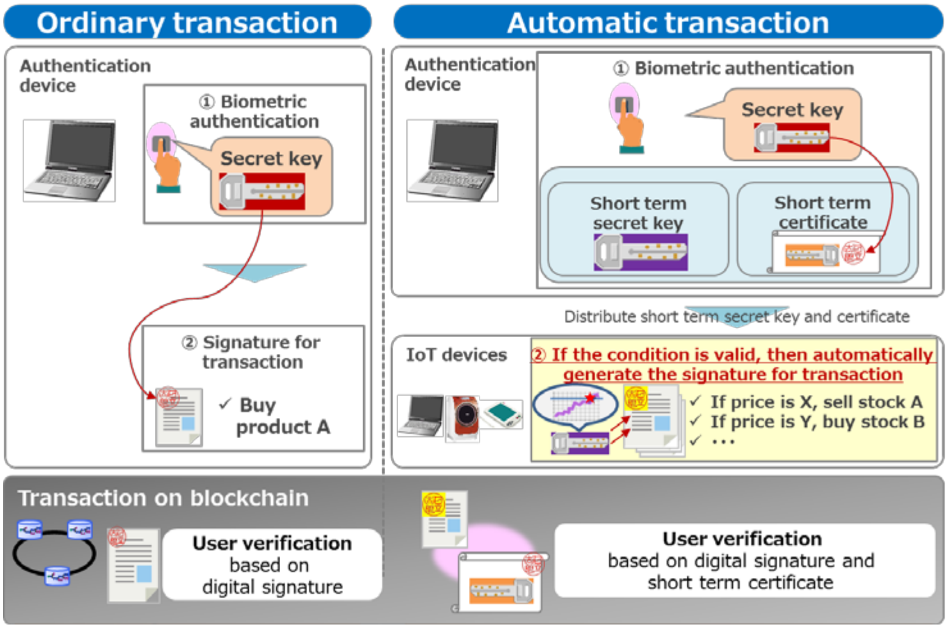
HITACHI
Inspire the Next

News Release

FOR IMMEDIATE RELEASE

Biometric authentication technology to realize secure trade on blockchain

Enabling IoT payments and automatic transactions through PBI[1]-blockchain cooperation technology



Ordinary transaction
Authentication device
① Biometric authentication
Secret key
② Signature for transaction
✓ Buy product A
Automatic transaction
Authentication device
① Biometric authentication
Secret key
Short term secret key
Short term certificate
Distribute short term secret key and certificate
IoT devices
② If the condition is valid, then automatically generate the signature for transaction
✓ If price is X, sell stock A
✓ If price is Y, buy stock B
✓ …
Transaction on blockchain
User verification based on digital signature
User verification based on digital signature and short term certificate

Overview of PBI-blockchain cooperation technology

Tokyo, October 5, 2017 --- Hitachi, Ltd. (TSE: 6501, Hitachi) today announced the development of PBI-blockchain cooperation technology, to realize secure transactions on blockchain based on the Public Biometric Infrastructure (PBI), Hitachi's original authentication technology that generates a digital signature[2] from biometric information. By using biometric information such as finger vein pattern which carries low risk of theft or leakage to generate a digital signature, this technology can be applied to transaction records as well as automatically generate a digital signature for predetermined conditions. As a result, secure and convenient user verification can be achieved for algorithmic transactions expected to employ blockchain, such as stock, electricity or automatic payment on IoT devices. Hitachi intends to develop a secure and convenient personal authentication platform on blockchain through verification tests with partners who plan to utilize blockchain technology.

Blockchain which does not require the mediation of a trusted third party is expected to find many applications including cryptocurrency, payment, and medical history. The validity of transactions over blockchain is guaranteed by a digital signature which each user adds to their transaction data based on a public-key cryptosystem[3] and which can be verified by anyone. However, if the user loses their secret key or it is leaked, there is a risk that assets may be lost or stolen through undesired trade by impersonators. For this reason, reliable user verification and prevention of impersonation were issues for current authentication technology, and measures such as storing the secret key on IC cards or servers and only enabling access by ID, password or biometric authentication have been taken.

To address these issues, Hitachi developed PBI-block chain cooperation technology to leverage PBI that can generate digital signatures from biometric information. Unlike conventional biometric authentication technology, as the user can use their own biometric information as the secret key with PBI, there is no need for external management of the secret key and thus, more secure trade is possible. Further, by developing "short-term device certificate" generation technology to enable the automatic generation of digital signatures based on pre-set conditions, automatic trading is also realized as it resolve the time-consuming process of generating signatures whenever a transaction is required. Features of the technology are as below:

1. PBI-blockchain cooperation technology

Cooperation technology was developed using PBI to generate and verify digital signatures for transactions on Hyperledger Fabric,[4] a representative blockchain OSS. Although the conventional Hyperledger Fabric application manages the user's private key and generates the signature for transaction on the application server, it was confirmed that when the new technology was implemented on a Hyperledger Fabric environment created by Hitachi, digital signatures could be generated and verified on the user terminal side. Further, there is no need to manage a secret key as PBI temporarily derives the secret key from the users' biometric each time, therefore, resolving the issue of unauthorized use through loss or theft. As a digital signature can only be created by the actual person, the transaction is guaranteed by reliable identity verification.

2. Short term device certificate management technique for the automatic trade

A technique was developed to automatically generate a digital signature for transactions when an IoT device, such as a PC or smartphone, automatically transfers transactions to the blockchain as in algorithmic trade of stock or electricity. Specifically, when a user orders a logic of trade conditions to a device "to sell how much of a given stock when it is at a given price," the user generates for the device, a "short-term secret key" and a paired "short-term certificate" with user's original signature. The device stores the short-term secret key and short-term certificate for a set period of time, and only generates the digital signature when the transaction conditions are satisfied. As a result, it is possible to automatically trade without requiring the device owner to authenticate each transaction. By storing the short-term secret key and short-term certificate on selected IoT devices, it will be possible to conduct settlement on those IoT devices. Further, as the validity of the certificate can be set for a short period, the risks are reduced when the secret key is leaked.

Through verification tests together with partners who are considering utilizing blockchain in their business, Hitachi is aiming to bring this technology to the market during fiscal 2018, as well as establishing a secure and convenient blockchain infrastructure by developing an API(5) function as OSS(6) that enables users to select and change the method of digital signatures.

A part of this research result will be presented at Blockchain EXE(7) meetups to be held on 11th October 2017 in Tokyo, Japan, and on 9th January 2018 in New York, USA.(8)

(1) PBI (Public Biometrics Infrastructure): Hitachi's original technology that extracts a secret key by correcting "fluctuations" in biometric information such as vein patterns, and generates a digital signature based on a public key cryptosystem. With previous technology, as biometric information always contains "fluctuations", it was impossible to generate an secret key which needs to be unique data as identical data could not be obtained every time. With PBI, as it is unnecessary to manage a secret key stored on an IC card or a password, it is possible to realize convenient, low cost and secure user authentication. Further, as biometric information is converted into data that is cryptographically difficult to restore (PBI public key) using a "one way function," the original biometric information is not stored anywhere and thus the risk of leakage is minimized .

(2) Digital signature: A signature that fulfills a role corresponding to a seal or signature on a paper document. It is mainly used for user authentication and to prevent forgery/ falsification.

(3) Public key cryptosystem: An encryption method that uses a public key publicly disclosed with a secret key managed only by the message receiver. The encrypted message with the public key can only be decrypted with the paired secret key.

(4) Hyperledger Fabric: An open source blockchain framework developed by The Linux Foundation, established in a joint development project "Hyperledger" blockchain technology.

(5) API: Application Programming Interface

(6) OSS: Open Source Software

(7) https://blockchainexe.com/

(8) https://www.meetup.com/ja-JP/ConsenSys-Ethereum-Meetup/events/245558130/?eventId=245558130

About Hitachi, Ltd.
Hitachi, Ltd. (TSE: 6501), headquartered in Tokyo, Japan, delivers innovations that answer society’s challenges. The company’s consolidated revenues for fiscal 2016 (ended March 31, 2017) totaled 9,162.2 billion yen ($81.8 billion). The Hitachi Group is a global leader in the Social Innovation Business, and it has approximately 304,000 employees worldwide. Through collaborative creation, Hitachi is providing solutions to customers in a broad range of sectors, including Power / Energy, Industry / Distribution / Water, Urban Development, and Finance / Government & Public / Healthcare. For more information on Hitachi, please visit the company's website at http://www.hitachi.com.

# # #

Information contained in this news release is current as of the date of the press announcement, but may be subject to change without prior notice.
