Blockchain Kaigi 2023 (BCK23) Program (Final version)

The Integrated Innovation Building (IIB) at the RIKEN Kobe Campus.
October 28th -29th, 2023

October 28th (Sat) Morning

Opening Remarks, including Announcement of Proceedings (9:00-9:10)
Yuichi Ikeda (Kyoto University)

Keynote Speech (9:10-9:50) (Online, West Coast: 27th 17:10, East Coast: 27th 20:10) SC: Yuichi Ikeda (Kyoto University)
(K1) Aanchal Malhotra (Ripple Lab Inc.) [30 min Talk, 10 min Q&A]
"The Future Outlook of the XRPL"

Invited Talks (9:50-11:10) SC: Tetsuo Hatsuda (RIKEN iTHEMS)
(I1) Victor Fang (AnChain.AI) [30 min Talk, 10 min Q&A]
"How Artificial Intelligence Disrupts Status Quo of Web3 Security"
(I2) Tsuyoshi Ide (IBM Thomas J. Watson Research Center) [30 min Talk, 10 min Q&A]
"Decentralized Collaborative Machine Learning Framework with Democracy, Diversity, and Privacy"

General Talks (11:10-12:00) SC: Tetsuo Hatsuda (RIKEN iTHEMS)
(G1) Claudio J. Tessone (University of Zurich) [15 min Talk, 10 min Q&A]
"Deceptive Trading in Decentralised Finance and NFT Markets: A blockchain analytics approach"
(G2) Hideaki Aoyama (Kyoto University/RIETI) [15 min Talk, 10 min Q&A]
"Where are the Cryptoasset nodes located? -Eye-Map identification of the longitude of nodes-"

Lunch break (12:00-13:40)

October 28th (Sat) Afternoon

General Talks (13:40-14:55) SC: Akihiro Fujihara (Chiba Institute of Technology)
(G3) Masaki Sakurai (Chiba Institute of Technology) [15 min Talk, 10 min Q&A]
"Proposal of Fact-Checking Registry using Bitcoin SV"

(G4) Yu Kimura (Interoperability Labs Ltd.) [15 min Talk, 10 min Q&A]
"Theory of EDISON-X order automation using several machine learning approaches"
(G5) Ryosuke Nakazawa (Chiba Institute of Technology) [15 min Talk, 10 min Q&A]
"Proposal of fact-checking DAO and its experimental trials"

Break (14:55-15:15)

General Talks (15:15-16:30) SC: Claudio J. Tessone (Univ. of Zurich)
(G6) Shinya Hirata (Kyushu University) [15 min Talk, 10 min Q&A]
"Bitcoin Transactions Stochastic Model Simulation"
(G7) Zheng Nan (Yamanashi Gakuin University) [15 min Talk, 10 min Q&A]
"How did bitcoin markets evolve: A comparison with the USD/EUR foreign exchange spot market?"
(G8) Abhijit Chakraborty (Kyoto University) [15 min Talk, 10 min Q&A]
"Dynamic relationship between XRP price and correlation tensor spectra of the transaction network"

October 29th (Sun) Morning

Keynote Speech (9:00-9:40) (Online, West Coast: 28th 17:00, East Coast: 28th 20:00) SC: Tomoyuki Shirai (Kyushu University)
(K2) Wakefield Scott Stornetta (Creative Destruction Lab) [30 min Talk, 10 min Q&A]
"The Blockchain: Past, Present, and Future"

Invited Talks (9:40-10:20) SC: Tomoyuki Shirai (Kyushu University)
(I3) Hiroyoshi Miwa (Kwansei Gakuin University) [30 min Talk, 10 min Q&A]
"Developing human resources capable of using blockchain technology"

General Talks (10:20-11:35) SC: Yoshimasa Hidaka (KEK Theory Center)
(G9) Taishi Nakai (Kyoto University) [15 min Talk, 10 min Q&A]
"Towards Mathematical Formulation of the Blockchain Trilemma"
(G10) Gopikrishnan Muraleedharan (Macquarie University) [15 min Talk, 10 min Q&A]
"Proof-of-work consensus by quantum sampling"
(G11) Tsuyoshi Hirayama (IBM Japan, Ltd.) [15 min Talk, 10 min Q&A]
"Breakthrough of Crypto Currency Derivatives and Quantum Finance Utilization"

Lunch break (11:35-13:15)

October 29th (Sun) Afternoon

Invited Talk (13:15-15:15) SC: Abhijit Chakraborty (Kyoto University)

(I4) Shoji Kasahara (Nara Institute of Science and Technology) [30 min Talk, 10 min Q&A]
“Modeling and Analysis of Bitcoin Mining Mechanism –A Queueing Theoretical Approach–”
(I5) Wang Qin (CSIRO) [30 min Talk, 10 min Q&A]
“Tokenomics and Beyond”
(I6) Shingo Fujimoto (Data & Security Research laboratory, Fujitsu Limited.) [30 min Talk, 10 min Q&A]
“Smart contract-based automated token economy”

Break (15:15-15:35)

General Talks (15:35-16:00) SC: Yuichi Ikeda (Kyoto University)

(G12) Akihiro Fujihara (Chiba Institute of Technology) [15 min Talk, 10 min Q&A]
“Investigating the probability distribution of average block time in proof-of-stake consensus algorithm using extreme value theory”

Invited Talk (Company Session in Japanese) (16:00-17:00) SC: Yuichi Ikeda (Kyoto University)

(I7) Syuga Yamamoto (Gaiax Co.Ltd) [20 min Talk, 10 min Q&A]
「日本に馴染む DAO の形」
(I8) Mayu Yokoyama (Nippon Yusen Kabushiki Kaisha) [20 min Talk, 10 min Q&A]
「日本郵船　社内有志 DAO 活動の紹介」

Closing Remark, including Announcement of Proceedings (17:00-17:10)

Tetsuo Hatsuda (RIKEN iTHEMS)

Deceptive Trading in Decentralised Finance and NFT Markets: A blockchain analytics approach

CLAUDIO J. TESSONE, UZH Blockchain Center, University of Zurich

Decentralised finance (DeFi) platforms and Non-Fungible Token (NFT) markets have introduced groundbreaking mechanisms for trading and investment, gaining significant traction and attention. Yet, they are not without challenges. A lack of regulatory oversight has led to a surge in deceptive trading practices, posing a risk to both liquidity and market stability. This talk will focus on deceptive activities such as "Rug-pull" attacks in DeFi platforms like Uniswap and wash trading in NFT markets.

Uniswap, as the leading decentralised exchange with an Automated Market Maker (AMM) mechanism, offers enormous opportunities but also exposes investors to various attacks. By applying blockchain analytics, we detect Rug-pull events by replaying each mint, swap, and burn event, further examining the change ratio in primary token reserves. We demonstrate how Rug-pull attacks affect not only the price and liquidity of individual liquidity pools but also have broader implications on the market's stability and network connectivity.

Similarly, in NFT markets, deceptive tactics like wash trading distort genuine market activity and artificially inflate prices. We introduce a novel algorithm to identify wash trading by analysing the blockchain's chain of ownership. The algorithm detects multi-layer wash trading patterns and identifies traders who manipulate prices repeatedly.

The talk aims to bridge these two realms by leveraging blockchain analytics to detect deceptive trading practices. By employing extensive data analysis, we illuminate the vulnerabilities in both DeFi and NFT markets, striving for a more transparent, safer, and equitable trading environment. Our findings point to the critical need for community-driven oversight and potentially, targeted regulation, to mitigate the risks associated with these innovative but vulnerable digital asset spaces.

Additional Key Words and Phrases: Decentralised Finance, Non-Fungible Tokens, Blockchain Analytics, Deceptive Trading, Market Integrity

Reference:
Claudio J. Tessone. 2023. Deceptive Trading in Decentralised Finance and NFT Markets: A blockchain analytics approach. 1, 1, Article 1 (September 2023), 1 pages.

Where are the Cryptoasset nodes located?

— Eye-Map identification of the longitude of nodes —[*]

Hideaki Aoyama[†‡], Wataru Souma[⋆‡], Yoshi Fujiwara[⋆], and Yuichi Ikeda[‡]

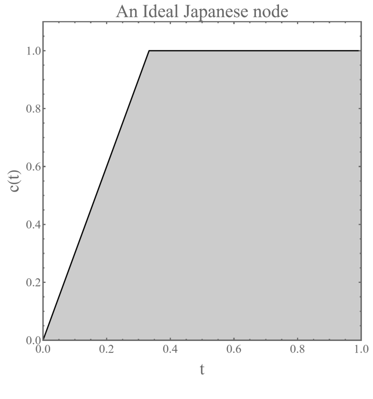
[‡]GSAIS, Kyoto University, Kyoto, Japan
[‡]RIKEN, iTHEMS, Wako, Japan
[⋆]Faculty of Data Science, Rissho University, Kumagaya, Japan
[⋆]University of Hyogo, Kobe, Japan

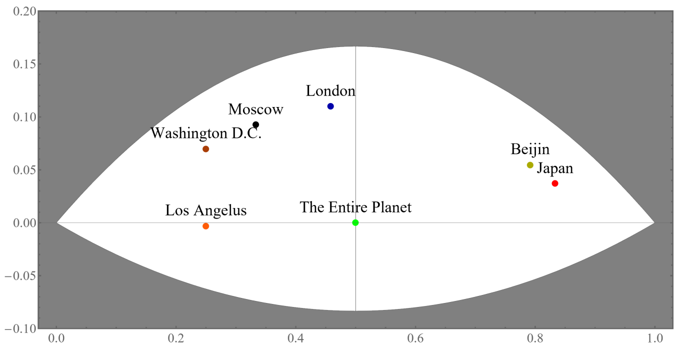
Transaction records available for many cryptoassets contain time-records (in UTC). By collecting them for a particular user, we can draw a time-portrait of the user's activity, which may reveal information about the longitude of the user: If the user is located in Japan and does the transactions at a constant rate from 9 a.m. to 5 p.m. in JST, which is 0:00-09:00 UTC, it works as a clear sign of its location.

In order to do this kind of analysis, we use the *Eye-map analysis* recently invented by some of the current authors (HA and SW). This method allows mapping from a monotonically increasing function to a 2-dimensional region, whose position reflects some of the most basic global characterizations of the curve. We propose the application of this Eye-map analysis to the cumulative distribution of the transaction time within a day (or a collection of days, mapped to a single day) as a simple way to obtain a good guess as to the latitude of transaction nodes.

Let us denote the function to be analyzed (cumulative distribution of the transactions) as $c(t)$, where t is a rescaled time that varies from 0 to 1 for 0:00-24:00. Its value is also re-scaled by the total number of transactions during the 24 hour period so that $c(0) = 0, c(1) = 1$. In the case of the Japanese node mentioned above, $c(t)$ behaves as in left figure below.

In Eye-map, the location of this curve is obtained as follows: (i) The horizontal coordinate S is the area of the region below the curve $c(t)$ (the shadowed region in the left figure), $S = \int_0^1 c(t)dt$. (ii) In order to obtain the vertical coordinate A, We first calculate the second moment of $c(t)$, namely, the area below the squared curve $c^2(t)$, $M_2 = \int_0^1 c^2(t)dt$. Then $A = M_2 - (S + 2S^2)/3$. From this construction, all the points obtained from the two-dimensional curves fit within the white regions in the right figure below. The name "Eye Map" comes from the similarity of this white region to the shape of human eye. The points obtained from such calculations of several major cities, including the ideal 9-5 Japanese company mentioned above. are shown in the same figure.





In reality, of course, the transaction nodes behave rather erratically. The central point "The Entire Planet" in this Eye-map is, in fact, the node that does transactions for all 24 hours at a constant rate. In the proposed talk, we will present results containing non-ideal companies, which allow error estimates of the Eye-map estimates of the actual XRP nodes.

[*] Submitted to Blockchain Kaigi 2023 (BCK23)

Proposal of Fact-Checking Registry using Bitcoin SV

Masaki Sakurai, Akihiro Fujihara
Chiba Institute of Technology

Abstract

Fact-checking [1] is gaining attention as an effective countermeasure against the current situation in which disinformation and misinformation on SNS is increasing, making it difficult for citizens to make information judgments. Fact-checking provides accurate information through investigation of sources and verification of authenticity, and organizations such as POLITIFACT [2] collect unverified information and carefully select fact-checking suggestions from clients. These organizations are funded by donations from individuals and organizations to raise operating costs, and if they operate on their own, they are generally free of charge. And while fact-checking can be adept at curbing disinformation and misinformation, it's not easy to ensure that articles are immutable.

In this research, therefore, we propose a system to provide virtual currency compensation from clients based on the evaluation of fact-check content, and construct a fact-check registry that ensures reliability and responsibility using blockchain technology. The blockchain to be used is Bitcoin SV. Bitcoin SV, with a maximum block size of 4GB, is a very large standard, which means it can reduce the processing speed delays and steep fees associated with the increasing number of blockchain users. And because articles in the registry will remain permanently on the blockchain, it will not only preserve historical information and fact-checking results for posterity, but also provide proof of what each fact-checker has done.

We also want to incorporate a design in which we receive fees from clients in cryptocurrency so that fact checkers can cover the operating costs of their activities with the fact checking activities themselves. Therefore, we will hold a fact-checking contest to solve fact-checking problems using a prototype system. Before and after the contest, a questionnaire survey is conducted on the fees sought by the fact checker and the fees offered by the client to clarify the appropriate amount of compensation for the fact checker. Figure 1 shows the results of the questionnaire, with n representing the total number of contestants. Based on the correlation between the compensation offered for fact-checking requests and the compensation sought, it can be estimated that the compensation to be offered by the client is approximately 1100 yen, and it is considered that offering more than this amount would be sustainable for fact-checking activities in the registry.

References

[1]What is fact-checking? https://ifcncodeofprinciples.poynter.org/ (accessed on September 17, 2023)
[2] About POLITIFACT https://www.politifact.com/who-pays-for-politifact/ (accessed on September 17, 2023)

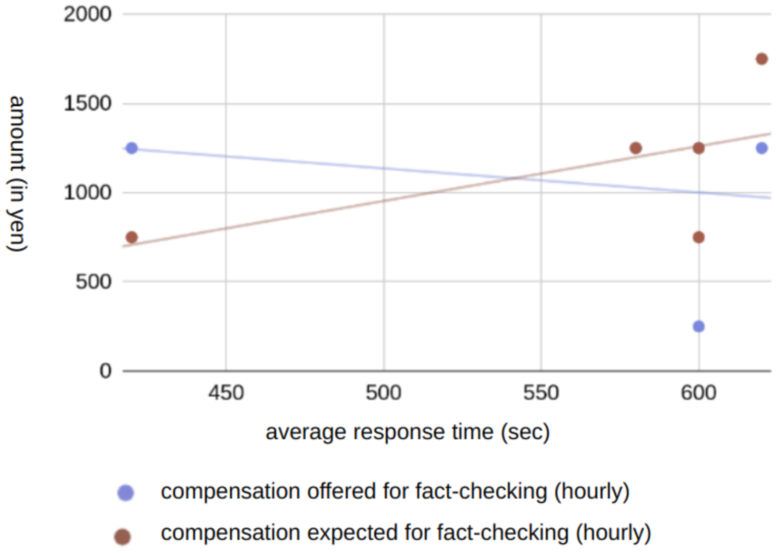


Figure 1, Response time and hourly rate (total number of contestants n = 8)

Theory of EDISON-X order automation using several machine learning approaches

Yu Kimura[1], Sena Omura[1], Yuichi Ikeda[2]

[1]*Interoperability Labs Ltd., Kyoto 602-8061, Japan*
[2]*Graduate School of Advanced Integrated Studies in Human Survivability, Kyoto University, Kyoto 606-8306, Japan*

E-mail: yu.kimura@cauchye.com

(Received September 2023)

Last year, we developed an energy trading system, EDISON-X, that uses blockchain technology to manage the buying and selling of electricity usage rights. 17 dormitory residents at our school conducted a verification experiment on the EDISON-X system, and they provided feedback that the process of daily order creation is cumbersome. Therefore, we have decided to incorporate a mechanism for automating the ordering processes into the EDISON-X system, aiming to optimize electricity trading prices and increase trading volumes. This paper examines what algorithm would be suitable for achieving an effective automatic ordering algorithm in the electricity trading market using the single-price auction mechanism within the EDISON-X system. The algorithms we examined contain several objective functions for optimization and reinforcement learning. This automatic ordering algorithm will be validated through a demonstration experiment in which our school's students will participate, starting in October.

KEYWORDS: energy trading system, blockchain, token, renewable energy, demonstration experiment, hypergraph, persistent homology, machine learning, reinforcement learning

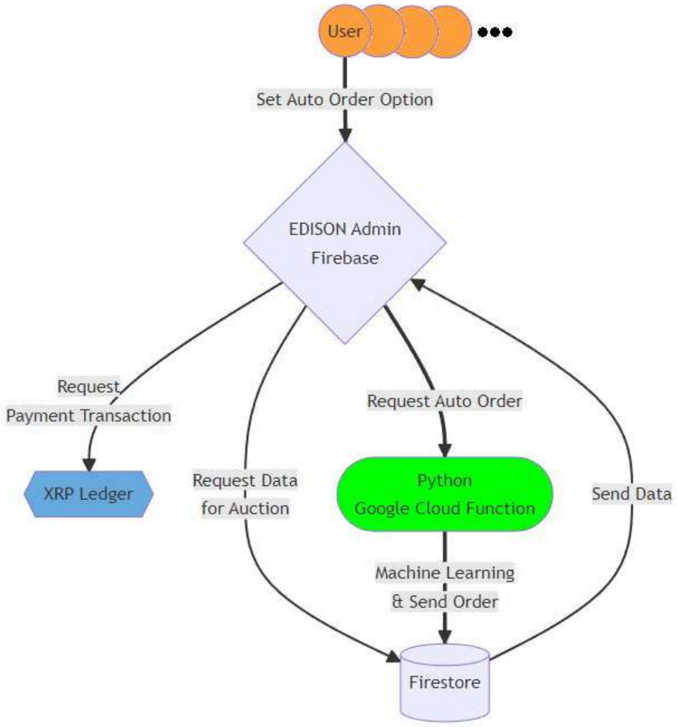


Fig. 1. EDISON-X: Auto Order Configuration, EDISON-X Auto order system is built in Python and runs on Google Cloud. This works as a plugin for EDISON-X, which is built on various technologies and frameworks developed by Google, Ripple Labs, and others as open source.

References

[1] Yuichi Ikeda, et al., "First Demonstration Experiment for Energy Trading System EDISON-X Using the XRP Ledger", https://arxiv.org/abs/2212.02044, December 2022.

Proposal of fact-checking DAO and its experimental trials

Ryosuke Nakazawa, Akihiro Fujihara, Chiba Institute of Technology

Abstract

In recent years, the remarkable progress in the development and spread of the Internet has made it easy for information that is uncertain of its authenticity or disinformation to spread around the world instantly. Especially in SNS, it is not easy to confirm the authenticity of spread information. Even if general users notice errors in information, the indication is not widely accepted.

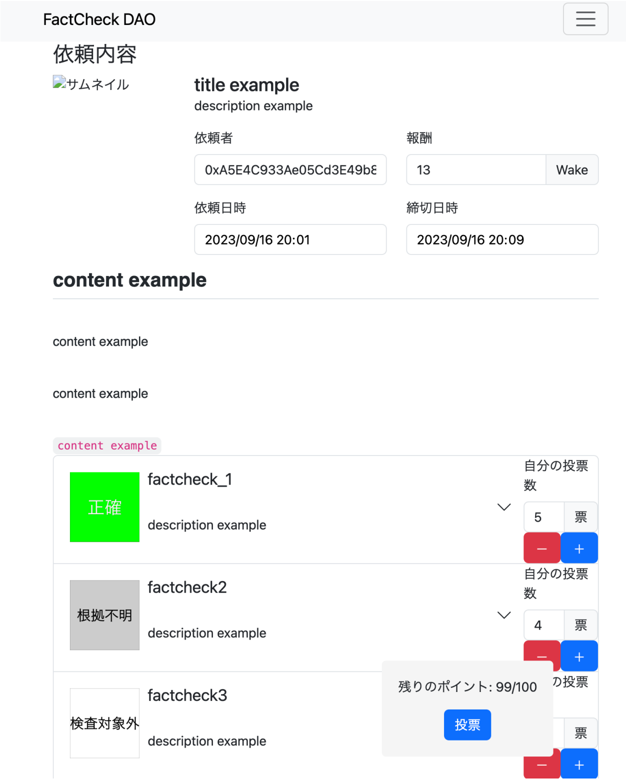
In this background, the role of fact-checking, which verifies authenticity and disseminates accurate information, has become increasingly important. However, most fact-checking is done by those who belong to a particular organization, and the problem is that they are susceptible to bias in the organization's opinion.

To improve this problem, we consider building a new platform where multiple organizations conduct fact-checking independently and publish and share the results. We adopted a decentralized organizational form to maintain diversity and neutrality without relying on the operation of a single organization, and examined the use of decentralized autonomous organizations (Decentralized Autonomous Organization, DAO) [1]. As a result, a fact-checking DAO was proposed and a web platform was prototyped to carry out the activity. Screenshots of the actual interface of this platform are shown in Figs.1 and 2.

We also conducted experiments using the prototype platform to actually launch DAO. In this talk, we report the results of this experiment and future directions.

References

[1] Ethereum Whitepaper https://ethereum.org/en/whitepaper/ (Accessed on September 16, 2023)



FactCheck DAO

依頼内容

サムネイル

title example

description example

依頼者: 0xA5E4C933Ae05Cd3E49bE

報酬: 13 Wake

依頼日時: 2023/09/16 20:01

締切日時: 2023/09/16 20:09

content example

content example

content example

`content example`

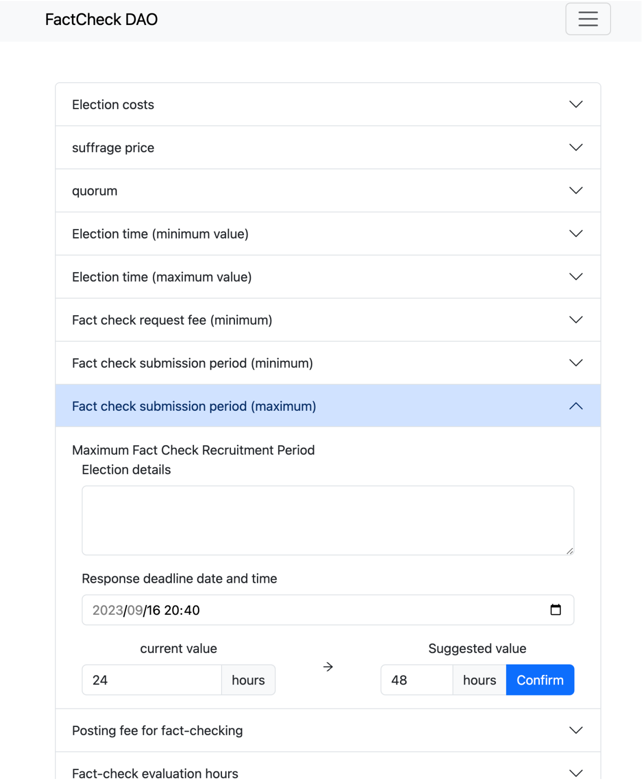
factcheck_1 — 正確 — description example — 自分の投票数 5 票

factcheck2 — 根拠不明 — description example — 自分の投票数 4 票

factcheck3 — 検査対象外 — description example — の投票 票

残りのポイント: 99/100

Fig. 1 Main page for viewing fact-checks results



FactCheck DAO

Election costs

suffrage price

quorum

Election time (minimum value)

Election time (maximum value)

Fact check request fee (minimum)

Fact check submission period (minimum)

Fact check submission period (maximum)

Maximum Fact Check Recruitment Period

Election details

Response deadline date and time: 2023/09/16 20:40

current value: 24 hours → Suggested value: 48 hours

Posting fee for fact-checking

Fact-check evaluation hours

Fig. 2 Changing DAO parameters.

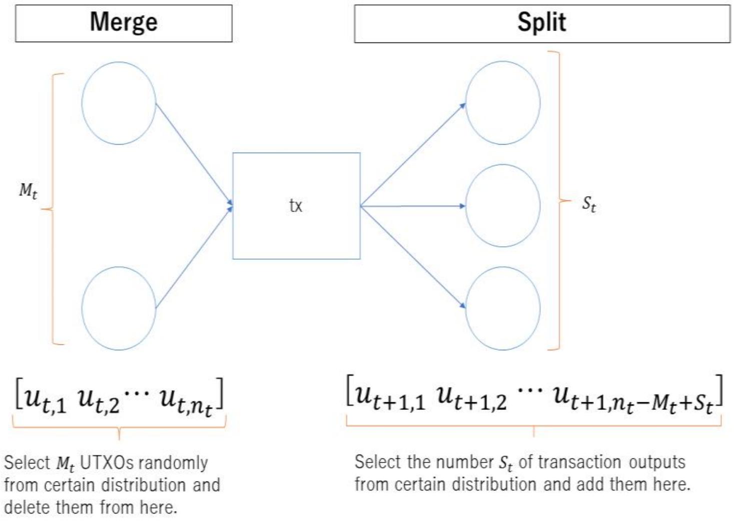
Bitcoin Transactions Stochastic Model Simulation

Presenter: Shinya Hirata (master's student in the Joint Graduate School of Mathematics for Innovations, Kyushu University)
Collaborator: Tomoyuki Shirai (professor at the Institute of Mathematics for Industry, Kyushu University)

We demonstrated the simulation of the UTXOs of Bitcoin to explore the nature of blockchain transactions. We found several properties of transactions. They may help optimize blockchain networks and other research.

There is much research on the nature of cryptocurrencies as a financial asset in inductive approaches. For example, Shaen et al. (2019) comprehensively reviewed them as financial assets. However, there is less research on the nature of Bitcoin transactions in deductive approaches. In this study, we simulated the moves of Bitcoin's UTXOs to analyze their nature in the deductive approach. Focusing on UTXOs enables us to make a simple model and analyze its features. Through our simulations, we can gain valuable insights into the behavior of Bitcoin networks under different conditions.

Our methodologies are as follows. First, we explored the characteristics of Bitcoin transactions from the Bitcoin network data. Second, we made a probabilistic model for UTXOs using the characteristics. Our model expressed a transaction as two processes: Merge and Split. The Merge process selected the number of inputs and the Split process selected that of outputs from certain probability distributions. These distributions have parameters called "Merge Rate" and "Split Rate." Third, we simulated the model with a computer program. Finally, we analyzed the nature of Bitcoin transactions from the model.


Merge
Split
M_t
tx
S_t
$[u_{t,1}\ u_{t,2}\cdots u_{t,n_t}]$
$[u_{t+1,1}\ u_{t+1,2}\cdots u_{t+1,n_t-M_t+S_t}]$

Select M_t UTXOs randomly from certain distribution and delete them from here.

Select the number S_t of transaction outputs from certain distribution and add them here.

We have gained some initial insights. For instance, our simulation results showed that the amounts of UTXOs follow a power law if the Split Rate is larger than Merge Rate.

Since our research is ongoing, we will improve our models by adding various Bitcoin features such as the half-decay period and transaction fees.

References

Shaen Corbet, Brian Lucey, Andrew Urquhart, Larisa Yarovaya, Cryptocurrencies as a financial asset: A systematic analysis, International Review of Financial Analysis, Volume 62, 2019, Pages 182-199.

1. Title of the presentation

How did bitcoin markets evolve: A comparison with the USD/EUR foreign exchange spot market?

2. Author

Zheng NAN
MA, Ph.D. (Economics)

Lecturer of Economics
Global Business & Economics Program Coordinator

International College of Liberal Arts
Yamanashi Gakuin University

F210 iCLA, 2-7-17 Sakaori, Kofu,
Yamanashi 400-0805, Japan

Email: nan.zheng@c2c.ac.jp
Tel: +81 (0)552 24 1976
Mobile: 080-6642-1998

3. Abstract

The US Securities and Exchange Commission (SEC) has been considering converting a NYSE Arca exchange-listed Hashdex Bitcoin Futures ETF into spot Bitcoin ETF (Johnson, 2023). This unprecedented move, if approved, differentiate bitcoins from other cryptocurrencies that are normally viewed as 'securities.' On the other hand, the regulators appear to gradually accept bitcoin-related assets to be traded in regulated markets like other commodities and currencies.

This paper aims to compare the bitcoin markets with the foreign exchange spot market, the biggest global decentralized market. Specifically, two questions are of interests: 1) How did the bitcoin markets perform comparing the foreign exchange spot market, the global decentralized market; 2) How did the bitcoin market evolve historically?

The results show that the bitcoin market has been going through at least three regimes. Hence, three models are proposed to investigate the speed of adjustment in those

three periods. The results show that the separations of regimes help improve model's accuracy and help us understand the history of bitcoin market mechanism comprehensively. (Zheng, 2023)

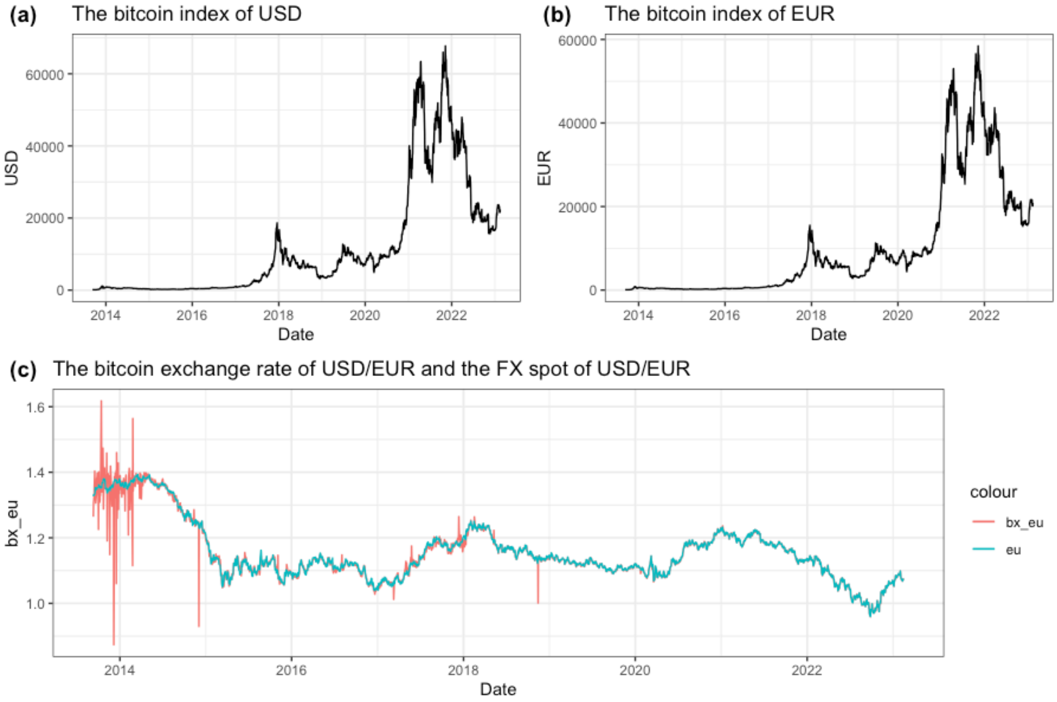


Figure 1. The bitcoin indices of USD and EUR, the derived bitcoin exchange rate of USD/EUR (bx_eu), and the FX spot of USD/EUR (eu) (10 September 2013 – 15 February 2020).

Dynamic relationship between XRP price and correlation tensor spectra of the transaction network

Abhijit Chakraborty[1,2], Tetsuo Hatsuda[2] and Yuichi Ikeda[1]

1 Graduate School of Advanced Integrated Studies in Human Survivability, Kyoto University, 1 Nakaadachi-cho, Yoshida, Sakyo-ku, Kyoto, 606-8306, Japan.

2 RIKEN Interdisciplinary Theoretical and Mathematical Sciences Program, 2-1 Hirosawa, Wako, Saitama, 606-8306, Japan.

The emergence of cryptoassets has sparked a paradigm shift in the world of finance and investment, ushering in a new era of digital assets with profound implications for the future of currency and asset management. A recent study [1] showed that during the bubble period around the year, 2018, the price of cryptoasset, XRP has a strong anti correlation with the largest singular values of the correlation tensors obtained from the weekly XRP transaction networks. In this study, we provide a detailed analysis of the method of correlation tensor spectra for XRP transaction networks [2]. We calculate and compare the distribution of the largest singular values of the correlation tensor using the random matrix theory with the largest singular values of the empirical correlation tensor. We investigate the correlation between the XRP price and the largest singular values for a period spanning two years. We also uncover the distinct dependence between XRP price and the singular values for bubble and non-bubble periods [Fig. 1]. The significance of time evolution of singular values is shown by comparison with the evolution of singular values of the reshuffled correlation tensor. Furthermore, we identify a set of driver nodes in the transaction networks that drives the market during the bubble period using the singular vectors.

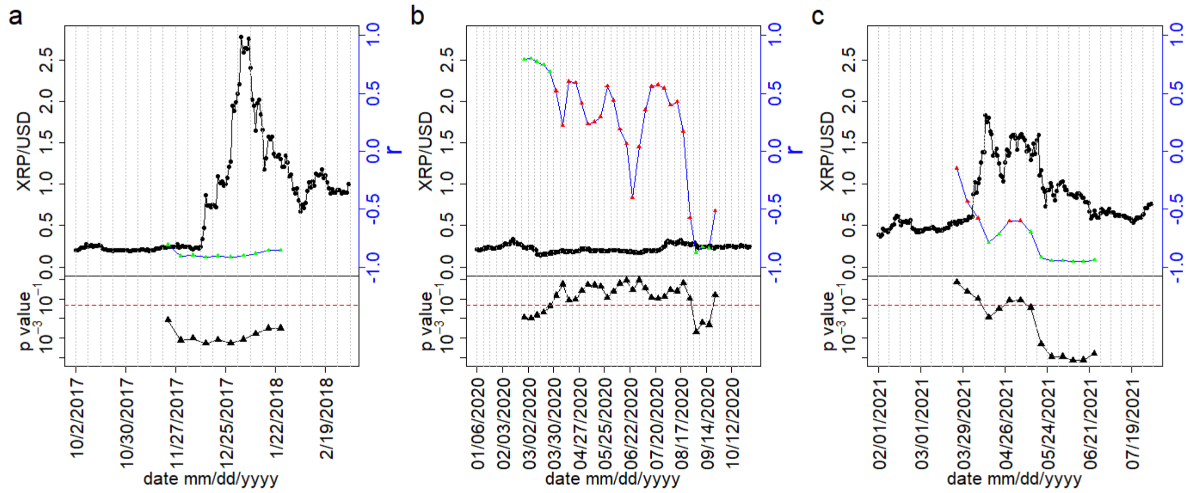


Fig 1: The comparison of daily XRP/USD price with the correlation r(t) between the weekly XRP/USD price, and the largest singular value using a moving window of 9 weeks for three different periods - (a) October 2, 2017- March 4, 2018, (b) January 6, 2020 - November 1, 2020 and (c) February 1, 2021- August 1, 2021.

References

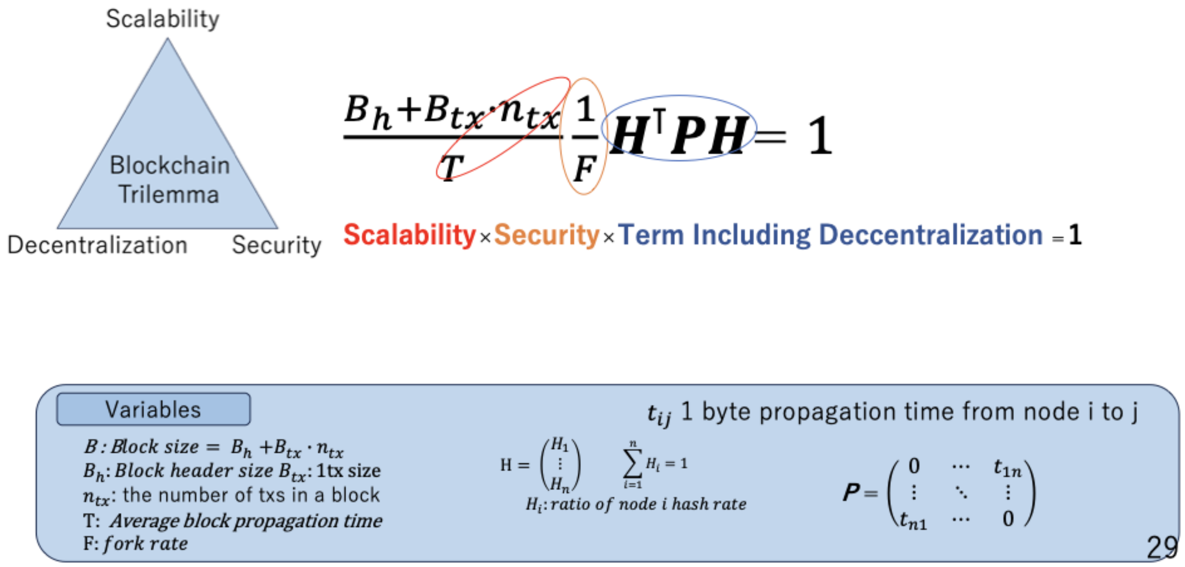
1. Chakraborty, A., Hatsuda, T., & Ikeda, Y. (2023). Projecting XRP price burst by correlation tensor spectra of transaction networks. Scientific Reports, 13(1), 4718.
2. Chakraborty, A., Hatsuda, T., & Ikeda, Y. (2023). Dynamic relationship between XRP price and correlation tensor spectra of the transaction network. arXiv preprint arXiv:2309.05935.

講演タイトル　Towards Mathematical Formulation of the Blockchain Trilemma
講演者　Taishi Nakai (Kyoto University)
共同研究者　Akira Sakurai (Tokyo Institute of Technology) Shiori Hironaka (Kyoto University) Shudo Kazuyuki (Kyoto University)

講演内容の説明

Vitalik Buterin, a co-founder of Ethereum, first discussed the blockchain trilemma in a 2017 blog article. This concept posits that achieving decentralization, scalability, and security all at once in a blockchain is unattainable. Though many have analyzed blockchain efficiency and generally accepted this notion, no mathematical representation for the trilemma has been set forth. In our study, we provide a formula that defines the trilemma for Proof of Work blockchains. Additionally, we outline two strategies to enhance blockchain efficiency within the trilemma's limitations. Moreover, we indicate how we plan to further develop this trilemma formula in the future.

説明を補足する図



$$\frac{B_h+B_{tx}\cdot n_{tx}}{T}\,\frac{1}{F}\,\boldsymbol{H}^{\top}\boldsymbol{P}\boldsymbol{H}=1$$

Scalability × Security × Term Including Deccentralization = 1

Variables

B : Block size $= B_h + B_{tx} \cdot n_{tx}$
B_h: Block header size B_{tx}: 1tx size
n_{tx}: the number of txs in a block
T: *Average block propagation time*
F: *fork rate*

t_{ij} 1 byte propagation time from node i to j

$$\mathrm{H} = \begin{pmatrix} H_1 \\ \vdots \\ H_n \end{pmatrix} \qquad \sum_{i=1}^{n} H_i = 1$$

H_i: *ratio of node i hash rate*

$$\boldsymbol{P} = \begin{pmatrix} 0 & \cdots & t_{1n} \\ \vdots & \ddots & \vdots \\ t_{n1} & \cdots & 0 \end{pmatrix}$$

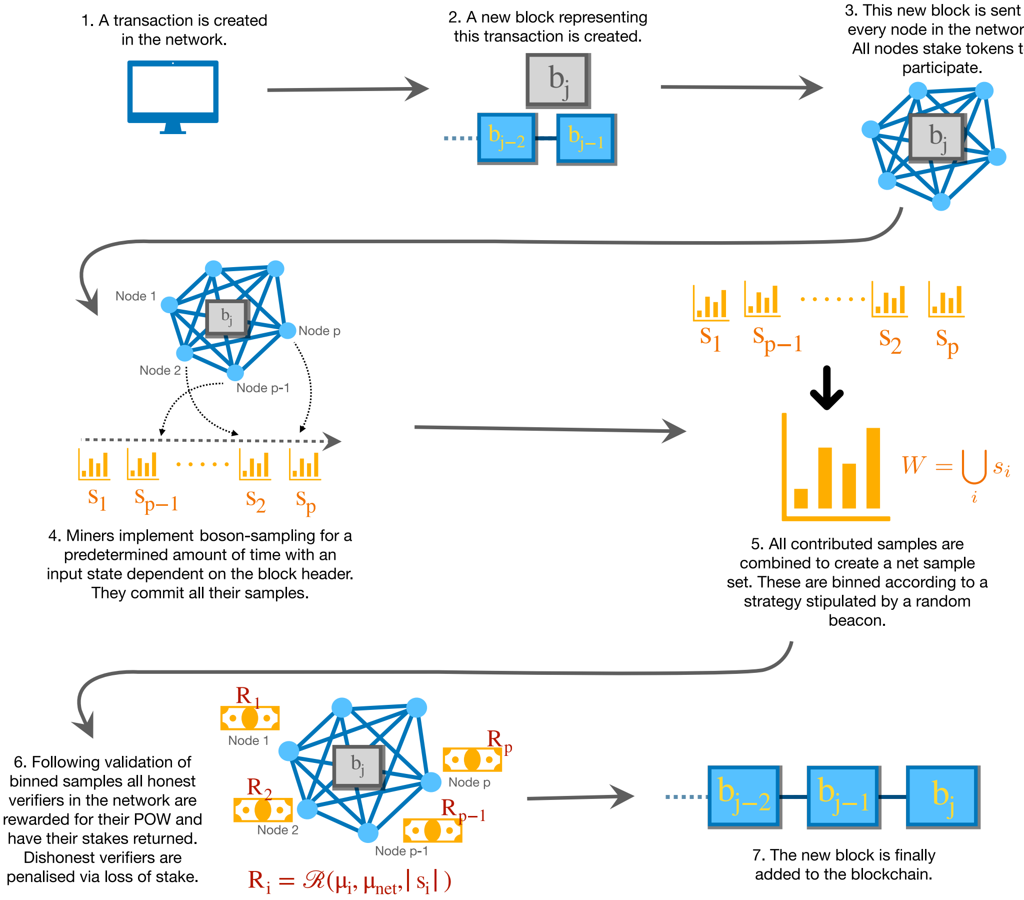
29

Proof-of-work consensus by quantum sampling

Deepesh Singh,[1] Boxiang Fu,[2] Gopikrishnan Muraleedharan,[3] Chen-Mou Cheng,[4] Nicolas Roussy Newton,[4] Peter P. Rohde,[5,3] and Gavin K. Brennen[3]

[1] *Centre for Quantum Computation & Communications Technology, School of Mathematics & Physics, The University of Queensland, St Lucia QLD 4072, Australia*
[2] *School of Physics, University of Melbourne, Melbourne, VIC 3010, Australia*
[3] *Center for Engineered Quantum Systems, School of Mathematical and Physical Sciences, Macquarie University, NSW 2109, Australia*
[4] *BTQ Technologies, 16-104 555 Burrard Street, Vancouver BC, V7X 1M8 Canada*
[5] *Hearne Institute for Theoretical Physics, Department of Physics & Astronomy, Louisiana State University, Baton Rouge LA, United States*

Proof-of-work is an algorithm to achieve network consensus with applications to blockchain technology. While it is secure and robust even in adversarial networks without centralised authority, the method can be extremely energy intensive, e.g. in 2022 the Bitcoin network consumed more energy than the country of Sweden. We propose to use coarse-grained boson-sampling (CGBS), as a quantum Proof-of-Work scheme for blockchain consensus. The users perform boson-sampling using input states that depend on the current block information and commit their samples to the network. Afterward, CGBS strategies are determined which can be used to both validate samples and to reward successful miners. By combining rewards to miners committing honest samples together with penalties to miners committing dishonest samples, a Nash equilibrium is found that incentivizes honest nodes. The scheme works for both Fock state boson sampling and Gaussian boson sampling and provides dramatic speedup and energy savings relative to computation by classical hardware.The figure below explains the steps involved in the protocol.


1. A transaction is created in the network.

2. A new block representing this transaction is created.

3. This new block is sent to every node in the network. All nodes stake tokens to participate.

4. Miners implement boson-sampling for a predetermined amount of time with an input state dependent on the block header. They commit all their samples.

5. All contributed samples are combined to create a net sample set. These are binned according to a strategy stipulated by a random beacon.

6. Following validation of binned samples all honest verifiers in the network are rewarded for their POW and have their stakes returned. Dishonest verifiers are penalised via loss of stake.

7. The new block is finally added to the blockchain.

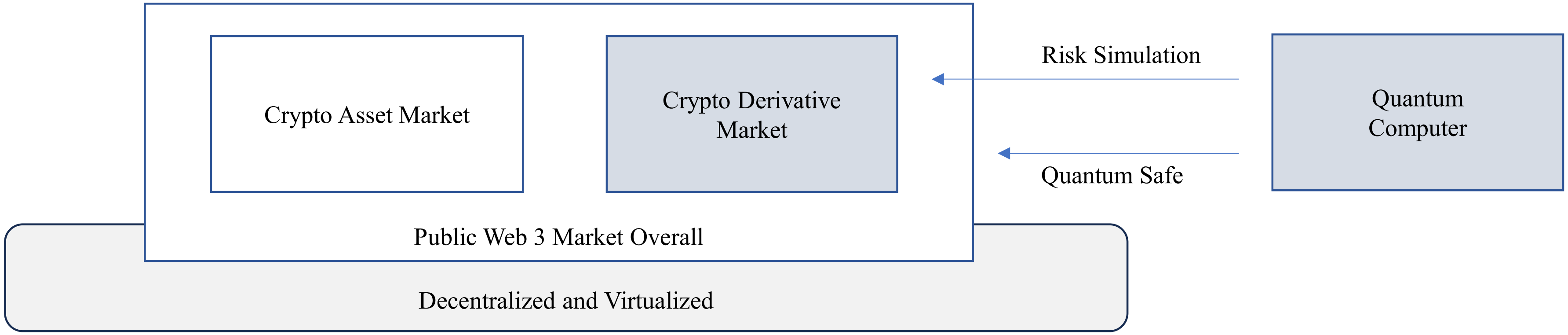
Figure 1. Blockchain architecture with the inclusion of boson-sampling routine.

[講演概要]
講演タイトル：暗号資産デリバティブの躍進と量子ファイナンス
　　　　　/ Breakthrough of Crypto Currency Derivatives and Quantum Finance Utilization
講演者：平山毅
　　　/ Tsuyoshi Hirayama
共同研究者の氏名と所属:IBM
講演内容の説明：

暗号資産市場は、価格変動と市場規模は落ち着いてきているが、その１つに現物市場と同様なデリバティブ商品が躍進していることが挙げられる。その実証分析と共に、ファンダメンタルが無い原資産である特性から、人工市場として、量子コンピューターを活用した量子ファイナンスの実用性も高いと考えられ、耐量子技術と共に機能と実証を紹介する。

:In the crypto asset market, price volatility and market size have been calming down, one of that reason is derivative products breakthrough similar to those in the physical market. Along with its empirical analysis, I will introduce the function and demonstration of quantum finance using quantum computers including quantum safe technology with as an artificial market, which is highly practical due to its characteristics as an underlying asset with no fundamentals.

説明を補足する図または表（どちらか１つ）:



2021年 [Blockchain in kyoto 2021]で講演実績有
Security token pricing trend related to each sto platform regulation system / IBM Tsuyoshi Hirayama
https://best-society.org/wp-content/uploads/2021/02/program_v210216.pdf

Investigating the probability distribution of average block time in proof-of-stake consensus algorithm using extreme value theory

Akihiro Fujihara, Chiba Institute of Technology

Abstract

Ethereum has moved its distributed consensus algorithm to Proof of Stake (PoS) on September 15, 2022. The average block generation time interval (or average block time) in PoS is known as about 12 seconds [1]. Ethereum uses a PBFT-inspired distributed consensus algorithm called Gasper (= GHOST + Casper) to generate a public blockchain[2]. In this algorithm, only a group of validator nodes that have staked its cryptocurrency can generate a block, and the generated block is sequentially approved by the other validator nodes.

It is known that block generation time intervals in blockchain systems that make consensus according to the Proof of Work, such as Bitcoin and old Ethereum before moving to PoS, follow an exponential distribution[3,4]. On the other hand, it is not well understood what kind of probability distribution the block generation time interval under PoS-based blockchain systems follows. Since Gasper performs to verify blocks transferred by the representative validator across the other validators, a distribution of the maximum block validating time is considered to determine the block generation time interval. Therefore, findings from the extreme value theory[5] can be useful to investigate the probability distribution of block generation time interval as shown in Fig. 1. In this talk, we investigate using the extreme value theory to show that the probability distribution of block generation time intervals in PoS-based blockchain systems seems to follow the Fréchet distribution.

References

[1] Ethereum Average Block Time Chart, Etherscan https://etherscan.io/chart/blocktime (Accessed on September 14, 2023).
[2] V. Buterin et al., “Combining GHOST and Casper” (2020). https://arxiv.org/abs/2003.03052
[3] T. Yanagihara and A. Fujihara “Cross-Referencing Method for Scalable Public Blockchain,” Internet of Things, Vol. 15, 100419 (2021).
[4] A. Fujihara, “Estimating the Relationship Between Block Size and Block Propagation Time in Bitcoin by Simulation,” INCoS 2023: Advances in Intelligent Networking and Collaborative Systems, pp. 166-176 (2023).
[5] S. Coles, “An Introduction to Statistical Modeling of Extreme Values” Springer (2021).

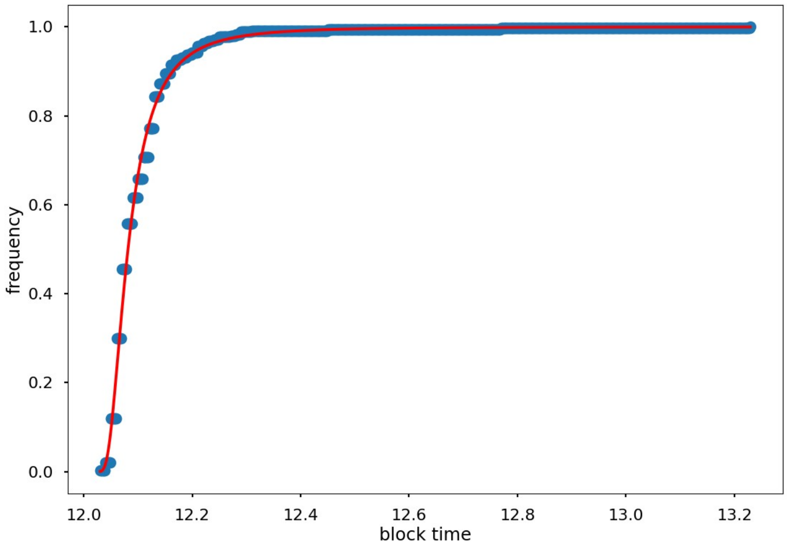


Fig. 1 Plot of the cumulative histogram of average block time in PoS Ethereum (blue dots) and its non-linear fitting (red solid line), where the data source is [1].