

Next-Generation Blockchain

miyabi



miyabi

bitFlyer, Inc.

Company Profile

bitFlyer, Inc.



Established	January 2014
Capital	4.1238 billion yen (including capital reserve)
Head offices address	Akasaka, Minato Ward, Tokyo
Overseas branches	The United States, Singapore, Luxembourg
Partnering Bank	Sumitomo Mitsui Banking Corporation
Account auditor	Ernst & Young, ShinNihon LLC
Law office	Mori Hamada & Matsumoto, Nishimura & Asahi, AZX Professionals Group, So Law Office
Tax corporation	Ernst & Young, Tax Co.
Employees	72



Over 900,000 users
Over 1.5 trillion yen in monthly transactions
About 4.1 billion yen in capital
Japan's largest bitcoin and blockchain company

What is blockchain?



The Japan Blockchain Association's Definition of Blockchain

Blockchain Put Simply —

A *shared network* database that

- Only allows *correct* records to be saved
- Does not allow the alteration, deletion, or falsification of records
- Automatically repairs itself when damaged
- Does not crash
- Only recognizes information that *everyone agrees on* as valid

(REF: *Ichiban Yasashii Blockchain no Kyohon (The Kindest Blockchain Textbook)*)

A blockchain is defined as a protocol, or implementation of a protocol, used by an unspecified number of nodes containing Byzantine faults, and converges the probability of consensus reversion with the passage of time to zero.

In a broader sense, a blockchain is a technology with a data structure which can easily detect manipulation using digital signatures and hash pointers, and where the data has high availability and integrity due to distribution across multiple nodes on a network.

(REF: *Japan Blockchain Association* — <http://jba-web.jp/>)

Blockchains are a new kind of database

They're unique in that data recorded on a blockchain cannot be modified or deleted, repairs itself when broken, and does not degrade.

This network sharing model makes only the information that all users agree on valid.

Unique Features of blockchain

Immutability

- Transactions (data) are stored across consecutive blocks. Because consecutive blocks are co-dependent, altered transaction data is highly easy to detect, and data corruption is virtually impossible.

Byzantine Fault Tolerance (BFT)

- When a system has BFT, the whole system continues to function normally as long as the total number of Byzantine nodes (nodes that do not behave properly due to hardware failure or server hacking) remain below a certain level.

No Single Point of Failure (SPOF)

- A part of a system that, if it fails, will stop the entire system from working. In non-blockchain systems, master, controller and certificate authorities can become SPOFs. Blockchain has no SPOF.

Introducing...

miyabi

A next-generation blockchain database

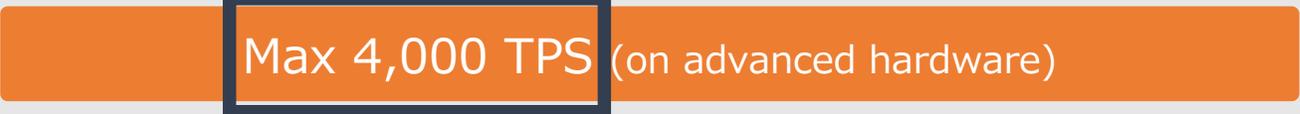


miyabi

World's Fastest Performance

miyabi realizes transaction processing speed that was thought of as nearly impossible using pre-existing technology.

1,500 - 2,000 TPS



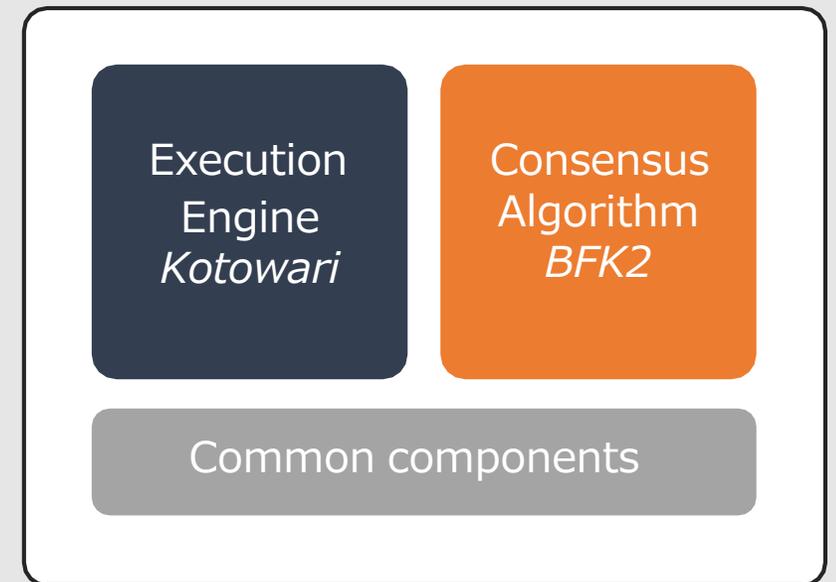
Max 4,000 TPS (on advanced hardware)

The image shows a horizontal orange bar representing a performance range. A dark blue rectangular box highlights the text 'Max 4,000 TPS (on advanced hardware)' which is positioned on the left side of the bar.

This performance power was realized through thorough optimization of the consensus algorithm, execution engine, and other common components.

Finality + Unmatched Performance

miyabi software



Merits of implementing *miyabi* (1)

Immutability

- *miyabi* offers an extremely high level of security not available in normal database systems.
- The data for each transaction is stored in a block, and a hash of the data in each block is stored in the next block, creating a chain of dependency between the blocks.
- Chaining together the blocks in this way allows the consistency of the transaction data to be guaranteed. It is easy to detect when transaction data is overwritten, making data tampering effectively impossible.

Finality

- *miyabi* allows for the securing of transactional finality in which the data for each transaction can be fully confirmed.
- One major problem with blockchains such as those used in Bitcoin and Ethereum is that the data stored therein is not permanently fixed. In a Bitcoin-style blockchain, the probability of existing data being overwritten decreases as time passes.
- However, *miyabi's* algorithm is written in such a way that data cannot be altered or lost as soon as it is written.

Byzantine fault tolerance (BFT)

- *miyabi* is a pure blockchain with Byzantine fault tolerance (BFT).
- Nodes (servers) that do not behave properly, whether due to hardware issues, hacking or other causes, are known as Byzantine nodes.
- A blockchain with Byzantine fault tolerance remains able to function properly as long as the number of Byzantine nodes does not exceed a certain amount. Older systems did not feature Byzantine fault tolerance, and the entire system would go down if even one server stopped working. Measures such as triple modular redundancy are used to help prevent such occurrences, but this does not completely protect the system from hacking.

Merits of implementing *miyabi* (2)



No Single Point of Failure

- *miyabi* does not require a certificate authority. A certificate authority is a single point of failure, and a technical issue or an incident such as a DDoS attack at the certificate authority poses the risk of taking the entire blockchain down. Even if redundancy measures are implemented at the certificate authority, this does not change that fact that it is a single point of trust (SPOT). With *miyabi*, privilege setting is done with a secret key, eliminating the weaknesses present with a single point of failure and a single point of trust.



Disaster countermeasures (High Availability)

- *miyabi* offers high availability even in the face of disasters. Even in the event that a subset of the servers (nodes) are lost due to a disaster, all of the data is stored in each node, and it remains possible to access the latest correct data. For example, an approach of maintaining servers in a variety of locations such as Japan, the United States and Europe allows for a flexible system that is highly disaster-resistant.



Performance (Throughput)

- *miyabi* is able to process 2,000 transactions per second (4,000 transactions per second on advanced hardware) and boasts the world's highest performance (according to an internal study) among finality-ensured blockchains.
- Existing blockchain technologies have struggled with the issue of extremely slow processing speeds.
- It is its support for finality and *BFT*, its elimination of the single point of failure (SPOF) and its high performance (throughput) that gives *miyabi* its technological superiority.



Latency

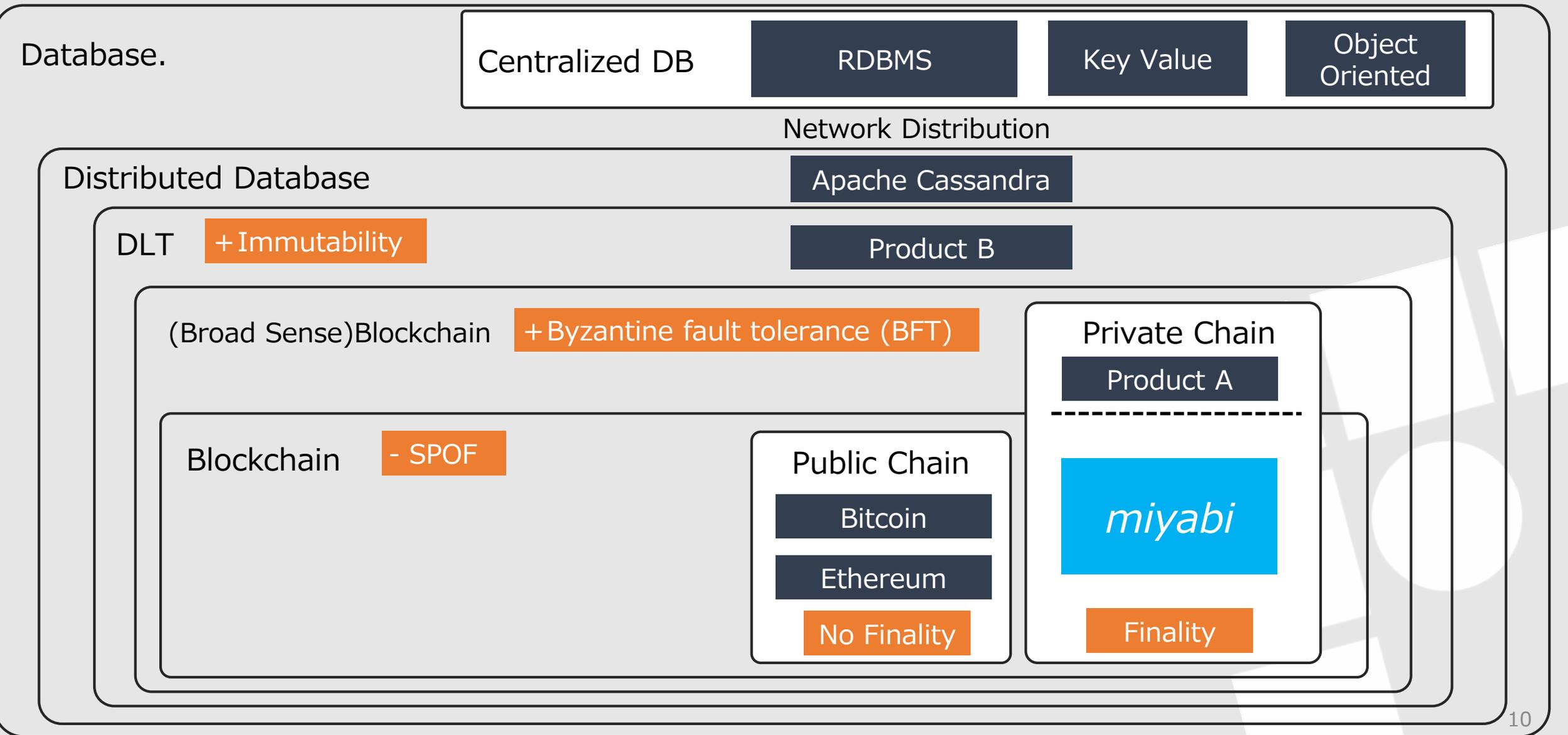
- At one to four seconds, *miyabi* features shorter delays than other blockchains (Ethereum has a 15-second delay and does not ensure finality).
- A blockchain is a type of distributed database. What we consider a blockchain is a system that includes a new database with features such as non-tamperability, finality and Byzantine fault tolerance as well as a smart contract execution environment. Since the nodes and data are distributed over the network, the processing speed, including the throughput and delay, depends greatly on the speed of the network.

The Pursuit of Finality

	Public chain		Private chain			Relational database
	Bitcoin	Ethereum	<i>miyabi</i>	Product A	Product B	RDBMS
Immutability	○	○	○	○	○	×
BFT	○	○	○	○	×	×
Finality	×	×	○	○	○	○
Consensus Algorithm	PoW	PoW⇒PoS	BFK2	PBFT	?	(N.A.)
Single Point of Failure	None	None	None	Yes Certificate Authority	Yes	-
Throughput	2	15	1,500- 2,000(4,000)	1,000		Over 100,000
Latency	10min	12sec	1-4 sec			1 msec

▶ **Blockchains without finality bear the risk of data turnover, making them unsuitable as enterprise solutions.**

Difference between *miyabi* and other databases



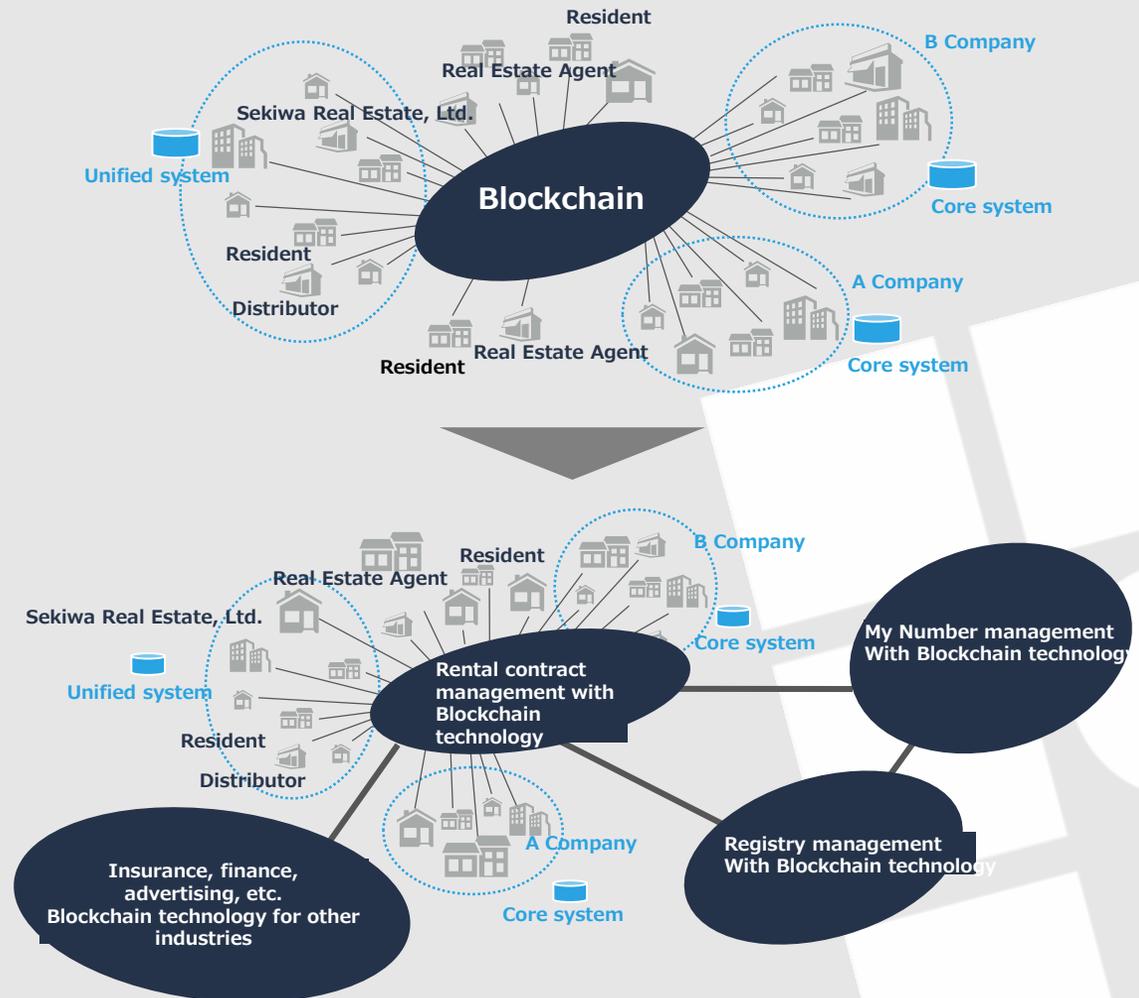
Upcoming for *miyabi*

Equipping Industry Leader Sekisui House with *miyabi*



Using blockchain technology to construct a real estate information management system

- ✓ Japan's first application of blockchain to enterprise operations
- ✓ Providing rental services using blockchain. Cross-industry consortium also currently under consideration.
- ✓ Aims to create standardized platform architecture for Japan's real estate industry (launch planned within FY2017)



Provision of Testing Platform for the Japanese Bankers Association



平成29年9月14日

各 位

一般社団法人全国銀行協会

ブロックチェーン連携プラットフォームのパートナーベンダー選定について

一般社団法人全国銀行協会（会長：平野信行 三菱UFJフィナンシャル・グループ社長）は、本日開催の理事会において、「ブロックチェーン連携プラットフォーム」（※）（以下「本プラットフォーム」という。）の実証実験環境を提供するベンダー（以下「パートナーベンダー」という。）として、株式会社エヌ・ティ・ティ・データ、株式会社日立製作所、株式会社bitFlyer、富士通株式会社の4社を選定することを決定いたしました。

今後、実証実験環境に関する詳細仕様等を調整したうえで、パートナーベンダーと契約締結を行い、本年10月中を目途に本プラットフォームの稼働を開始する予定です。

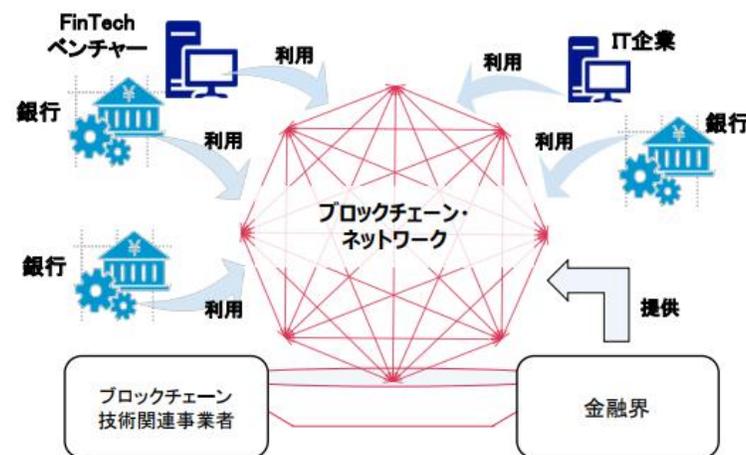
当協会は、本プラットフォームの整備を通じて、新たな決済・送金サービスや本人確認・取引時確認（KYC）、金融インフラ（全銀システム、でんさいネットシステム等）等のブロックチェーン技術/分散型台帳技術の活用が期待される分野における会員各行等の実用化に向けた検討を支援して参ります。

※

平成29年3月16日公表の「ブロックチェーン技術の活用可能性と課題に関する検討会報告書」において、銀行界を中心とした、連携・協働型の実証実験環境として、本プラットフォームの整備が提言されたことを受け、平成29年4月13日に、本プラットフォームの基本構想を全銀協ウェブサイト [🌐](#) に公表し、本年秋頃を目途とした整備に向けて検討を進めることとしておりました。

以上

【ブロックチェーン連携プラットフォーム】（仮称）のイメージ】



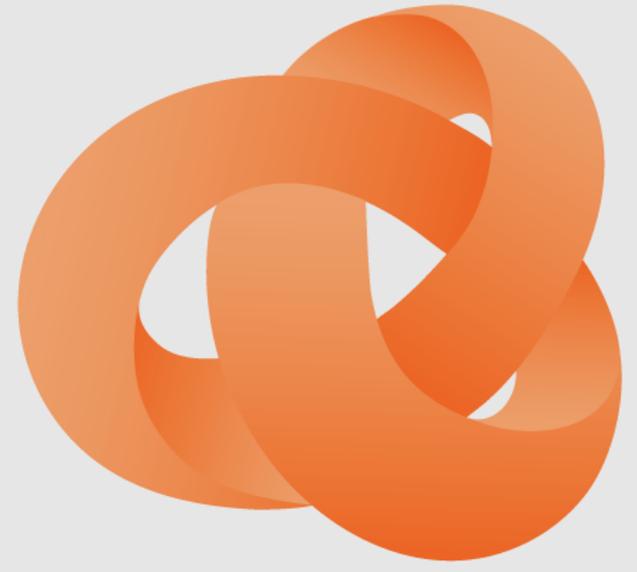
Source: <https://www.zenginkyo.or.jp/fileadmin/res/news/news290413.pdf>

Blockchain Research & Development at bitFlyer



- ✓ Acquired first patent using blockchain technology
- ✓ Patent covers private nodes, as well as related processing methods and program
- ✓ Ongoing dedication to the R&D of blockchain technology

Japan's First Integral
Blockchain Technology Patent



miyabi

