non-frozen chain of both chains always manages the global state of the counter value. Therefore, the user only needs

to read the counter value of the chain that has not been frozen to know the current global counter value.

However, after exit, it has to go through the challenge process in order for the state values to be reflected in both chains. There is a tradeoff in that the counter contract cannot be used during this period. To avoid such a situation, the state variable used for enter and exit must be different.

3.1.2.1.3 Trackable Counter The Freezable Counter has a tradeoff in that the counter cannot be used until the challenge is complete. An alternative implementation to solve this problem is a trackable counter. A trackable counter increments or decrements the value of the counter in both chains after checking that the state is ready to enter or exit through a separate state variable requestableN in the enter and exit process.

The core logic of the applyRequestInRootChain() function executed in the root chain is as follows:

```
function applyRequeastInRootChain(...) {
    ...
    if (isExit) {
      n = n.add(_n);
    } else {
      requestableN = requestableN.sub(_n);
    }
    ...
}
```

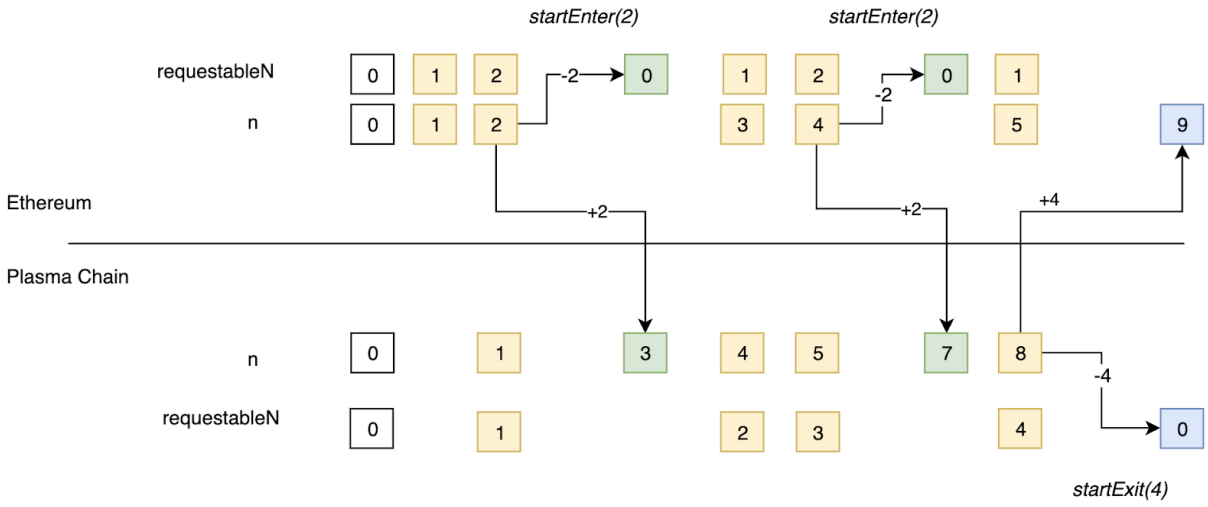

Figure 3.3: Trackable Counter

3.1.2.2 Token

In the case of a token contract, the simplest form of the enter rule is to burn the token in Ethereum and mint the token in the plasma chain. In the opposite, exit burns the token in the plasma chain and mints the token in Ethereum.

3.1.2.2.1 Requestable Simple Token A Requestable Simple Token is a modification of OpenZeppelin's mintable ERC20 token(ERC20Mintable) into a requestable form. The contract allows enter and exit for both state variables, owner and balances. In other words, a simple requestable token can be used across both Ethereum and the plasma chain.

The core logic of the applyRequestInRootChain() function executed in the root chain is as follows:

```
// apply exit
if (isExit) {
  if(bytes32(0) == trieKey) {
    owner = requestor;
  } else if (keccak256(bytes32(requestor), bytes32(2)) == trieKey) {
    balances[requestor] += trieValue.toUint();
  }
} else {
  // apply enter
  if(bytes32(0) == trieKey) {
    // just check permission.
    require(owner == requestor);
  } else if (keccak256(bytes32(requestor), bytes32(2)) == trieKey) {
    require(balances[requestor] >= trieValue.toUint());
    balances[requestor] -= trieValue.toUint();
  }
}
```

Depending on the trieKey, you can identify which variable is requested. When trieKey is 0x00, it is defined as a request for the owner variable. Because the balances variable is a mapping(hash table) with an address as a key, sha3(requestor, OxO2) is used to use trieKey as an identifier for the requestor.

3.1.2.2.2 Requestable ERC20 Wrapper Since the existing ERC20 token interface itself is not requestable, they need to be wrapped in a new token to use in Tokamak Plasma. These wrapped tokens are the redemption for the original token. Users can use this redemption in the Tokamak Plasma chain and exchange original tokens at any time in Ethereum.

The following RequestableERC20Wrapper contract implements the corresponding features.

```
contract RequestableERC20Wrapper is StandardToken, RequestableI{

    function deposit(uint _amount) external isInitialized returns (bool) {
      mint(msg.sender, _amount);
      require(token.transferFrom(msg.sender, this, _amount));
      return true;
    }

    function withdraw(uint _amount) external isInitialized returns (bool) {
      burn(msg.sender, _amount);
      require(token.transfer(msg.sender, _amount));
      return true;
    }

}
```

The following code implements feature to deposit/withdraw the underlying ERC20 token.

```
function applyRequestInRootChain(
  bool isExit,
  uint256 requestId,
  address requestor,
  bytes32 trieKey,
  bytes trieValue
) external isInitialized returns (bool success) {
    ...
    uint v = decodeTrieValue(trieValue);

    if (isExit) {
      mint(requestor, v);
    } else {
      burn(requestor, v);
    }
    return true;
 }

function applyRequestInChildChain(
  bool isExit,
  uint256 requestId,
  address requestor,
  bytes32 trieKey,
```

```
  bytes trieValue
) external returns (bool success) {
    ...
    uint v = decodeTrieValue(trieValue);
    if (isExit) {
      burn(requestor, v);
    } else {
      mint(requestor, v);
    }
    return true;
}
```

In the case of an enter request, the token is burned in Ethereum and minted in the Tokamak Plasma chain. Conversely, an exit request burns the token in the Tokamak Plasma chain and mints it in Ethereum. Since existing ERC20 tokens are wrapped in a RequestableERC20Wrapper in Ethereum, the user can always retrieve the original tokens from the wrapped tokens.

3.1.3 Verification Game : Challenge

The Turing Complete system can model other Turing Complete systems. The verifier contract is deployed on Ethereum and models the state transition rules of the plasma chain. Root chain contract can use the verifier contract to determine whether the state transition of the plasma chain has processed correctly. Users monitor the plasma block mined by the operator and raise challenges if an invalid block is submitted. Incorrect state transition and other protocol violations can be challenged. The null-account challenge, the exit challenge, and the minimum gas price challenge exemplify such a situation.

3.1.3.1 Verifier and Verification

Since the state transition of Ethereum is processed by Ethereum Virtual Machine(EVM), the EVM itself must be modeled in the root chain to verify the state of the plasma chain. Solevm[3] is an EVM implemented in Ethereum's smart contract language solidity, and its functional completeness has been improved via solEVM-enforcer[4], etc. In the future, if the plasma chain requires more features than the current EVM, the verifier contract may be diversified accordingly. As an example, the configuration and execution model of opcode(Ethereum basic computation unit) can be changed through eWASM in the process of introducing Ethereum 2.0, and verifier implementation suitable for the eWASM execution model can verify the plasma chain with new state transition rules.

State transition of blocks in Tokamak Plasma must always be processed correctly. For example, when user A sends 10 tokens to user B, it is a correct computation when balance of A decreases by

[3] https://github.com/Ohalo-Ltd/solevm
[4] https://github.com/leapdao/solEVM-enforcer

10 and balance of B increases by 10. If the increase/decrease in the two users' balances is different from this, it means that computation has not been performed correctly.

3.1.3.2 Exit Challenge

However, an exit request can be generated even if the state of the plasma chain cannot accept an exit request. For example, a request may be made to exit 1000 tokens, even if a particular account only has 100 tokens. The exit request transaction will be reverted in the plasma chain, but Ethereum cannot determine whether the request is valid when the request is generated. Exit challenge prevents invalid exit requests from being reflected in Ethereum by submitting proof which is the execution result of invalid exit request transaction in the plasma chain[12].

Even if the exit challenge is successful, the chain staking will not be slashed. Instead, the user deposits a small amount of exit deposit in the process of making an exit request. If the exit challenge is successful, the deposit is given to the challenger and used as an economic incentive for the exit challenge.

3.1.3.3 Protocol Challenge : Null-Address and MGP

In Tokamak Plasma(plasma EVM), null-account is used for reflecting the state transition requests generated outside the plasma chain. If the operator includes the request transaction in non-request blocks, instead of request blocks, it can be challenged with null-account challenges.

Minimum Gas Price means the price floor of transaction's Gas Price in Tokamak Plasma. If the plasma operator includes a transaction in the plasma block that pays less than the minimum gas price, then the block including this transaction can also be challenged.

Tokamak Plasma is likely to improve as Ethereum 2.0 roadmap progresses, and protocol challenges can be used as a useful means to deter violations of various additional rules to be made in the future.

3.2 Data Availability

Data unavailability in plasma means that users cannot access the block data of plasma chain. This may occur due to network failure or block withholding attacks, in which the operator maliciously does not propagate blocks.

If the data is not available, the security of the plasma data cannot be assured. Most plasmas have a challenge system that prevents double payment by submitting proof to the root chain when an operator or user attempts double-spending attacks. However, if no one can access the data to be challenged, it becomes impossible to determine the validity of the data. In other words, if the data is not available, the challenge system cannot be operated. As a result, the security of the plasma chain cannot be guaranteed.

Instead of explicitly determining whether the data is available or not, every plasma aims to ensure that users can safely exit from the chain at any time. The bottom line is that while it is

relatively easy to ensure that users can always exit safely in *turing incomplete plasma*, in *turing complete plasma*, such as Tokamak Plasma, it is not easy to ensure a safe exit.

The reason is that when blocks are withheld, it is not feasible to verify the state transition so all states must be considered to be invalid[**why-smart-contract-not-feasible-on-plasma**]. That is, even if users exit after a block withholding attack, they cannot be guaranteed the safety since all the states are not valid. For this reason, most plasmas limit Turing Completeness so that they can avoid this issue.

Tokamak Plasma addresses the data unavailability without limiting the feature of the plasma chain through the Continuous Rebase[12] of plasma EVM. If the data is not available in Tokamak Plasma, users can exit from the chain by submitting an escape request. Since the escape request is always processed first based on the last finalized state, user's data can always be secured even if data is unavailable.

3.3 No Consensus

No consensus is faster than no-consensus. For example, the performance of a blockchain consisting of nodes with Proof of Authority(PoA) is determined by the physical hardware and network specifications of those nodes. This is incomparably faster than the target performance of Proof of Work and Proof of Stake involving hundreds or thousands of unspecified nodes in a general public blockchain.

The security of the plasma chain is ensured by the plasma protocol of Ethereum. Therefore, it is not necessary to introduce an additional consensus algorithm into plasma for security. It is recommended to use Proof of Authority(PoA) in which only nodes that have deposited chain staking can mine blocks in plasma chain. However, even if the Tokamak Plasma adopts consensus algorithms such as Proof of Stake(PoS) and Byzantine Fault Tolerance(BFT), there are no restrictions on the plasma network configuration[5] Even if blocks are generated through a specific consensus in the plasma chain, state transition must be processed according to rules defined by verifier in the root chain.

In summary, the Tokamak protocol itself does not require a specific consensus in the plasma chain. Such non-consensus attribute gives a variety of choices of algorithms to be adopted depending on the purpose and situation of each plasma chain.

[5]These additional consensus algorithms can prevent transaction censorship in the Plasma chain.

4. Economic Model

4.1 Token and Seigniorage

4.1.1 Usage and Units of Tokens

Tokamak Network has an ERC20 token called TON. TON is used for a) chain staking and b) plasma transaction fees for the purpose of i) enforcing correct operation of the plasma chain and ii) prevention of Sybil attacks on the plasma chain. To open plasma chain in Tokamak Network, the operator must deposit minimum TON for chain staking in Ethereum. In addition, if the plasma chain is challenged, the staked token is given to the challenger as a prize. TON is also used for fees to send transactions in Tokamak Plasma chain. In this process, it is converted into stamina.

Generally, ERC20 tokens use 10^{18} decimal points. To minimize confusion when using tokens in low units, the name of each unit is set to the following:

- 1 = poon
- 10^{18} = ton

These units are similar to the relationship between "ether" and "wei" in Ethereum. The smallest unit, Poon, is used for micropayments and technical purposes, and the largest unit TON will be used for general and large transactions.

4.1.2 Token Seigniorage

Token seigniorage should work as an incentive for actions that generate the greatest value in the platform. The most important action in Tokamak Plasma is to reduce the transaction burdens by creating plasma blocks. Therefore, newly issued TON is awarded when operators(miners) commit plasma blocks to Ethereum.

Such newly minted TON is issued indefinitely every year in the amount of 0.19 of the initial supply (fixed quantity, not fixed percentage). The method of issuing a fixed quantity indefinitely is already a token issuance model used by Ethereum[5], which can open the opportunity of getting TON through the Plasma chain operation rather than the market for the long term.

In this case, the inflation rate of tokens converges to 0%, starting from 25%. In the process, the influence of contributors such as operators and communities of Tokamak Network can be gradually increased.

4.1.3 Seigniorage Distribution

The size of token seigniorage given to the operator is determined by the size of the chain staking and the enter deposit[21]. The chain staking is TON deposited on Ethereum when the genesis block of Tokamak Plasma chain is generated. The enter deposit is the amount of TON that users have entered into the plasma chain.

If the operator intends to operate a plasma chain with high reliability, the amount of chain staking will be high, and seigniorage gain will also increase. Even though the chain staking itself is not high, the operator's seigniorage gain can be increased if the amount of enter deposits is large enough[21]. The larger the chain staking, the more likely it is that the amount of the enter deposit also is larger. Therefore, the seigniorage is likely to be given mainly to operators with large capital. However, if these operators create an invalid block, the seigniorage and the chain staking will be given to challengers[21].

The core principle of seigniorage distribution is to give economic rewards to the entity that performs the right actions. Tokamak Network rewards operators who commit correct plasma blocks and challengers who discover malicious operators so that the security of the plasma chain can be assured.

4.1.4 Ether and Tokamak Network Tokens

The seigniorage is generated in the process of committing blocks to Ethereum in Tokamak Plasma. And Ether is used as a transaction fee in this process. The cost of transactions to commit blocks paid in Ether can alleviate transactions for the purpose of only getting the seigniorage.

4.2 Plasma Chain Staking

To deploy Tokamak Plasma chain, the operator must deposit a minimum amount of TON on Ethereum as chain staking. The chain staking not only serves as a basis for seigniorage gain that the operator receives in committing plasma blocks but also serves as a prize for verification games to prevent incorrect blocks[21]. If the operator intentionally commits an invalid block, the chain staking is given to the challenger through the verification game. The chain staking can be viewed as cost of litigation for future conflict situations(verification games), and it makes the operator to maintain the plasma chain properly.

The chain staking can be used as a key criterion for determining the stability and reliability of the chain before users choose to use the plasma chain. When users compare two plasma chains A, B, and if chain staking of A is larger than B's, they can intuitively determine that A is more reliable. However, the chain staking may not be the single criterion of reliability. If the operator has high reliability outside the blockchain - for example, if a company with a very large capital directly operates the plasma chain - the reliability of the chain can be high even if the chain staking is small.

Nonetheless, operators need a large amount of chain staking to make users trust the plasma chain. Note that the benefits arising from chain staking are not only for operators but also for users.

However, it is the operators that deposit chain staking, and since it cannot be used elsewhere, it can be considered as opportunity costs. When the chain staking is used only for the prize of verification games, the operators have to bear the cost with no benefits from it. Therefore, a token seigniorage that preserves the opportunity costs of the chain staking is necessary.

4.3 Plasma Transaction Fee

4.3.1 Sybil Attack and Transaction Fee

Users have to pay to use limited resources of the blockchain. The Gas and Gas Price in Ethereum are costs for using "computing power of Ethereum". With concepts 'Rivalry' and 'Excludability' of economics, the characteristics of resources which are "computing power of Ethereum" can be described as follows:

- Rivalry : If one account sends multiple transactions, it becomes hard for other accounts to send transactions. It is because the capacity of blocks to include transactions is fixed (Block Gas Limit of Ethereum).
- Excludability : In order to process computation, the cost(Gas Price) to be spent per a unit of computation is determined.

Resources with low excludability are subject to the 'tragedy of commons'. In other words, if there is no transaction fee or it is insufficient, computing resources of blockchain will be used excessively. In this sense, transaction fees such as Gas and Gas Price are inconvenient for users, but they are essential to stabilize the overall network. However, the method of the imposition of these fees may vary. EOS and Steem provide each account with the right to make transactions for a certain period of time, depending on the resources it holds. This type of policy can improve the user experience in terms of predictability.

Tokamak Plasma use flexible fee policy based on the transaction fee delegation model[23]. Stamina and Minimum Gas Price(MGP) discussed below specifically present improved fee policy of Ethereum.

4.3.2 Stamina: fee delegation and regeneration

Tokamak Plasma users can generate 'stamina' by depositing TON. Stamina is the right to make a certain number of transactions during a certain period in the plasma chain. When users send transactions, stamina is paid instead of Ether and regenerated after a certain period of time[21]. This type of fee policy is like renting 'bandwidth' where users can use the plasma chain for a certain period of time. Rental costs can be seen as the time opportunity cost of TON deposited during that period. Stamina can also be delegated to other accounts. The accounts of delegator-delegatee are called the stamina pair.[24].

Stamina pairs can be applied in a variety of ways. For example, if the service provider(DApp developers) wants to make users free from fees, one can make the service provider's manager account

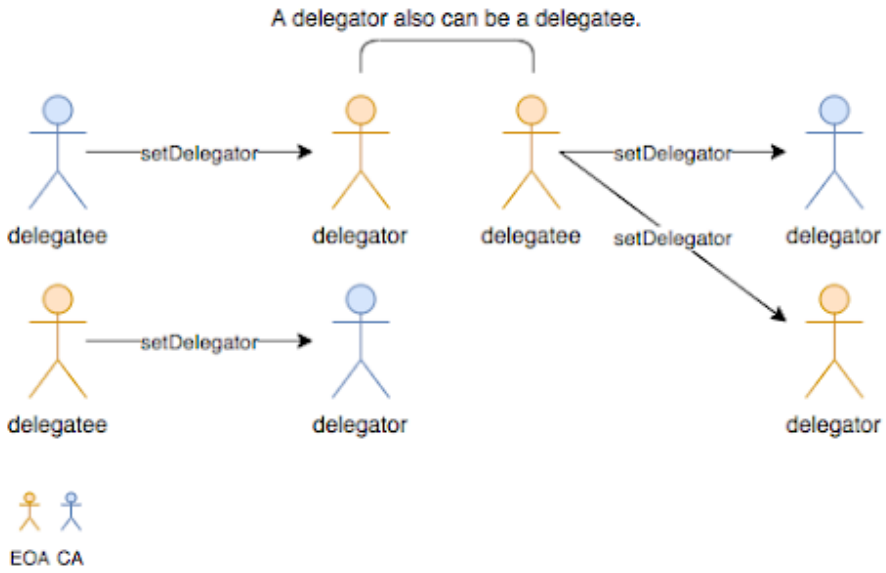

Figure 4.1: Stamina Pair

and the user's account as the stamina pair so that users do not need to pay for fees. This is like giving free call time to a customer who bought a prepaid phone, and it can attract initial customers and bootstrap the service. Likewise, DApp service providers who want to attract early users are more likely to utilize stamina pairs actively.

4.3.3 Minimum Gas Price; MGP

Minimum Gas Price means the minimum price that users must pay to send transactions in the plasma chain. Unlike Ethereum, Tokamak Plasma does not include transactions with high Gas Price first. The operator of Tokamak Plasma does not have any incentive to include transactions based on Gas Price. Instead, the operator receives seigniorage proportional to the chain staking and enter deposit. In most cases, Gas Price remains stable until the block is filled with transactions, fixed fee policy also can be adopted[6].

The minimum gas price should be determined when the plasma chain is first deployed, but it can change any time. Combining minimum gas price and stamina pairs can create a very flexible fee model. For example, if the minimum gas price is set at a very low level, and the service provider has a minimum TON to create stamina pairs for users, both the users and the service providers will not actually pay anything to use the plasma chain. However, these low costs cannot be sustained over the long term because of the tragedy of common resources. The minimum gas price may be raised above a certain level to prevent free riders.

This pricing policy can often be seen in reality. In the case of online games, users are provided service free of charge until a certain number of users join. For home appliances, sellers allow customers

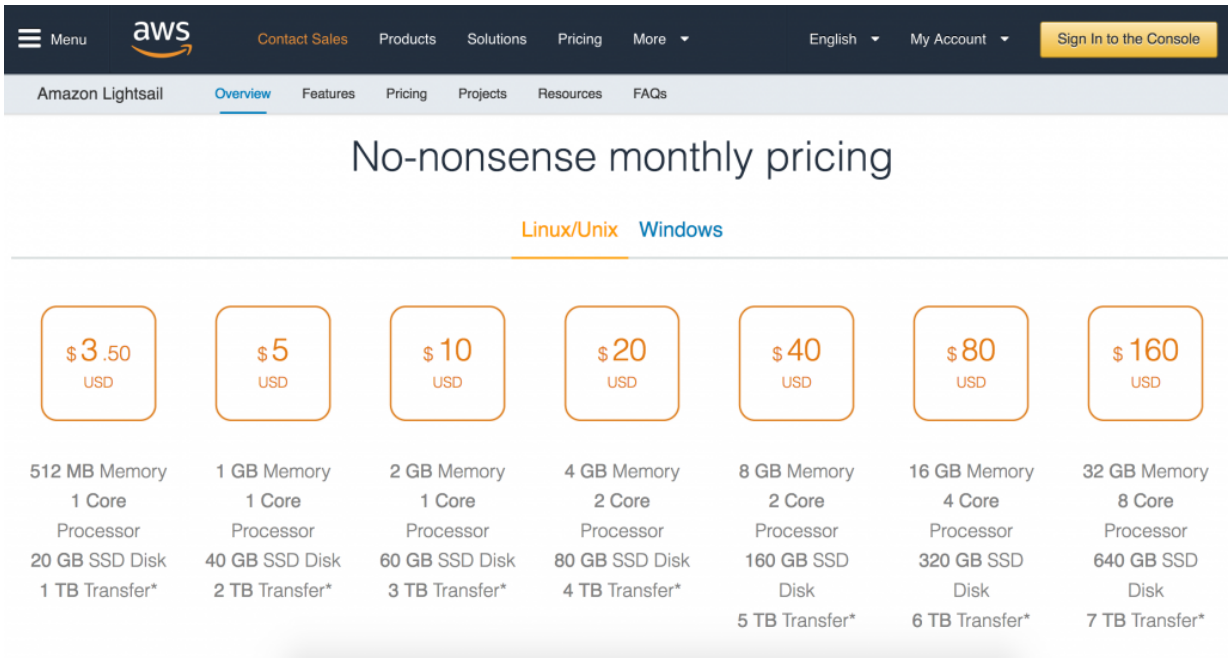

Figure 4.2: Amazon Web Services Billing Policy

to use it free for a certain period and buy later. Amazon Web Services provides low-performance instances at a low cost. In the process of using it, users will need higher performance. Then they will consider purchasing high-performance, expensive instances.

5. Decentralized Application Blockchain

Chapter 5 describes various Tokamak Plasma applications that can operate on plasma and its derived business models. The structure of the plasma chain created in Tokamak Network is the same as that of Ethereum. Therefore, various DApps such as DEX, games, wallets, and payments which are already running on the mainnet can be ported and operated. It can connect existing Ethereum-based private chains to Ethereum through plasmifying. Such ㅐlasma chains can be used for various purposes. In addition, Tokamak's fee model and token seigniorage create new business opportunities in areas other than applications.

However, the following business model will not be implemented by Onther PTE. LTD., and only explains about possible business model that can operate on Tokamak Plasma through DApp porting by participants, not Onther PTE. LTD. Also, all requirements such as reports or licenses related to corresponding business model must be completed by participants who port it on their responsibilities, and Onther PTE. LTD. does not guarantee in any related matters or is responsible for any related issues.

5.1 Plasma DApps

5.1.1 Decentralized exchange(DEX)

Centralized exchanges have a larger market share than decentralized exchanges due to superior usability. However, starting with the Mt.Gox[36] hack in 2014 in which $405 million worth of cryptocurrency was stolen, dozens of centralized exchanges have been disappearing or shutting down for unclear reasons. As such, problems with centralized exchanges have been continuously raised. Fundamentally, such problems result from the fact that protocol of the cryptocurrencies is decentralized, but most of the infrastructure in which they are traded is centralized.

Decentralized exchanges i) enable direct trading between users without the involvement of a central server; ii) keep users' funds in the wallets of the users and not the exchange; iii) implement order book and settlement processes through smart contracts on the blockchain; and iv) adopt a structure that converts fiat currency or other assets to tokens(Digix Gold, USDT, etc.) that can be traded in the blockchain using ERC20 proxy tokens.

In this way, many decentralized exchanges have been created in the form of Ether Delta[1], IDEX[2],

[1] https://etherdelta.com/
[2] https://idex.market/

OASIS Dex[3]. However, the market share is low due to inefficiency and poor usability such as 1) latency caused by the block mining time of Ethereum, ii) transaction fees paid for all actions to trade on chain.

In Tokamak Plasma chain, we can port existing decentralized exchanges, and it can support highly frequent transactions with no censensus. It can also improve its usability by paying fees in stamina for trading on the Plasma chain.

However, even in a high-performance decentralized exchange, matching the bid and ask prices of the order book would not only put a burden on the blockchain, but front running may also occur [17][16] if a single or a small number of operator perform this.

In this case, the decentralized exchange can provide a public interface that can attach a market maker that matches the bid and ask of the order book. By creating and distributing bots that perform this efficiently, anyone can become a market maker and compete. This makes it possible to prevent front running that occurs during bid and ask matching.

However, in the case of opening a decentralized exchange, considering the guidelines related to the cryptocurrency in the Financial Action Task Force on Money Laundering(FATF), the operator must carefully examine the procedures such as authorization/approval under the jurisdiction that can be applied to the operator, and obtain the necessary authorization/approval for the responsibility required of the operator.

5.1.1.1 Cryptocurrency Collateral System(Compound Protocol)

Compound Protocol is a lending platform that replaces existing interest rate calculation method with an algorithm. It is designed to eliminate the imbalance of demand/supply that can easily occur when the number of lenders and borrowers in the existing P2P lending platform is small.

To use Compound Protocol, all users(lenders, borrowers) have to supply the collateral assets to the money market contract of the Compound Protocol. In this case, if the user only supplies and does not borrow[4], the interest(cryptocurrency instead of actual money) is distributed according to the "SupplyRateIndex" calculated by the algorithm in the pool of the relevant asset. The lender can borrow from another pool of assets equal to two-thirds of the value of the collateral. For example, you can deposit 3 ETH and borrow DAI or ERC20 assets equivalent to 2 ETH.

In the collateral lending method in Compound Protocol, users can borrow various assets such as B, C, D with the assets of A as collateral. However, in this process, price oracles are necessary for calculating the value of each collateral. The protocol requires more transactions for the oracle price feed for each asset supported which will burden the network. Tokamak Network has an advantage in operating various loan assets over the current main network because there is no transaction fee charged to maintain price oracles for a variety of assets.

Compound Protocol can be used in other decentralized applications, such as exchanges. If a compound lending system is added to a decentralized exchange that has already been created in

[3] https://oasisdex.com/
[4] lender

Tokamak Network, decentralized finance is possible. In this environment, users have the advantage of leveraging their assets, and it becomes easier for the exchanges to acquire liquidity. Such a lending system can be a business model applied and operated by individual users of Tokamak Network.

5.1.2 CryptoKitties(ERC721)

Recently, there have been many decentralized games with crypto collectible such as CryptoKitties using non-fungible tokens(ERC721). At this point, however, they only focus on "collectible" items, and the interaction between users is limited to simple functions, such as breeding and auctioning. The key points to facilitate user-to-user interaction in blockchain are i) processing transactions at high speed and ii) reducing the burden of cost between transactions. Tokamak Plasma can process a large number of transactions that enable interactions between users.

In order for these games to work in Tokamak Plasma, game contracts should be developed as a requestable contract. In case of breeding between CryptoKitty, to breed kitties in plasma chain, i) identifier of kitty such as kitty ID managed on the kitty core contract needs to be hashed using gene information, etc., and ii) ownership, iii) kitties data(genetic information, etc.) and iv) block hash of the root chain, need to each be converted into requestable variables.

The reason for i) is because the identifier of the individual kitties of kitty core is an auto-increment sequence, so when kitties that have entered the plasma chain produce new kitties through breeding, the kitty identifiers can collide when exiting to the root chain. ii) and iii) are because anyone should be able to request data to track the information of ancestor kitties. iv) is because in the gene information mixing process during breeding, the block hash of Ethereum is used as a parameter[27].

What is interesting is that when there is one version on Ethereum, there can be multiple plasma chains to use it simultaneously. For example, assume that after 10,000 kitties were created, 2,000 of them entered into plasma chain B with 8,000 already were entered into plasma chain A. Kitties of the same kitty contract are now split and managed on both A and B chains. However, divided kitties are structurally separated; they are not logically separate [10]. The kitties of A can be transferred to B at any time, and the kitties generated in B can be transferred to A at any time. This is possible because all plasma chains maintain a logical consistency of the global state of decentralized applications through a structure called requestable contract.

The most important design principle of a plasmified crypto game is which factors affect the global state of the game and how these elements are implemented in a requestable contract. In the case of CryptoKitty, the most important global state value is the genetic information of the kitties, and key parameter for generating genetic information is the gene of the parents and the block hash of Ethereum[27]. Requestable CryptoKitty contracts are designed such that these state variables can be exchanged between both chains.

5.1.3 Cryptocurrency Wallets and Payment

As the cryptocurrency market grew, wallet hardware and software have come into the limelight over the last few years. These wallets can be divided into two categories according to the location of

the key. First one is decentralized wallets to store the private key directly in the device. Second one is centralized wallets in which the service provider directly holds the key and sign on behalf of users. Centralized wallets have gained a lot of popularity compared to decentralized wallets even though service providers may lose the key or keys may be stolen. One of the reasons for this is the convenient features provided by centralized wallets(participation in ICOs, air drops, payments, zero-fee transfers, etc.) and low burden as users do not have to manage their own keys.

The reason why decentralized wallets can not offer convenient features compared to centralized wallets is because, paradoxically, each user has control over their key. This is because they have to pay transaction fees to process any action on-chain. For example, a decentralized wallet service can assign a multi-signature wallet to each user to hedge the risk of losing a key. If users lose the key, they can restore keys through 2/3 approval by the company or a designated agent. However, this type of multi-signature contract cause astronomical transaction costs when issued to hundreds of thousands of users. It will be exacerbated when providing various payment options such as escrow smart contracts.

Such costs can be reduced if decentralized wallets run on Tokamak Network. Multi-signature contracts can be deployed on the plasma chain and distributed to users. In addition, wallet services can assign bandwidth to users for a certain period of time through stamina and adjust the level of the bandwidth according to users. The service experience of wallet users is also improved because users do not have to hold Ethereum to send transactions.

5.1.4 Decentralized Value Stabilization Token(MakerDAO)

The DAI of MakerDAO is a representative decentralized stable token made with Ethereum and ERC20 as collateral. MakerDAO's decentralized token generation algorithm requires several participants to operate. MakerDAO Smart Contracts are designed to contribute naturally to the MakerDAO ecosystem in the process of each of these participants maximizing their own profits.

The MakerDAO system consists of several contracts, which are Dai contract, Tub contracts to generate the token, and Tap contracts for settlement of bad debt. The value stabilization protocol operates 24 hours a day, and each contract continues to generate transactions. Of these, most transactions are generated from the Dai token contract, followed by Tub and Tap. The average monthly transaction volume of Dai, Tub, and Tap and transaction fees paid in this process are as follows.

	Monthly average number of tx	Monthly average transaction fees	Annual user fees (1 ETH = 165.45 USD)
Dai (Sai)	15677.3	20.2 ETH	40,105.0 USD
MakerDAO (Tub, Tap)	623	1.5867 ETH	3,150.2 USD

Table 5.1: 2019.1.1 $\sim$ 2019. 3.31 Dai,MakerDAO Transaction Fees

There are also voting for the operation of the stable token system and various third-party smart contracts using Dai (multi-signature wallets, escrow contracts, etc.). As the ecosystem expands, transactions generated by third-party contracts will increase and the burden of fees will also increase. Tokamak Plasma, which can adopt flexible fee policies, can easily accommodate these requirements, and the following Native Stable Coin andNon-Native Stable Coin describe such use cases.

5.1.4.1 Native Stable Coin

In Tokamak Network, we can issue stable coin by generating CDP[5] which is collateralized security based on specific token. This can be done on Ethereum as well, but if (Oracle) transactions recording the market price information of the collateral tokens increases and there are no separate incentives to do it, it will be a significant burden. Running MakerDAO's stable coin on Tokamak Plasma can reduce (Oracle) transaction costs.

In addition, when implementing the stable coin in the form of requestable contract, it can be exited and used with various smart contracts already running on Ethereum. It can be listed on a centralized and decentralized exchange already made.

5.1.4.2 Non-Native Stable Coin

Transactions using Dai token in Ethereum have been on an increasing trend since the second half of 2018. If this trend continues, at the beginning of 2020, a monthly average of 2.2 times the current level of transactions will be generated.

Considering the increasing number of decentralized applications on Ethereum platform, we will need higher Gas Price to use Dai tokens. If Dai transactions could be distributed to Tokamak Network, it can reduce the burden of many transactions in Ethereum.

If Dai is wrapped in the form of requestable token, already issued Dai tokens can enter Tokamak Network. The most representative use of Dai in this form is to use it as a base currency for a decentralized exchange operating on Tokamak Network. In addition, it can solve scalability problems that arise in the process of using Dai in various smart contracts on Tokamak Network such as complex-state custody services which include multi-signing, escrowing and payments using Dai, Dai-secured smart contracts, etc.

5.2 Domain-specific Plasma

5.2.1 Privacy

5.2.1.1 Anonymous ERC20

Advances in cryptographic technology, including zero knowledge proof, have accelerated the emergence of a variety of techniques that simultaneously guarantee the integrity and privacy of public blockchain

[5] https://cdp.makerdao.com/

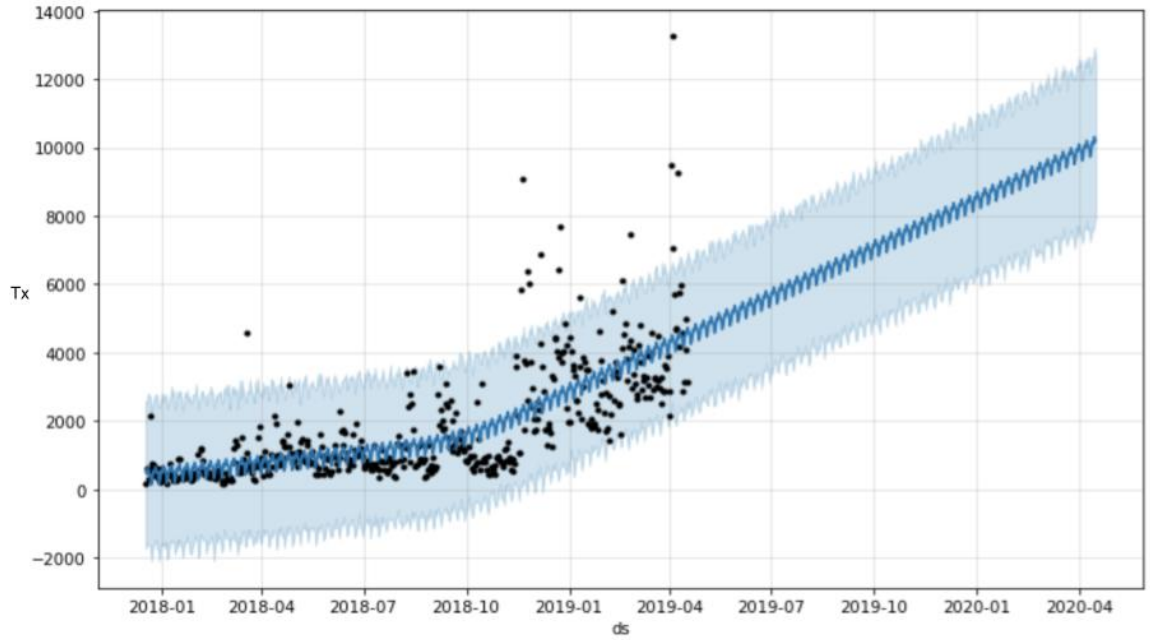

Figure 5.1: Dai Transaction Volume and Trend

data. In particular, diverse research [31][2][37][1] has been conducted to ensure the anonymity of tokens at the decentralized application layer without a significant change in Ethereum protocol using the turing completeness of smart contracts. However, such proposals are more suitable for layer-2(Plasma) than layer-1 (Ethereum) due to scalability issues in the following areas.

- A data structure that proves ownership of separate tokens such as Note is recorded in a smart contract.
- Smart contracts perform zero-knowledge proof verification of transactions.

Note is ownership of encrypted and hashed tokens, and each Note holds information about i) the owner, ii) the Note's balance. For transactions, the Note's owner burns and splits existing Notes to create new Notes. If it is assumed that n number of transactions causes m number of ownership transfer, the size of the Notes to be recorded increases exponentially(mn). Zether, ZETH, AZTEC, and ZKDai utilize smart contract objects as databases[6], so the storage costs will also increase exponentially.

The ZK Proof that proves that the ownership of Notes has been transferred correctly is verified via smart contract, and the gas required for verification is at least 2 million to 7 million depending on the implementation[2][31][1]. Based on the gas limit of 8 million gas per block in Ethereum, It is difficult to include more than four Note transfer transactions (1 or more, depending on implementation) in one block.

[6]ZETH uses MTree, merkle tree implemented as a smart contract, to store Note, and ZKDai uses two arrays to manage such Note data.

Since the Block Gas Limit of Tokamak Plasma is more than 300 million gas [32], more than 30 times the same Note transfer transaction can be included in one block, and the stamina also reduces the user's financial burden regarding the transaction itself. Furthermore, it can scale by adding a separate encryption and arithmetic operator to new opcode of the Plasma EVM for improving verification.

5.2.1.2 Quorum-based Plasma

JP Morgan's Quorum is a private blockchain based on Ethereum implementation (go-ethereum). A unique point of Quorum nodes is that they manage a private state in which only designated nodes are shared within the network. If private transactions that a user does not want to be disclosed on this network are generated, the disclosure level of the transactions will be adjusted while sharing data through unidirectional communication between pre-designated nodes, which is called constellation[13].

The Quorum chain can also be plasmified through Tokamak protocol. In this case, plasma contract is divided into two parts: one to record public transactions and state hashes, and one to record private transactions and state hashes. However, in this case, the challenge related to the state transition that occurs through the private transaction should be made available only to the designated challenger.

In this case, it is important to design governance which determine the challengers. It is also possible, for example, for an initial operator to decide without separate elective governance, and also by voting with DApp tokens used on the Plasma chain. The Tokamak Network does not intervene in this type of challenger election governance. However, if the elected challenger tries to win a verification game via predefined verifier contract through the challenge, the chain staking of the operator is slashed and awarded to the challenger.

Note that some of the transaction and state values may be exposed during the verification game. This is because the verification game takes place in Ethereum, not in the plasma chain. In this case, a separate state verification method is required instead of a verification game. In the process, zero-knowledge proof can be a handy method. This is because zero-knowledge proof can be used to verify that the state transition has been executed correctly by only using proof and the state root hash value.

5.2.2 Cloud Storage

Ethereum records any state value that is permanently stored and pays large costs to modify it. This is because the process itself is a burden to recalculate the state merkle information[18]. In addition, if the size of the block and sync state data to become a full node is too large, it becomes difficult to maintain the decentralization of the platform. Because of this, Ethereum has evolved to use protocols such as SWARM and IPFS to store large amounts of data.

However, because the pure IPFS and SWARM protocols themselves do not have an incentive layer, it is imperative to make this part separate from Ethereum(e.g. Filecoin), and the Oracle-related issue of referencing data outside the blockchain is not completely resolved.

Plasma chain with high throughput and less burden with storing relatively large data can be an alternative to this. By deploying a smart contract in the plasma chain that acts as a database schema, and putting binary data into the state variables managed by this smart contract, the plasma chain becomes an excellent data storage. This type of storage uses a plasma protocol, which eliminates the need for an incentive layer, and also can prevent the problems of data availability and risk of data tampering, as well as oracle problems.

5.3 Derived Businesses

5.3.1 Fee Loan Market

The plasma of Tokamak Network improves the structure in which the users pay for each transaction directly in ether (ETH), making it possible for third party delegation of transaction fees. The service providers themselves can become delegators by depositing a certain amount of TON to pay fees instead of users. It can make a special user experience with no fees.

To reduce the fee burden for users, the service provider has two choices. The first one is that service providers themselves become chain operators to lower the Minimum Gas Price(MGP). The second choice is to rent another user's TON and use it as a fee for a certain period.

First one would completely eliminate the fee burden, but it can be vulnerable to the DoS attack. It is desirable for providers to rent resources paying interests so that they can reduce the burden from users.

On the other hand, fee loans can be provided in two ways.

1. TON(TON, Stamina) loans in Ethereum
2. TON(TON, Stamina) loans in the Plasma chain

In the first case, the owner of the TON in Ethereum lends the fee resources through the chain operator. A separate contract deployed to Ethereum allows users to deposit TON for the purpose of lending. The chain operator provides the service providers with this, and receive fees from them to pay interest to depositors. If the service provider operates the plasma chain for oneself, one can pay the interest directly. It can use the DEX protocol, which has built-in liquidity similar to that of Bancor, in the process of opening the chain to automate these transactions if necessary.

In the second case, a service such as chintai[7] and rex[8] of EOS is directly implemented in each Plasma chain. It can create a fee market that is traded between users, so that TON borrowers can leverage service usage without purchasing large amounts of TON. In the case of TON lenders, it is possible to generate interest income by holding TON by lending it to users who need TON.

Anyone can open a fee exchange in the plasma chain, and it is possible to use ForkDelta[9], which is offered as open-source, or to utilize other types of decentralized exchanges already implemented.

[7] https://eos.chintai.io/exchange/
[8] https://eosrex.io/
[9] https://github.com/forkdelta/

5.3.2 Plasma operator who submits empty blocks(Plasma mining pool)

The operator receives newly issued TON when committing plasma blocks to the root chain. If the market value of the TON issued is greater than the market value of transaction fees to Ethereum, the operator generates a net profit on the operation of Tokamak Plasma chain. (In the opposite case, a net loss occurs.)

If profit is generated only through plasma operation, the operator can create an empty block that does not include transactions and commit it to the root chain. Because there may be other reasons for submitting empty blocks, we cannot determine its validity through the fact that the block is empty. Therefore, if the chain is operated purely for capital gains, there may be a lot of operators who commit and create empty blocks in a period of high profitability. In addition, in the case of users who have a small amount of TON or who is burdened with the complexity of generating an empty block in the plasma chain, it is possible to delegate TON to an operator who submits empty blocks to share token seigniorage. At this time, the plasma chain is similar to the mining pool of PoW in which the hash power is collected to share block rewards.

6. OTHER ISSUES

6.1 Ethereum 2.0 and the Tokamak Network

Plasma is basically a layer-2 solution that uses Ethereum as the base layer. Current Ethereum 1.0 will be upgraded [30] to the 2.0, and plasma also will be affected by the upgrade. However, in the point of view of layer-1, layer-2 is considered as a smart contract (decentralized application). Since the upgrade to 2.0 is about the protocol itself, the effects on plasma are limited [26]. However, the finality and verification of plasma blocks are directly related to the finality and performance of the base layer. Many of the technologies used in Ethereum 2.0 can provide Tokamak Plasma with various features.

6.1.1 Proof of Work vs Proof of Stake

Proof of Work algorithm called modified GHOST protocol[1] is used as consensus in current Ethereum. Reorganization means that canonical chain is changed in the process of fork choice. If blocks are reorganized, transactions included in those blocks can be cancelled. The following scenario describes situations in which blocks can be reorganized.

- User A attempts to Enter 100 tokens.
- A sends transaction for enter request in Ethereum.
- Once the enter request is processed, 100 tokens will be burned in Ethereum and minted in the plasma chain.
- If blocks are reorganized and the transaction related with the enter request is cancelled in Ethereum, burned tokens will roll back but minted tokens will still remain in the Plasma chain.

Such reorganization can cause potential double spending, and for this reason, PoW cannot assure the finality of blocks. In Tokamak Network, in order to reflect enter/exit request in the Plasma chain, it needs some time to minimize the double spending condition.

On the other hand, the Proof of Stake(PoS) of Ethereum 2.0 guarantees the finality of the block by setting checkpoints and finalizing blocks at every checkpoint[11]. There is no reorganization of

[1] It adopts a method in which the modified GHOST protocol selects the main chain that has a large number of blocks included in the subtree.

blocks in PoS. However, in order for blocks to be confirmed, the stakeholders must vote. During voting period, it is hard to immediately reflect enter/exit requests in the plasma chain. In conclusion, requests must be reflected after a certain period of time in PoS. However, in the case of PoS, blocks are finalized after voting. It makes it easy to have stability than PoW, which needs to wait for a certain period of time for request processing.

6.1.2 eWasm

eWasm is one of the major projects included in Ethereum 2.0 roadmap and aims to port Web Assembly to Ethereum. Web Assembly is designed to effectively compile relatively low-level languages such as C, C++, and RUST. With Wasm, code written in multiple languages on the web can be run at near its original speed.

If eWasm is applied, we will have better performance as the existing smart contract execution model EVM(Ethereum Virtual Machine) improves. In addition, smart contracts can be developed with eWasm-supported programming languages(C, C ++, RUST, Go). Another important advantage is that eWasm is not a stand-alone project and is supported by a huge community called Web Assembly. In this process, Tokamak Plasma is also affected, and the detailed contents are as follows.

6.1.2.1 Improvement of TPS(Transactions Per Second) in Tokamak Plasma

Tokamak Plasma can be optimized for eWasm environment. The TPS improvement effect of introducing eWasm in Tokamak Plasma can be greater than in Ethereum. The process of performance improvement in the introduction of eWasm in Ethereum can be summarized as follows. (Assuming that Block Gas Limit is fixed, and Gas Table, which defines amount of gas consumed per computation, is adjusted).

- In Ethereum, block mining time is determined by consensus.
- If eWasm improves computing power, more transactions can be included in one block.

Since block mining times are determined by consensus in Ethereum, there is no guarantee that TPS will be improved by the same degree as computing power being improved.

On the other hand, if eWasm is introduced in Tokamak protocol,

- Like Ethereum, the computing power is improved and more transactions can be included in one block.
- Since there is no consensus in Tokamak Plasma, the block mining time is not determined by consensus but is determined by the amount of data to be processed and computation speed.
- Therefore, assuming that the amount of data to be processed is fixed, if the computation speed is increased, the block mining time will be improved.

Therefore, the improvement of the TPS in this process is relatively larger than that of Ethereum.

6.1.2.2 Standard Library

One of the main goals of eWasm project is to enable writing smart contracts in existing languages. It can provide developers with many of the existing resources to develop smart contracts. For example, developers do not need to build a standard library, instead they can import libraries and deploy it on blockchain. However, since transactions in Ethereum cannot exceed the Block Gas Limit, all standard libraries created cannot be deployed without restriction. Because the Gas Limit of Tokamak Plasma can be increased to the required level, developers will have a much wider choice of libraries.

6.1.2.3 Application of eWasm to the Plasma Chain

Computation challenge model must be changed after eWasm is introduced in Tokamak Plasma. To verify state transition of eWasm, we should be able to use both EVM verifier contract and eWasm verifier contract, protocol challenge of Tokamak Plasma must be newly implemented.

In Tokamak Plasma, solEVM contract, which is modeling EVM in solidity, is used for computation challenge to verify state transtion. After introducing eWasm to Tokamak Plasma, spcific contract like solEVM must be implemented to verify state transition of eWasm.

6.2 Scalability of Plasma Blockchain

If users and transactions increase in the plasma chain, it will face the same scalability issues Ethereum currently has. In such a case, we can extend plasma to a tree structure[29] using turing completeness, which is an advantage of Tokamak Plasma (Figure 6.1). The layer-2 plasma chain will be the child of the layer-1 chain, and will be the parent of layer-3 plasma chain.

6.3 Diversity of Plasma Chain

Plasma chain contains more features than the current EVM. As a simple example, pre-compiled contracts or additional opcodes can be added to the plasma chain. Note that verifier contract which can verify state transition using newly added features must be implemented in the root chain. However, it should be noted that the newly added features can restrict the requestable contract in the process of reflecting states. Examples of plasma chain optimized for specific purpose are as follows:

- Plasma chain with various cryptographic computations added
- Plasma chain supporting various algebraic and mathematical statistics computations
- Plasma chain applying alternative state transition model (alternative virtual machine to EVM)
- Plasma chain with experimental fee model introduced

Due to the ability to easily implement and test various features, Tokamak Plasma can also be used as a means to test new features of future Ethereum.

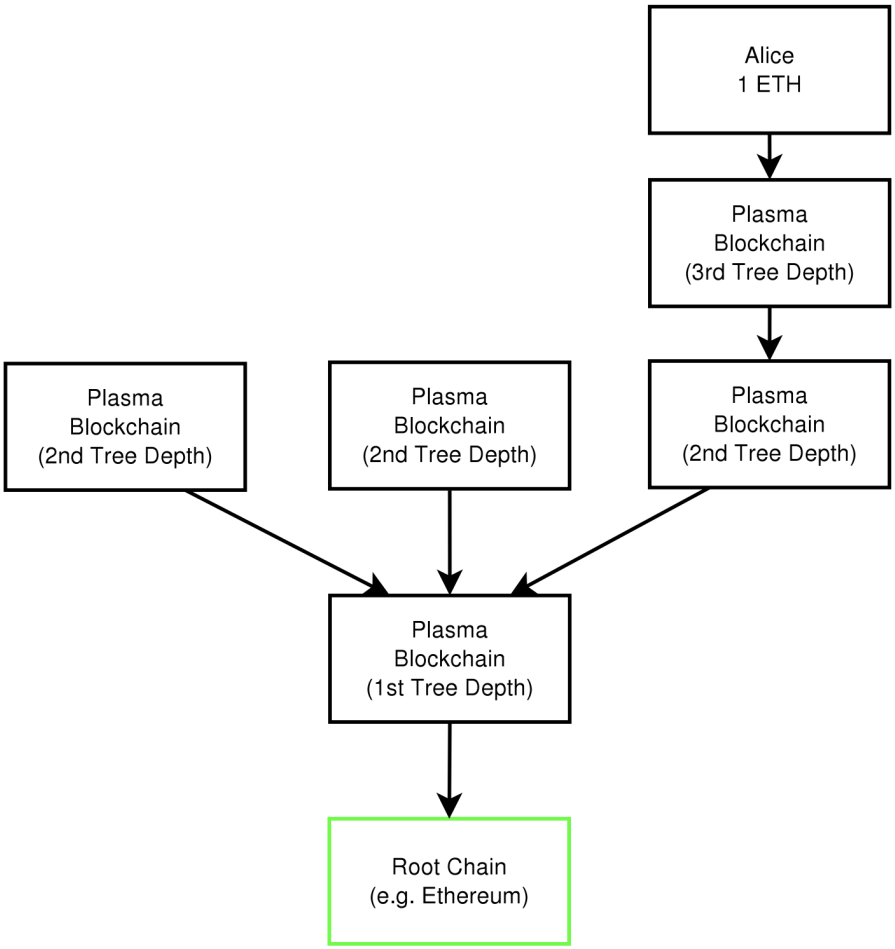

Figure 6.1: Plasma Tree [Source: Plasma Whitepaper]

7. CONCLUSION

Tokamak Network is intended to connect various turing complete plasma chain to Ethereum, with a purpose to improve scalability and usability of Ethereum. With Tokamak Protocol, we can connect turing complete plasma chain with various features implemented through the validator contract deployed on the root chain. Developer customized rules for the enter/exit of data enables trustless state exchange between chains. Such a turing complete Tokamak Plasma chain can be used in a variety of areas such as decentralized exchanges, games, wallets, payments, data storage, stable coin, etc. The protocol can also ensure the privacy of data in blockchains.

In this process, the Tokamak Network token(TON) is used for incentive and disincentive such as token seigniorage, chain staking and challenges. This economic model will serve as a driving force for operators to behave properly and maintain decentralization.

The "verification of correct state transition" in Tokamak Protocol can be used to create platforms optimized for various domains and industries. It can simply make consistent state transitions in a decentralized way without a separate layer or centralized method to exchange data between chains. We believe that Tokamak Plasma will expand the application areas of traditional plasma, which has been used only for the specific purpose of token transfer, so that it can create many kinds of services in the financial and non-financial areas originally targeted by Ethereum.

APPENDIX

.1 Terms

.1.1 GENERAL

- Ethereum : Ethereum , Ethereum public chain
- Tokamak Plasma chain : Tokamak Network Plasma chain, Plasma chain created via Tokamak protocol, and Plasma EVM is used as the core.
- Root chain: Parent chain. It monitors and evaluates the state transformation process of the plasma chain, which is a child chain.
- Plasma Chain: A child chain of the root chain. It is subject to the state transition constraints of the root chain.
- Plasma operators: The main body that operates the Tokamak Plasma chain, the plasma block miners
- Service Providers: AA (Autonomous Agents), Decentralized Autonomous Organizations (DAO), Decentralized Organizations (DO), Decentralized Autonomous Corporations (DAC), and Decentralized Corporations (DC)[1] that operate services on the Tokamak Plasma chain.
- Users: Users of the plasma blockchain and services with Ethereum accounts
- State Transition: A change in the account state that results from a transaction.
- Challenge: A coordination process to correct a block submitted in the Tokamak Plasma chain if it is not valid
- Challenger: A user who engages in a challenge

.1.2 SYSTEM CONFIGURATION

- State reflection: state transition due to a request or null-address.

[1] https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

- Enter: Transfer of account storage (crypto assets, etc.) from Ethereum to the Tokamak Plasma chain.
- Exit: Transfer of account storage (crypto assets, etc.) from the Tokamak Plasma chain to Ethereum.
- Commit: The act of plasma chain submitting a summary of the block to the root chain.
- Verification: The process of determining whether the state of a plasma block is valid. Tokamak Plasma determines the validity of a plasma block through True-bit like verification game (= challenge).
- Verifier: A smart contract that determines the validity of state transition.
- Continuous Rebase : Data availability solution used in Plasma EVM
- Verification Game: Verification process through interaction between a challenger, verifier, and operator
- Request: A transaction to request a state reflection between the root chain and the plasma chain.
- Request Transaction: Transaction requesting entry and exit
- Requestable Contract: A smart contract that defines an enter and exit interface.
- Requestable Variable: Smart contract variables that can enter and exit
- Escape Request: A form of request transaction that is processed with high priority to ensure data availability in the Plasma EVM.
- Rootchain Contract: This is a smart contract implemented in the root chain, which plays the role of managing the chain stakes, verifications, and requests.
- Null-Address: Ethereum account with address 0x00..00
- Minimum Gas Price: The minimum gas price of a transaction included in the plasma chain, as specified in the root chain.
- Block Withholding Attack: The act of a plasma operator hiding the contents of a plasma block.

.1.3 ECONOMIC MODEL AND OTHER

- TON: Tokamak Network token (ERC20) issued to Ethereum. Entered TON is used as transaction fees and plasma chain stakes.
- Chain staking: TON tokens staked by an operator to operate the Tokamak Plasma chain, which are reduced when challenged.

- Enter staking: TON tokens entered into the Tokamak Plasma chain by a user
- Stamina: A unit of transaction fee that is payable in TON, certain transaction senders can send transactions within the stamina limit.
- Fee Delegators: Users who delegate fees in Tokamak Plasma
- Delegatee: Delegatees bear the transaction fees of the delegators within their stamina limit.
- Stamina Pair: When a relationship between a delegatee and delegator is formed, these two accounts are referred to as a stamina pair.
- Oracle: The act of recording external data within the blockchain.
- Oracle Transaction: A transaction that performs Oracle tasks.

References

[1] Arpit Agarwal. *ZkDai—Private DAI transactions on Ethereum using Zk-SNARKs*. URL: https://medium.com/@atvanguard/zkdai-private-dai-transactions-on-ethereum-using-zk-snarks-9e3ef4676e22. (accessed: 05.26.2019).

[2] Benedikt B¨unz et al. *Zether: Towards Privacy in a Smart Contract World*. URL: https://crypto.stanford.edu/~buenz/papers/zether.pdf.

[3] Johann Barbie. *Plasma Leap - a State-Enabled Computing Model for Plasma*. URL: https://ethresear.ch/t/plasma-leap-a-state-enabled-computing-model-for-plasma/3539. (accessed: 04.28.2019).

[4] block.one. *EOS.IO Technical White Paper v2*. URL: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.

[5] Vitalik Buterin. *A Next-Generation Smart Contract and Decentralized Application Platform*. URL: https://github.com/ethereum/wiki/wiki/White-Paper. (accessed: 04.28.2019).

[6] Vitalik Buterin. *Fixed fees aren't that bad*. URL: https://ethresear.ch/t/fixed-fees-arent-that-bad/935. (accessed: 05.04.2019).

[7] Vitalik Buterin. *Layer 1 Should Be Innovative in the Short Term but Less in the Long Term*. URL: https://vitalik.ca/general/2018/08/26/layer_1.html. (accessed: 04.28.2019).

[8] Vitalik Buterin. *Minimal Viable Plasma*. URL: https://ethresear.ch/t/minimal-viable-plasma/426. (accessed: 04.28.2019).

[9] Vitalik Buterin. *Plasma Cash: Plasma with much less per-user data checking*. URL: https://ethresear.ch/t/plasma-cash-plasma-with-much-less-per-user-data-checking/1298. (accessed: 04.28.2019).

[10] Vitalik Buterin. *The Meaning of Decentralization*. URL: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. (accessed: 05.13.2019).

[11] Vitalik Buterin and Virgil Griffith. *Casper the Friendly Finality Gadget*. URL: https://arxiv.org/abs/1710.09437.

[12] Aiden Park Carl Park and Kevin Jeong. *Plasma EVM*. URL: http://tokamak.network/kr/tech-paper.pdf.

[13] jp morgan chase. *quorum*. URL: https://github.com/jpmorganchase/quorum. (accessed: 05.14.2019).

[14] CryptoKitties. *Herding one-million cats*. URL: https://medium.com/cryptokitties/herding-one-million-cats-7dbec6c77476. (accessed: 04.28.2019).

[15] Rasmus Dahlberg, Tobias Pulls, and Roel Peeters. *Efficient Sparse Merkle Trees*. URL: https://eprint.iacr.org/2016/683.pdf.

[16] Philip Daian et al. *Flash Boys 2.0 : Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges*. URL: https://arxiv.org/pdf/1904.05234.pdf.

[17] Shayan Eskandari, Seyedehmahsa Moosavi, and Jeremy Clark. *Transparent Dishonesty: Front-running Attacks on Blockchain*. URL: https://arxiv.org/pdf/1902.05164.pdf.

[18] *EVM: SSTORE/SLOAD gas costs split into processing and storage costs*. URL: https://github.com/ethereum/EIPs/issues/142. (accessed: 05.05.2019).

[19] *Finite-state machine*. URL: https://en.wikipedia.org/wiki/Finite-state_machine.

[20] FIO. *Blockchain Usability Report*. URL: https://fio.foundation/wp-content/themes/fio/dist/files/blockchain-usability-report-2019.pdf.

[21] Danny Her et al. *Plasma EVM Economics Paper : The Mechanism Design and Economic Philosophy (v.0.9)*. URL: https://hackmd.io/s/rJgPxWYTm#2-%EC%9C%A0%EC%A0%80%EC%9D%98-Exit%EC%97%90-%EB%8C%80%ED%95%9C-Challenge--Exit-Challenge.

[22] Kevin Jeong. *Plasma MVP Audit(Script)*. URL: https://medium.com/onther-tech/plasma-mvp-audit-%EB%85%B9%EC%B7%A8%EB%A1%9D-script-166a2c5012b4.

[23] Kevin Jeong et al. *EVM Compatible Transaction Fee(GAS) Delegated Execution Architecture*. URL: https://hackmd.io/s/SkxNKAXU7.

[24] Kevin Jeong et al. *EVM Compatible Transaction Fee(GAS) Delegated Execution Architecture for Plasma Chain*. URL: https://ethresear.ch/t/evm-compatible-transaction-fee-gas-delegated-execution-architecture-for-plasma-chain/3106.

[25] Ben Jones and Kelvin Fichter. *More Viable Plasma*. URL: https://ethresear.ch/t/more-viable-plasma/2160.

[26] Raul Jordan. *How to Scale Ethereum: Sharding Explained*. URL: https://medium.com/prysmatic-labs/how-to-scale-ethereum-sharding-explained-ba2e283b7fce. (accessed: 05.13.2019).

[27] Carl Park. *CryptoKitties in Plasma EVM (KR)*. URL: https://medium.com/onther-tech/cryptokitties-in-plasma-574159c581dc. (accessed: 05.26.2019).

[28] Learn Plasma. *Plasma Cash*. URL: https://www.learnplasma.org/en/learn/cash.html.

[29] Joseph Poon and Vitalik Buterin. *Plasma: Scalable Autonomous Smart Contracts*. URL: https://plasma.io/. (accessed: 04.28.2019).

[30] James Ray. *Sharding roadmap*. URL: https://github.com/ethereum/wiki/wiki/Sharding-roadmap. (accessed: 05.13.2019).

[31] Antoine Rondelet and Michal Zajac. *ZETH: On Integrating Zerocash on Ethereum*. URL: https://arxiv.org/abs/1904.00905.

[32] Thomas Shin. *Plasma EVM Performance Test*. URL: https://medium.com/onther-tech/plasma-evm-%EC%84%B1%EB%8A%A5-%ED%85%8C%EC%8A%A4%ED%8A%B8-ff3a66c7fdaf. (accessed: 05.26.2019).

[33] *Steem : An incentivized, blockchain-based, public content platform*. URL: https://steem.com/steem-whitepaper.pdf.

[34] Jason Teutsch and Christian Reitwießner. *A scalable verification solution for blockchains*. URL: https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf.

[35] Toshi Times. *EOS Stumbles Once More as Speculation Causes RAM Prices to Spike Beyond Affordability*. URL: https://toshitimes.com/eos-stumbles-once-more-as-speculation-causes-ram-prices-to-spike-beyond-affordability/. (accessed: 05.03.2019).

[36] wikipedia. *Mt.$_G$ox*. URL: https://en.wikipedia.org/wiki/Mt._Gox. (accessed: 05.14.2019).

[37] Dr Zachary J. Williamson. *The AZTEC Protocol*. URL: https://github.com/AztecProtocol/AZTEC/blob/master/AZTEC.pdf.

[38] Gavin Wood. *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*. URL: https://ethereum.github.io/yellowpaper/paper.pdf.