Technical Trends for DID

2021.3.4

Index

1. Self-Introduction
2. Technical Trends for DID (ERC725)
3. The Future of DID
4. Bonus: My Inspiration

Self-Introduction: Hello!

שלום!

Ryutaro Suda

☑ 3rd year student at the University of Tokyo Faculty of Engineering Department of Mathematical Engineering and Information Physics (enrollment by recommendation)

☑ 4th term at the CO.NECT University of Tokyo Blockchain Student Entrepreneur Support Program

☑ Conducting research and development on ID and the ERC725 standard

☑ Interning at Couger since January 2021

Other Activities:

○ Representative of Japan for Red Bull Basement 2020

○ Member of the 6th graduating class at MAKERS UNIVERSITY

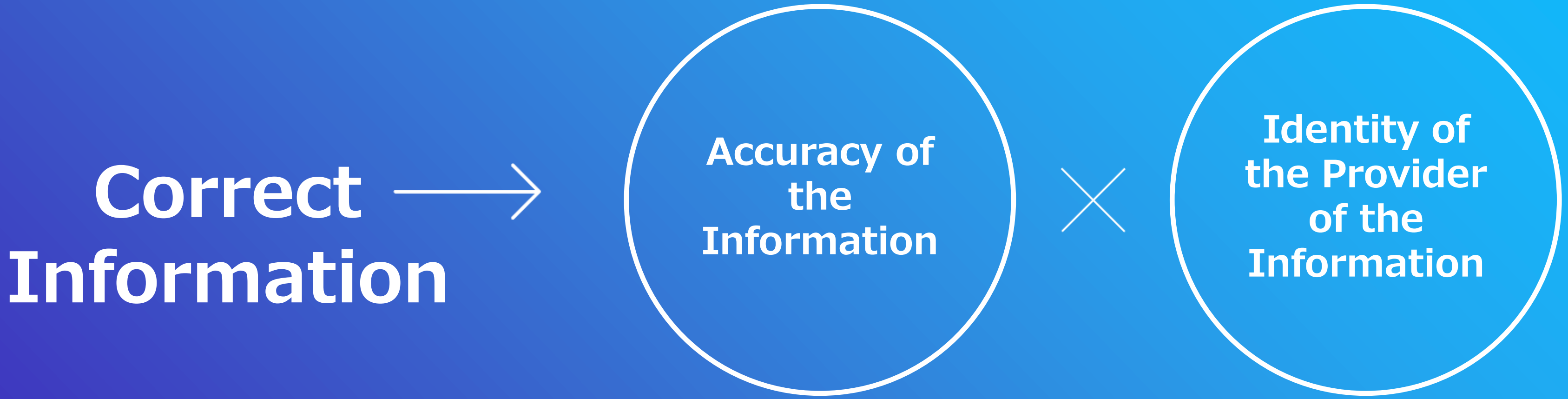
The Subject of My Thoughts Over the Past Year

Building a system that values people who add correct information

The Subject of My Thoughts Over the Past Year

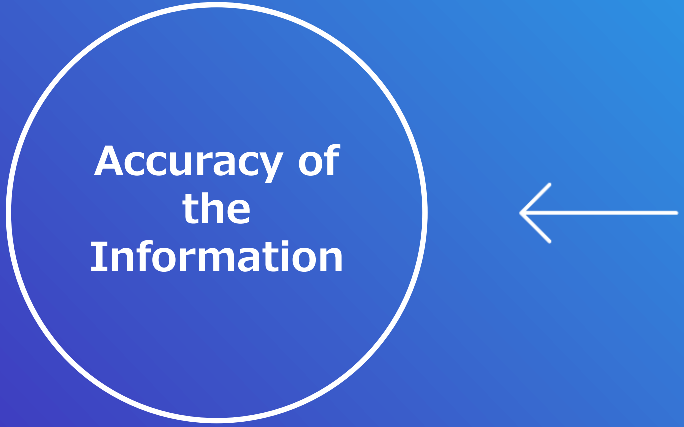
Building a system that values people who add correct information

The Subject of My Thoughts Over the Past Year



Correct Information → Accuracy of the Information × Identity of the Provider of the Information

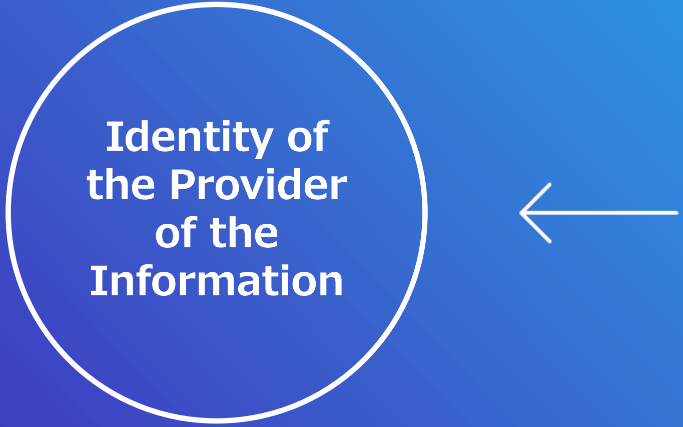
Elements of the Accuracy of the Information



Accuracy of the Information

1. **Resistance to falsification**
2. **Incentives for accuracy**
3. **3rd party reevaluation**

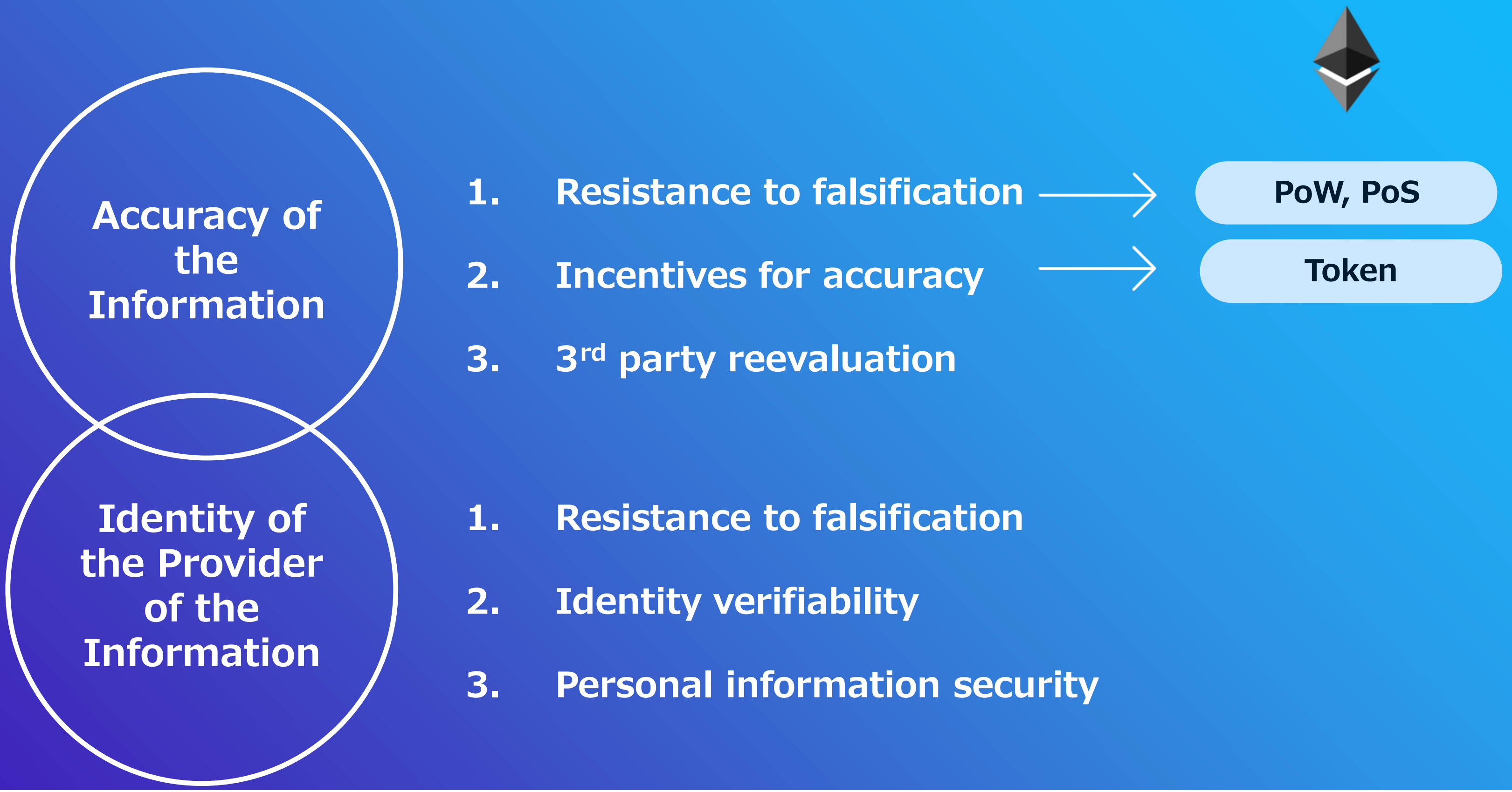
Conditions Necessary to Ensure Identity



Identity of the Provider of the Information

1. **Resistance to falsification**
2. **Identity verifiability**
3. **Personal information security**

What Blockchain Can Do



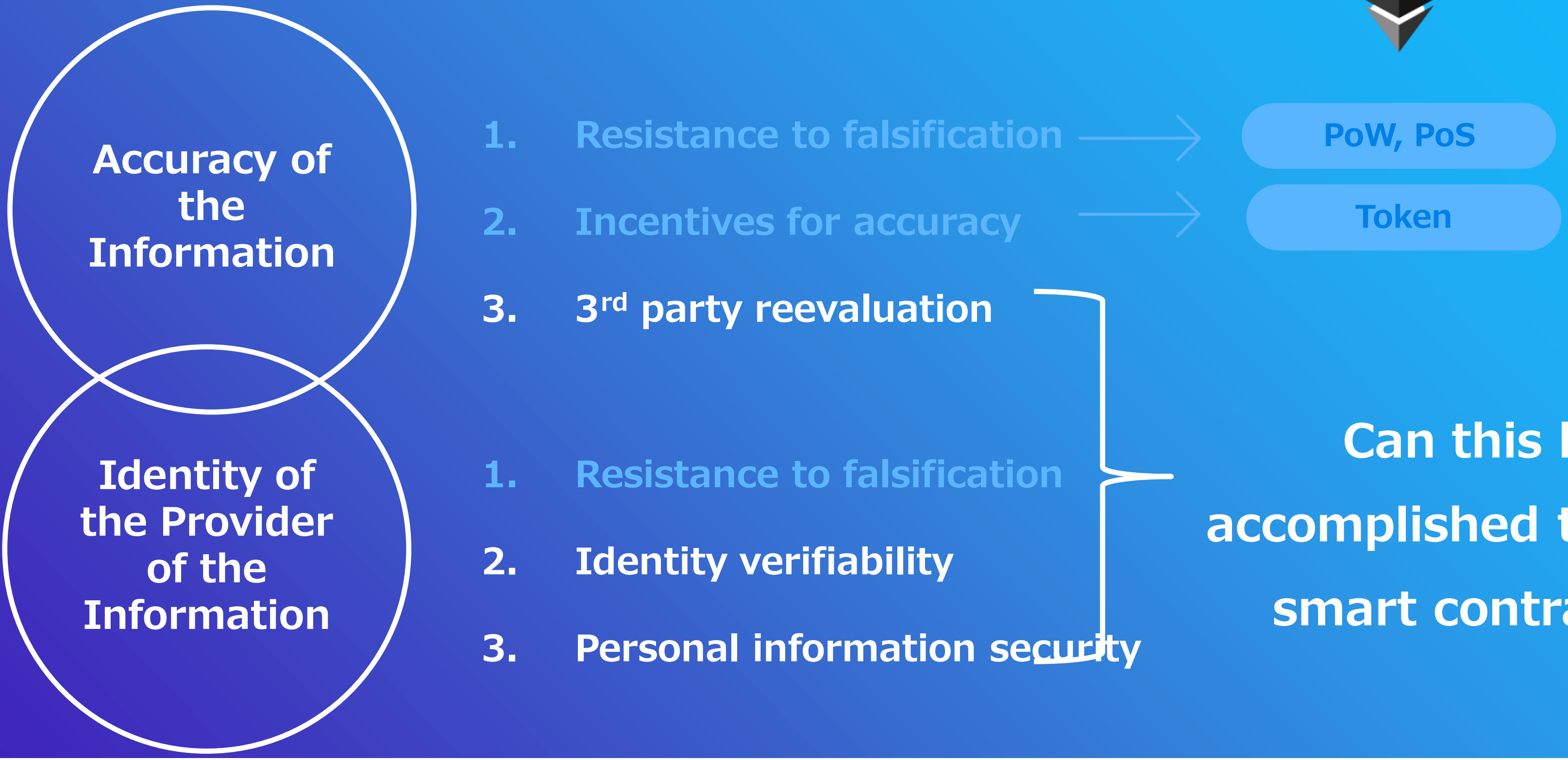
Accuracy of the Information

1. Resistance to falsification → PoW, PoS
2. Incentives for accuracy → Token
3. 3rd party reevaluation

Identity of the Provider of the Information

1. Resistance to falsification
2. Identity verifiability
3. Personal information security

What Blockchain Can Do



Accuracy of the Information

1. Resistance to falsification → PoW, PoS
2. Incentives for accuracy → Token
3. 3rd party reevaluation

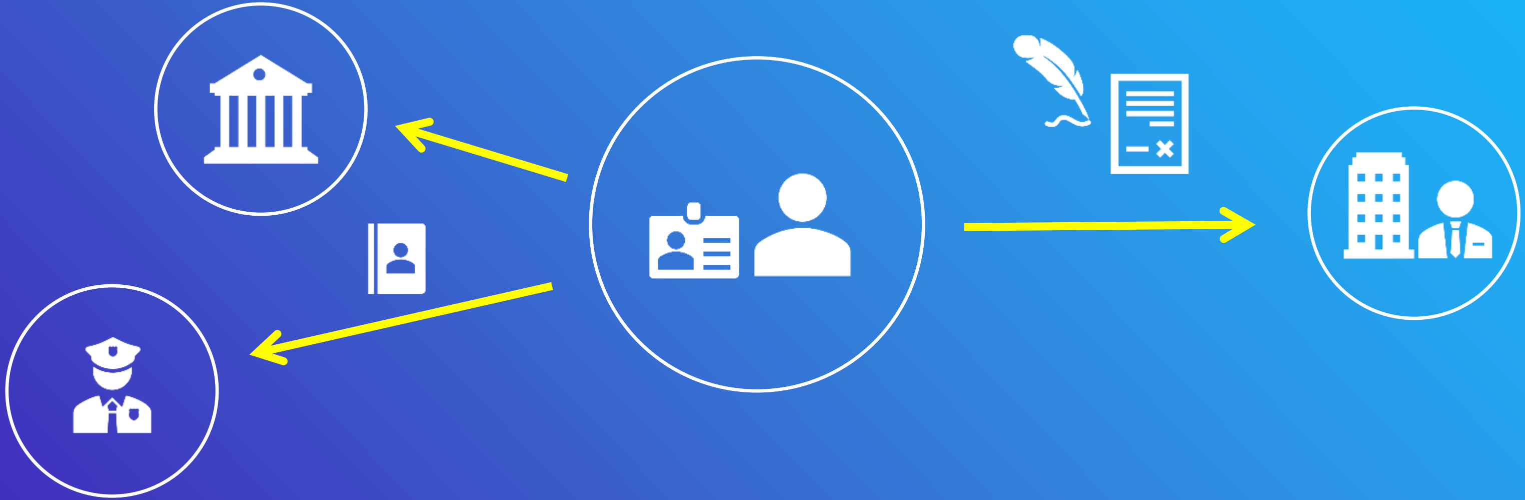
Identity of the Provider of the Information

1. Resistance to falsification
2. Identity verifiability
3. Personal information security

Can this be accomplished through smart contracts?

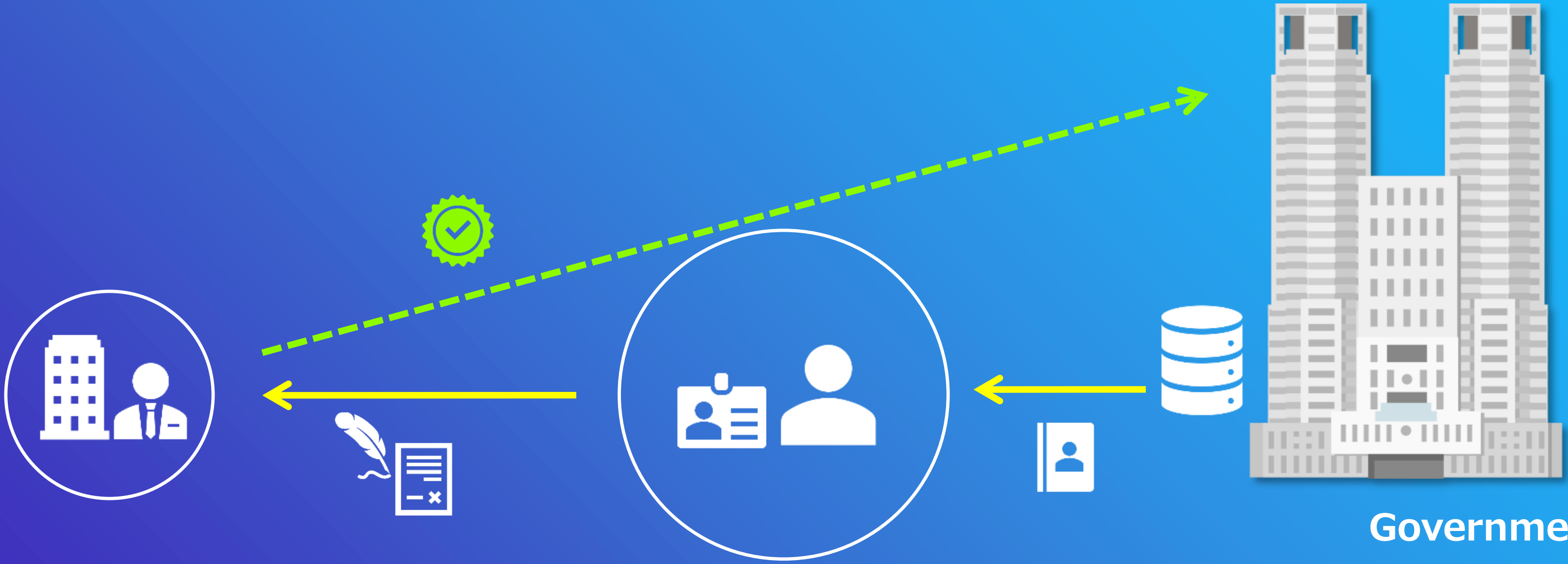
What is Identity?

Identity checks are always required



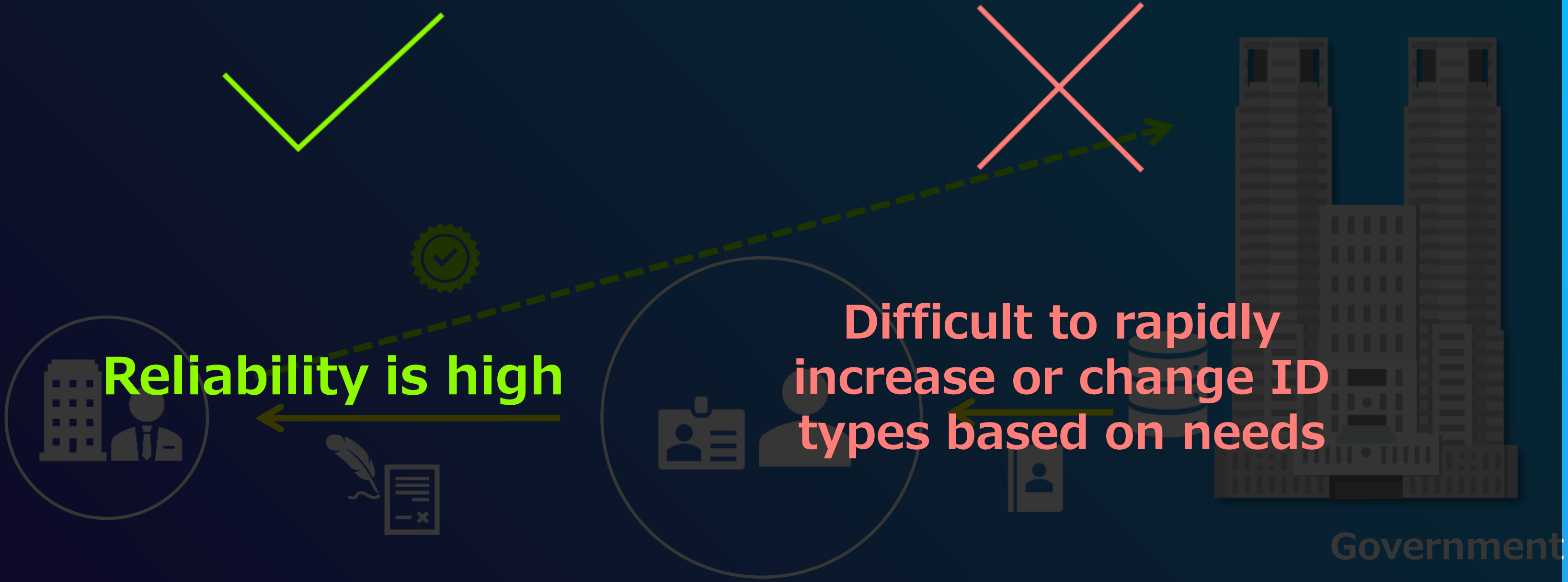
Centralized Identity

Trust is based on governments and other centralized organizations



Centralized Identity

Trust is based on governments and other centralized organizations



Reliability is high
Difficult to rapidly increase or change ID types based on needs
Government

What is Decentralized Identity (DID)?

ERC: Identity

ethereum

https://www.slideshare.net/FabianVogelsteller/erc-725-identity

What is ERC725?

- ERC725: A standard that was proposed by Fabian Vogelsteller in October 2017 with the purpose of achieving DID on Ethereum.
    - Fabian is a developer who has been involved with Ethereum from its early stages and also the inventor of the ERC20 token standard.
    - He is currently serving as the founder of “LUKSO,” the platform for ICO.
- There is a movement to standardize the Ethereum Identity using ERC725, and over 30 projects are participating officially (ERC725Alliance).
- On the other hand, perhaps it has yet to permeate to the level of a service for general users, despite the passing of over 3 years since the proposal.
    - For example, the process is “register user through the github connection → select a wallet → grant support” for gitcoin user verification.
    - The same platform was also used to raise grant funds for C.R.E.A.M..

Thoughts Process for ERC: Identity

Keys

Public Key

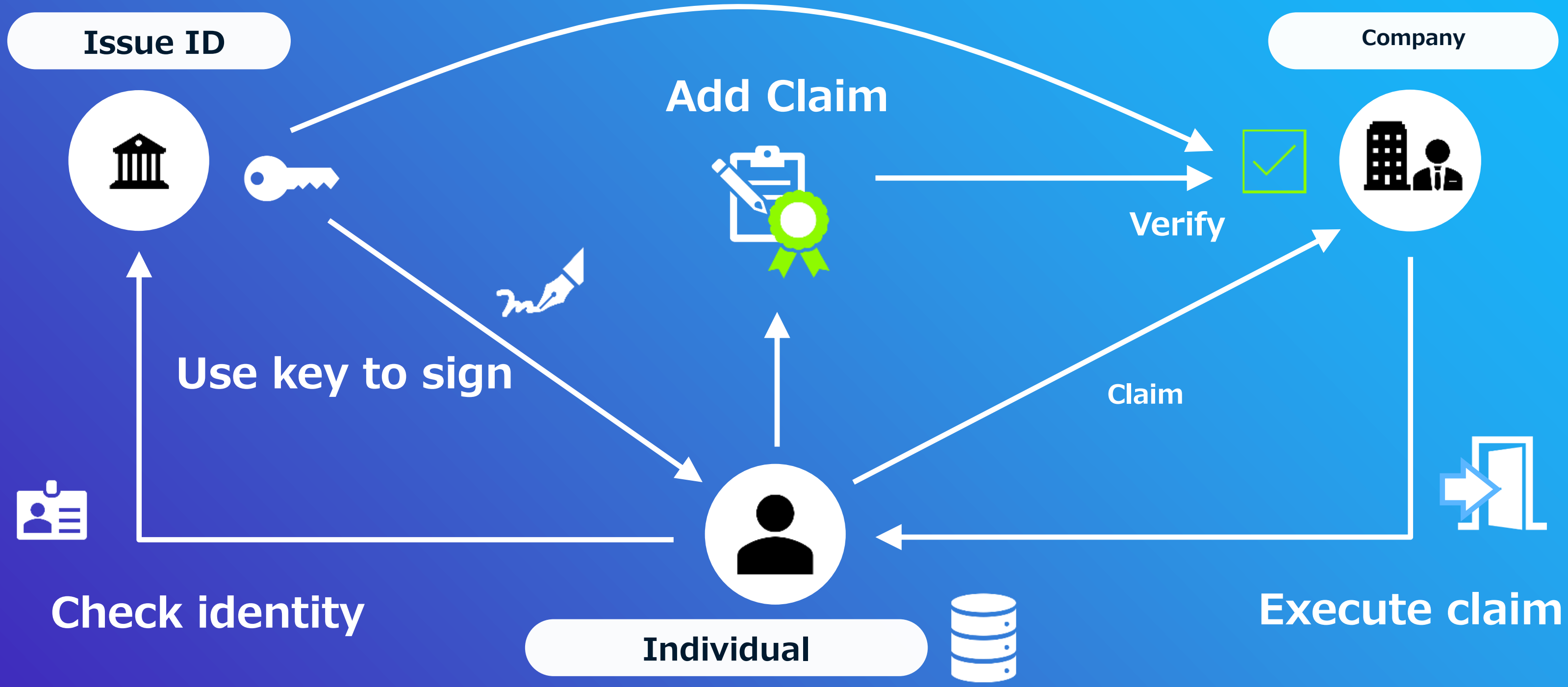
Execution

Execute

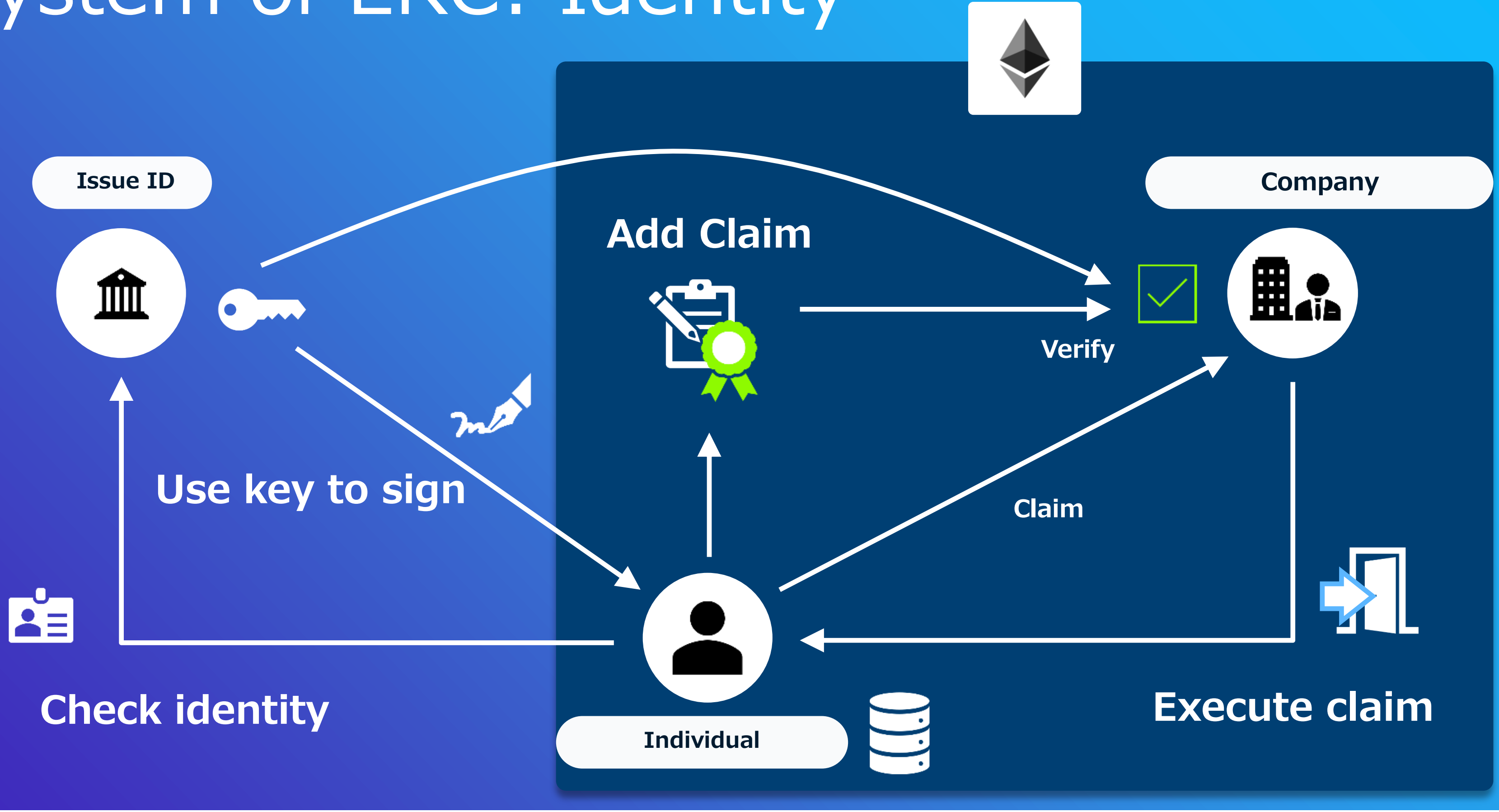
Claims

Claim

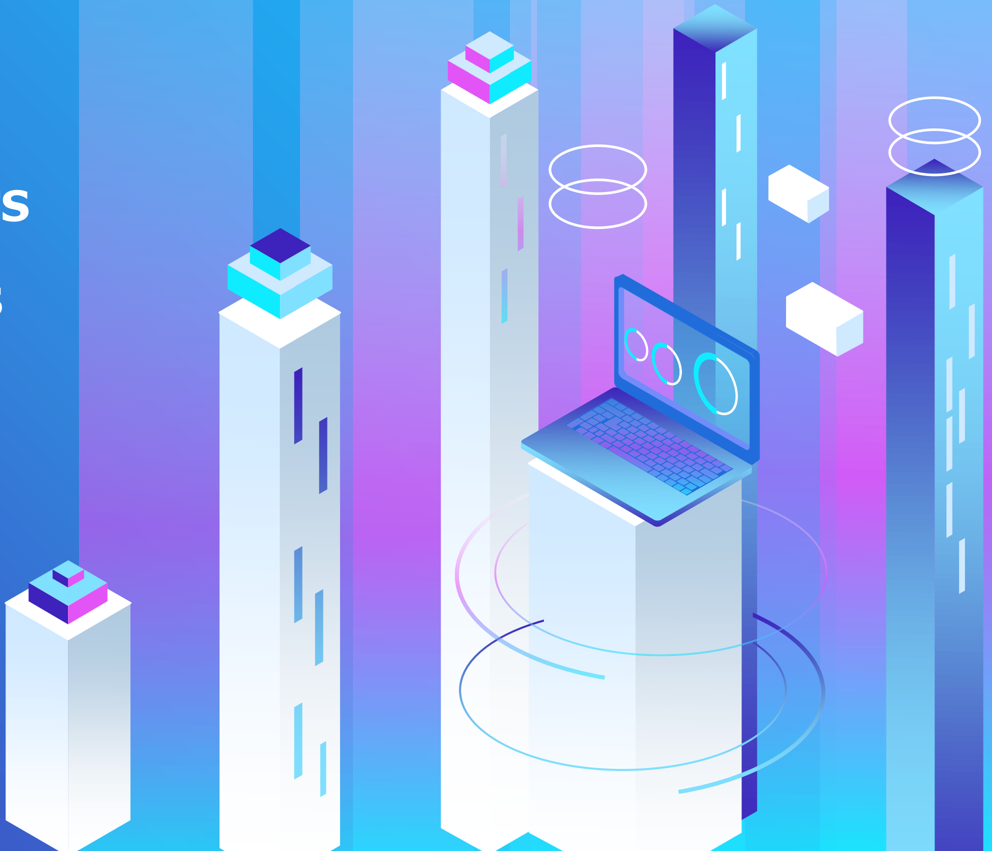
System of ERC: Identity



System of ERC: Identity



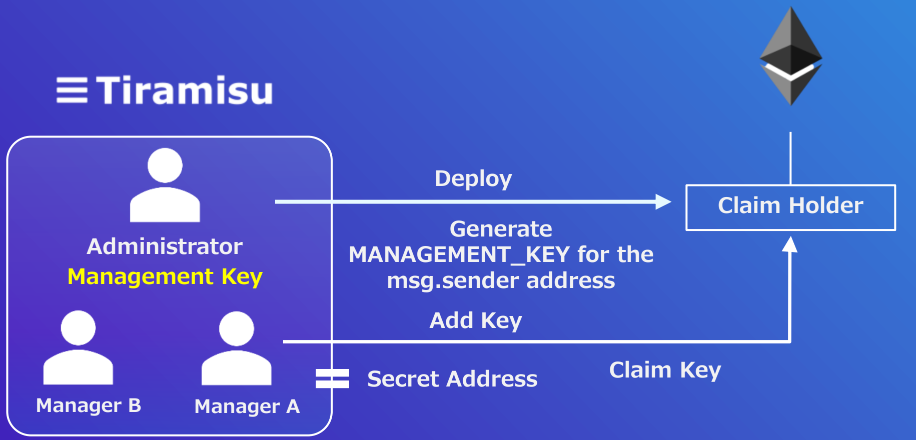
Platform to Verify Reviewers and Provide Token Rewards Using Decentralized ID



Demo

1. Setup Key Registration

Can register multiple keys based on roles



≡Tiramisu

Administrator

Management Key

Manager B

Manager A

Deploy

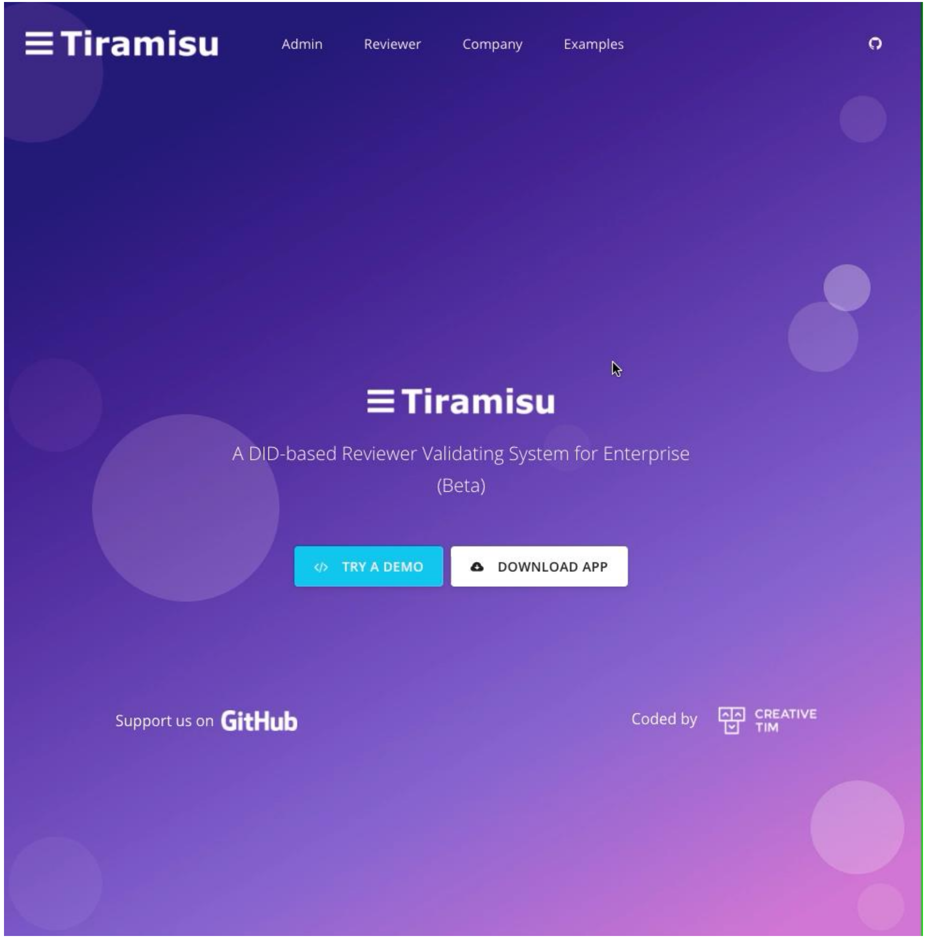
Claim Holder

Generate MANAGEMENT_KEY for the msg.sender address

Add Key

= Secret Address

Claim Key



≡Tiramisu

A DID-based Reviewer Validating System for Enterprise (Beta)

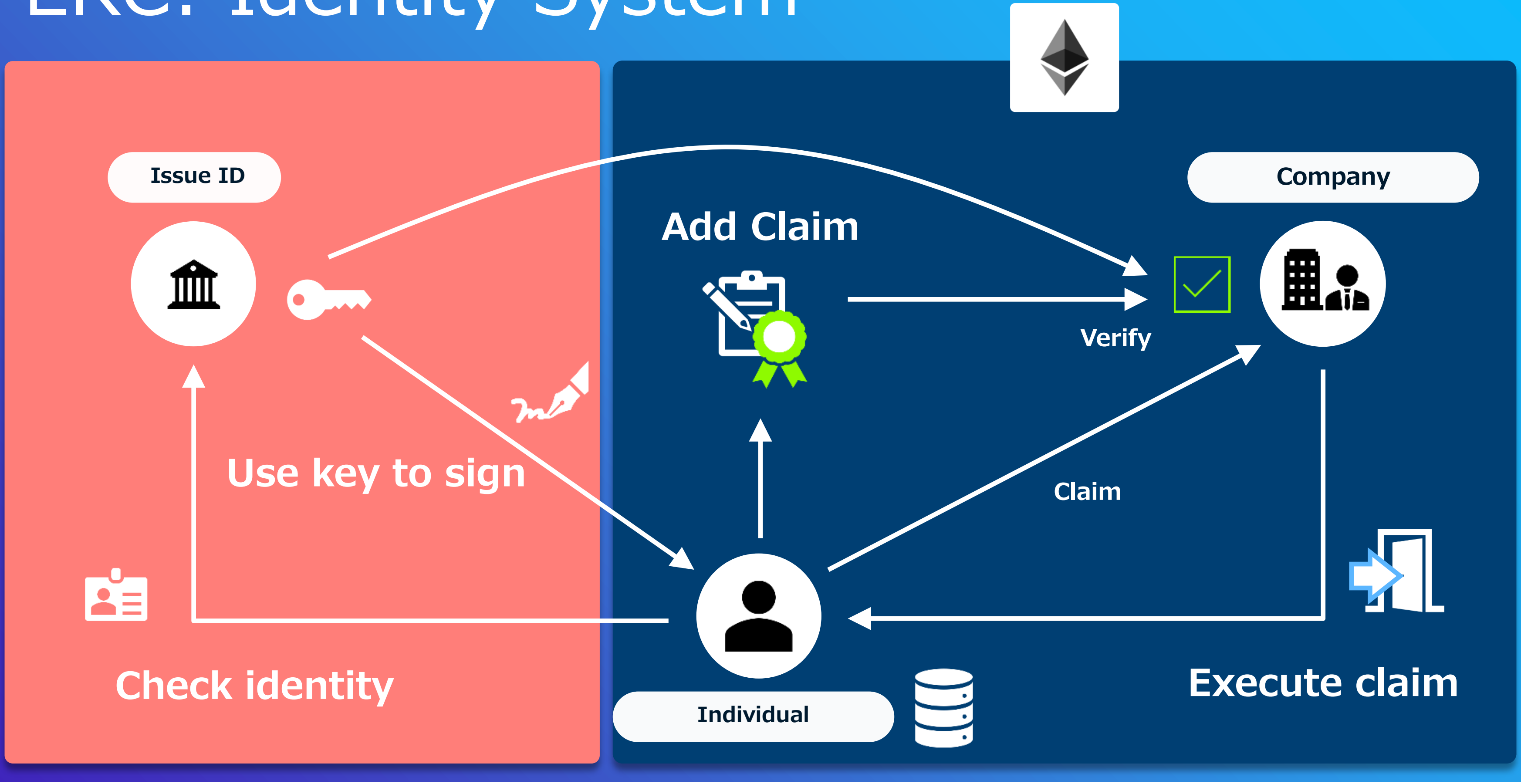
Support us on GitHub

Coded by CREATIVE TIM

ERC725 Summary

1. **ERC725 is key, signature, and claim**
2. **The reality of an identity is to be able to execute desired functions**
3. **Issue: The original ID check is off the chain**

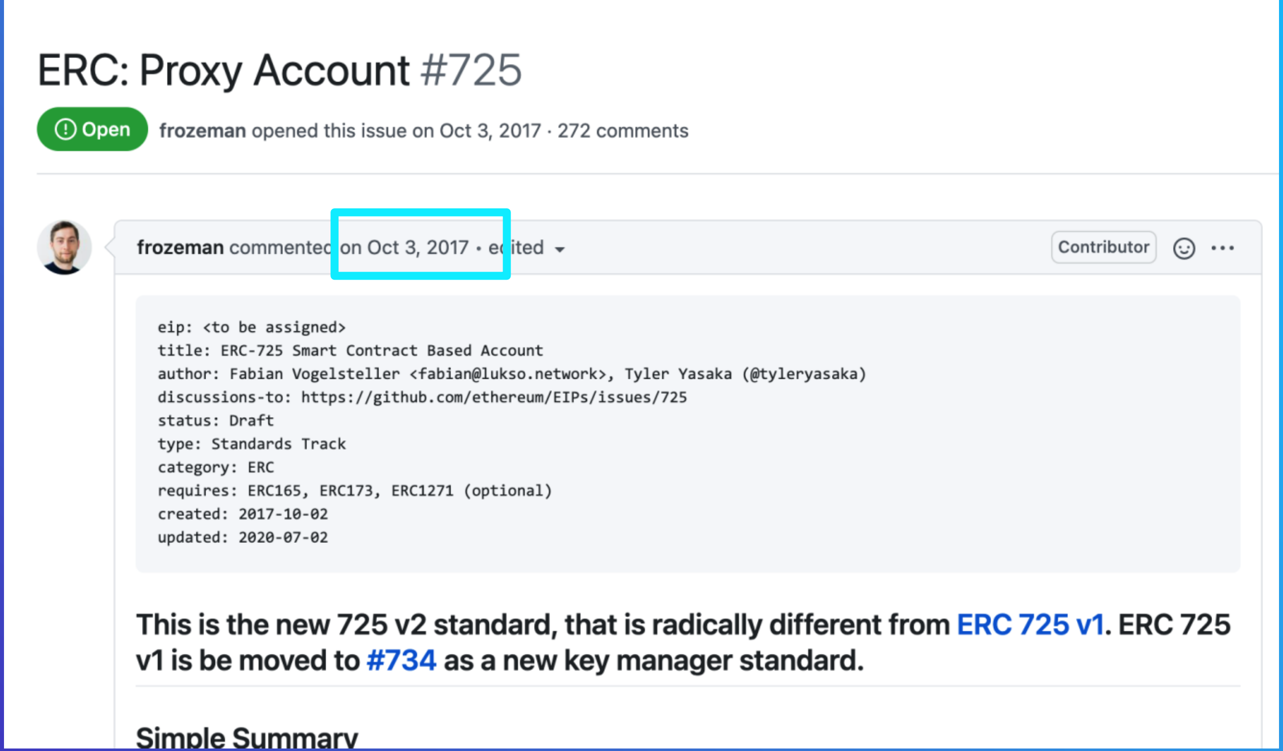
ERC: Identity System



ERC725’s Transition and Future

1. Current state of ERC725
2. Examination of ERC725’s issues
3. Possibility of application in IoT

ERC725 v2 Proposal



ERC: Proxy Account #725

Open frozeman opened this issue on Oct 3, 2017 · 272 comments

frozeman commented on Oct 3, 2017 · edited

Contributor

```
eip: <to be assigned>
title: ERC-725 Smart Contract Based Account
author: Fabian Vogelsteller <fabian@lukso.network>, Tyler Yasaka (@tyleryasaka)
discussions-to: https://github.com/ethereum/EIPs/issues/725
status: Draft
type: Standards Track
category: ERC
requires: ERC165, ERC173, ERC1271 (optional)
created: 2017-10-02
updated: 2020-07-02
```

This is the new 725 v2 standard, that is radically different from ERC 725 v1. ERC 725 v1 is be moved to #734 as a new key manager standard.

Simple Summary

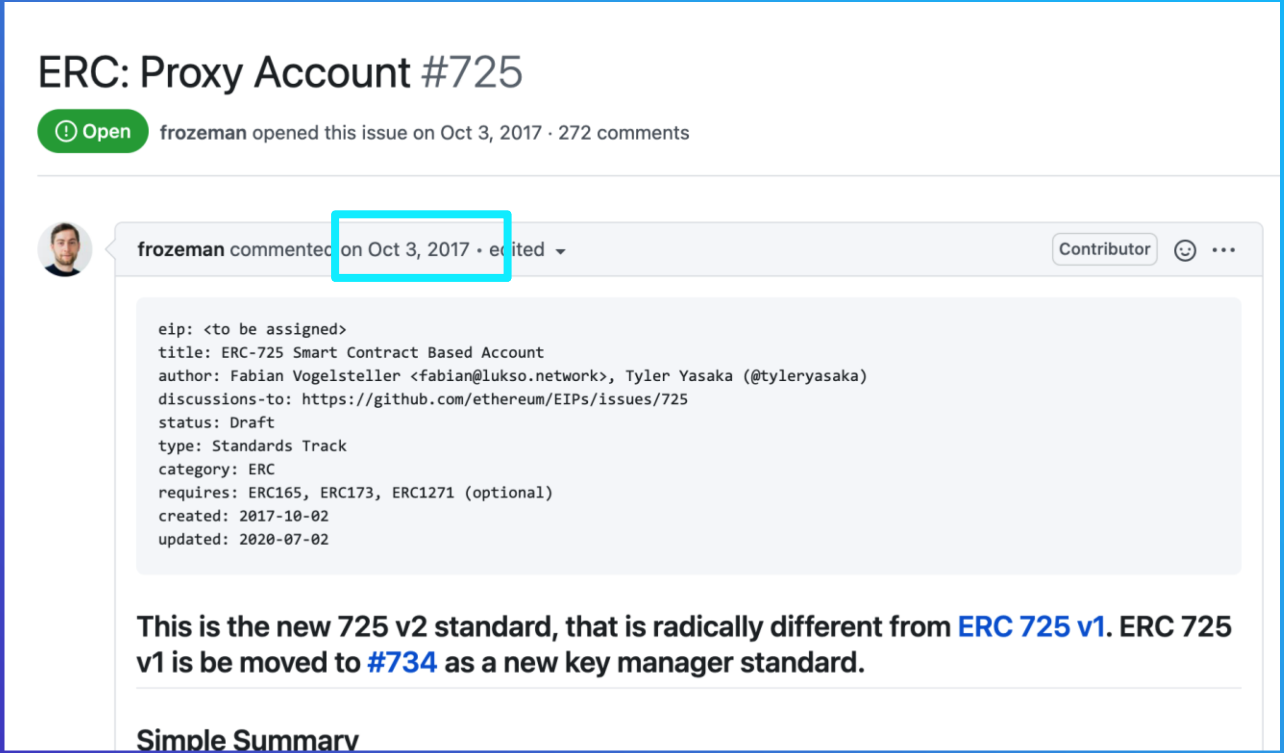
https://github.com/ethereum/EIPs/issues/725

ERC725 : v1→v2

1. **Aiming for a more comprehensive framework than v1**
2. **Can execute and deploy other smart contracts**
3. **Smart contract = ID → "Can execute (access)" is proof of the ID**
4. **Formed of 2 subcontracts**

- ERC725X: Access (execute, deploy) other smart contracts
- ERC725Y: Contract owner can register data indiscriminately

ERC725 v2 Proposal



ERC: Proxy Account #725

frozeman opened this issue on Oct 3, 2017 · 272 comments

frozeman commented on Oct 3, 2017 · edited

```
eip: <to be assigned>
title: ERC-725 Smart Contract Based Account
author: Fabian Vogelsteller <fabian@lukso.network>, Tyler Yasaka (@tyleryasaka)
discussions-to: https://github.com/ethereum/EIPs/issues/725
status: Draft
type: Standards Track
category: ERC
requires: ERC165, ERC173, ERC1271 (optional)
created: 2017-10-02
updated: 2020-07-02
```

This is the new 725 v2 standard, that is radically different from ERC 725 v1. ERC 725 v1 is be moved to #734 as a new key manager standard.

Simple Summary

https://github.com/ethereum/EIPs/issues/725

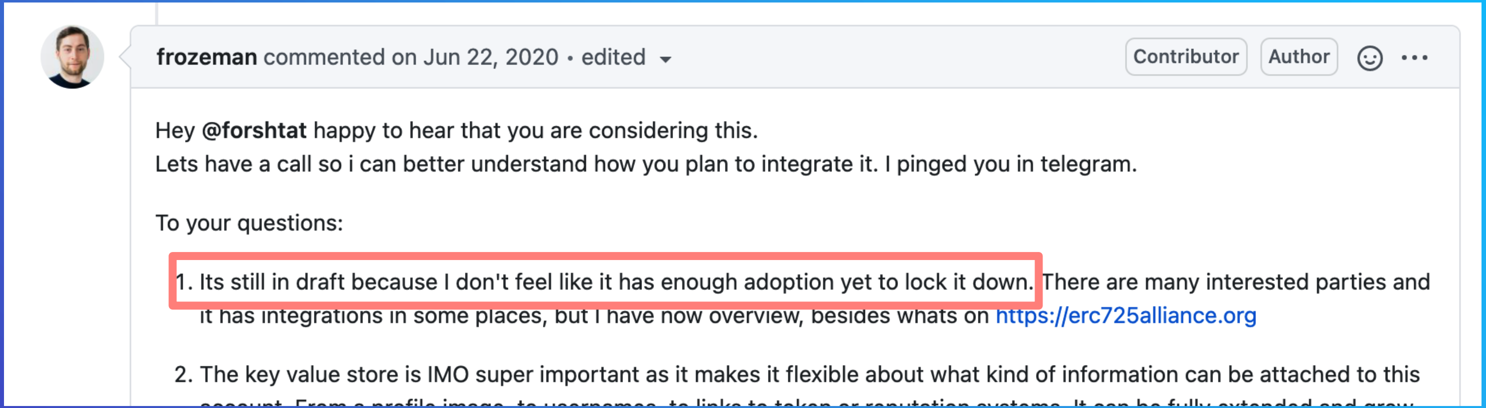
ERC725’s Current State and Issues

1. **Fabian himself is not satisfied with the draft**

2. **ERC725 only exists due to LUKSO**

3. **Meta transactions are difficult (will it scale?)**

Fabian Himself Is Not Satisfied with the Draft



frozeman commented on Jun 22, 2020 • edited

Hey **@forshtat** happy to hear that you are considering this.
Lets have a call so i can better understand how you plan to integrate it. I pinged you in telegram.

To your questions:

1. Its still in draft because I don't feel like it has enough adoption yet to lock it down. There are many interested parties and it has integrations in some places, but I have now overview, besides whats on https://erc725alliance.org
2. The key value store is IMO super important as it makes it flexible about what kind of information can be attached to this account. From a profile image, to usernames, to links to token or reputation systems. It can be fully extended and grow

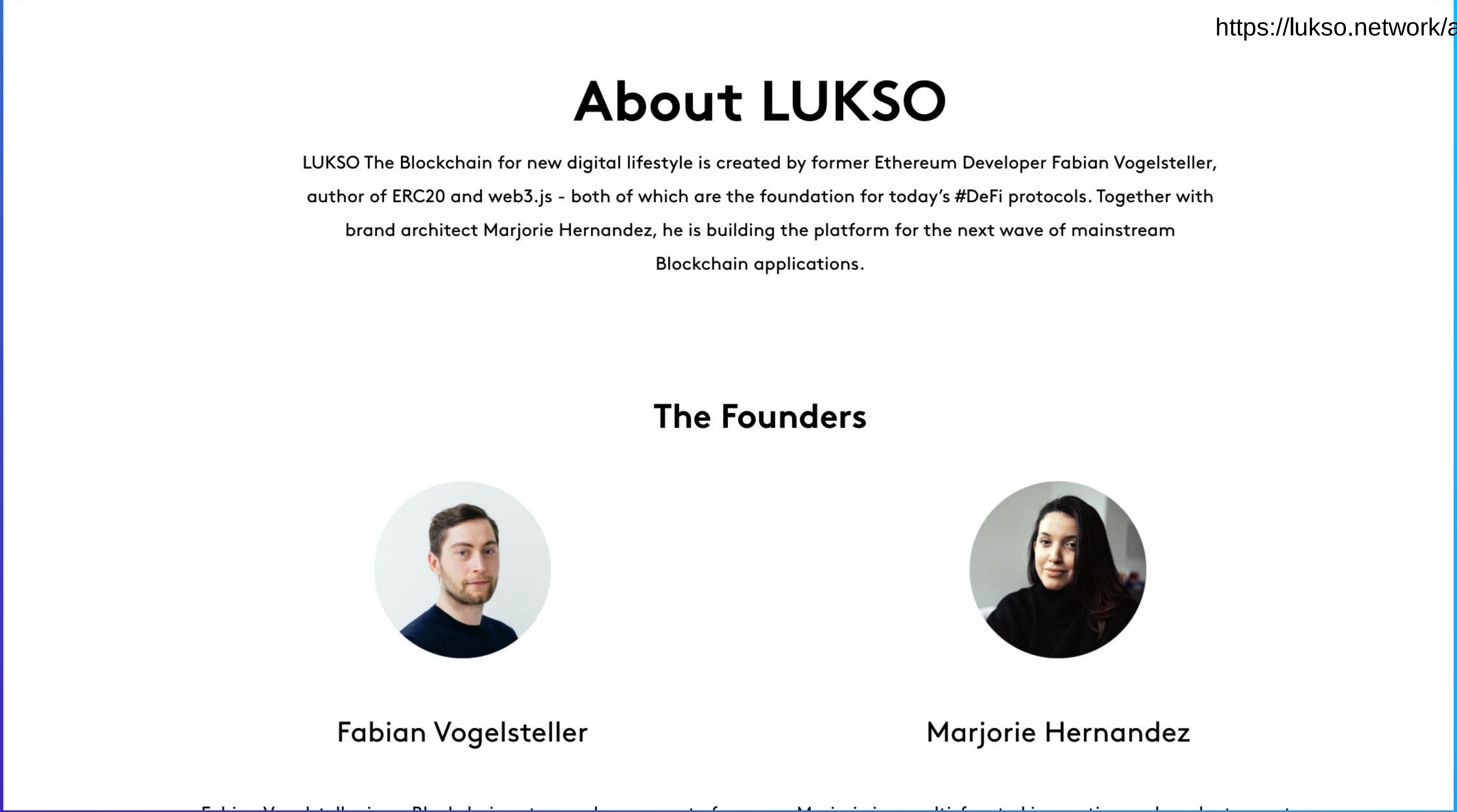
- **Meanwhile, the outline has been solidified.**
- **The ERC725 package has been made public (November 2020) (beta version) on npm**
- **The above is also used in LUKSO's test version (LUKSO's git repository)**

ERC725 Only Exists Due to LUKSO

LUKSO

LUKSO ・・・ Blockchain infrastructure (trading platform) that provides standards and resolutions to increase transparency for consumer goods (physical or digital)

https://lukso.network/about



About LUKSO

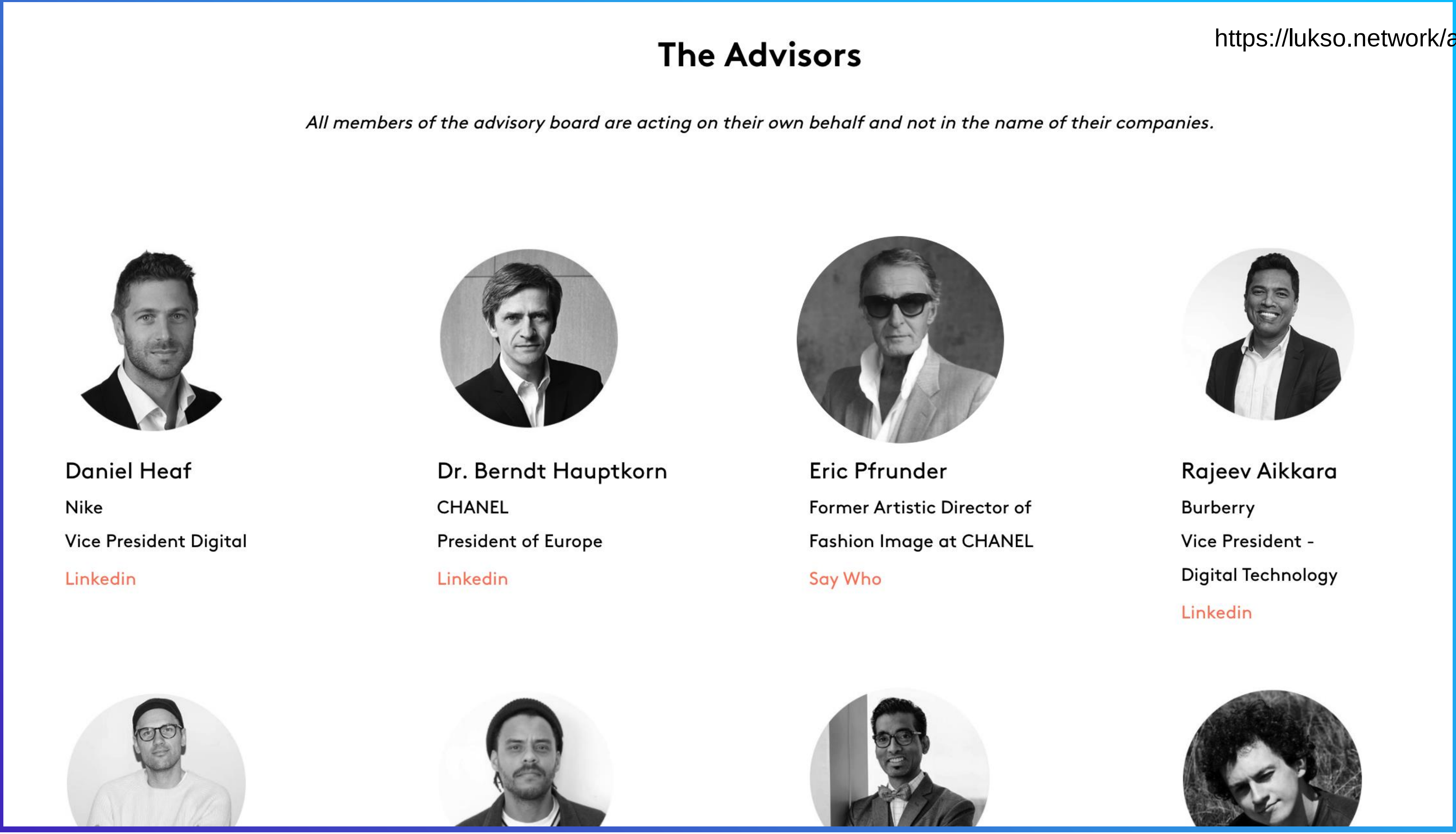
LUKSO The Blockchain for new digital lifestyle is created by former Ethereum Developer Fabian Vogelsteller, author of ERC20 and web3.js - both of which are the foundation for today's #DeFi protocols. Together with brand architect Marjorie Hernandez, he is building the platform for the next wave of mainstream Blockchain applications.

The Founders

Fabian Vogelsteller

Marjorie Hernandez

https://lukso.network/about



The Advisors

All members of the advisory board are acting on their own behalf and not in the name of their companies.

Daniel Heaf

Nike

Vice President Digital

Linkedin

Dr. Berndt Hauptkorn

CHANEL

President of Europe

Linkedin

Eric Pfrunder

Former Artistic Director of

Fashion Image at CHANEL

Say Who

Rajeev Aikkara

Burberry

Vice President -

Digital Technology

Linkedin

Meta Transactions Are Difficult (Will It Scale?)

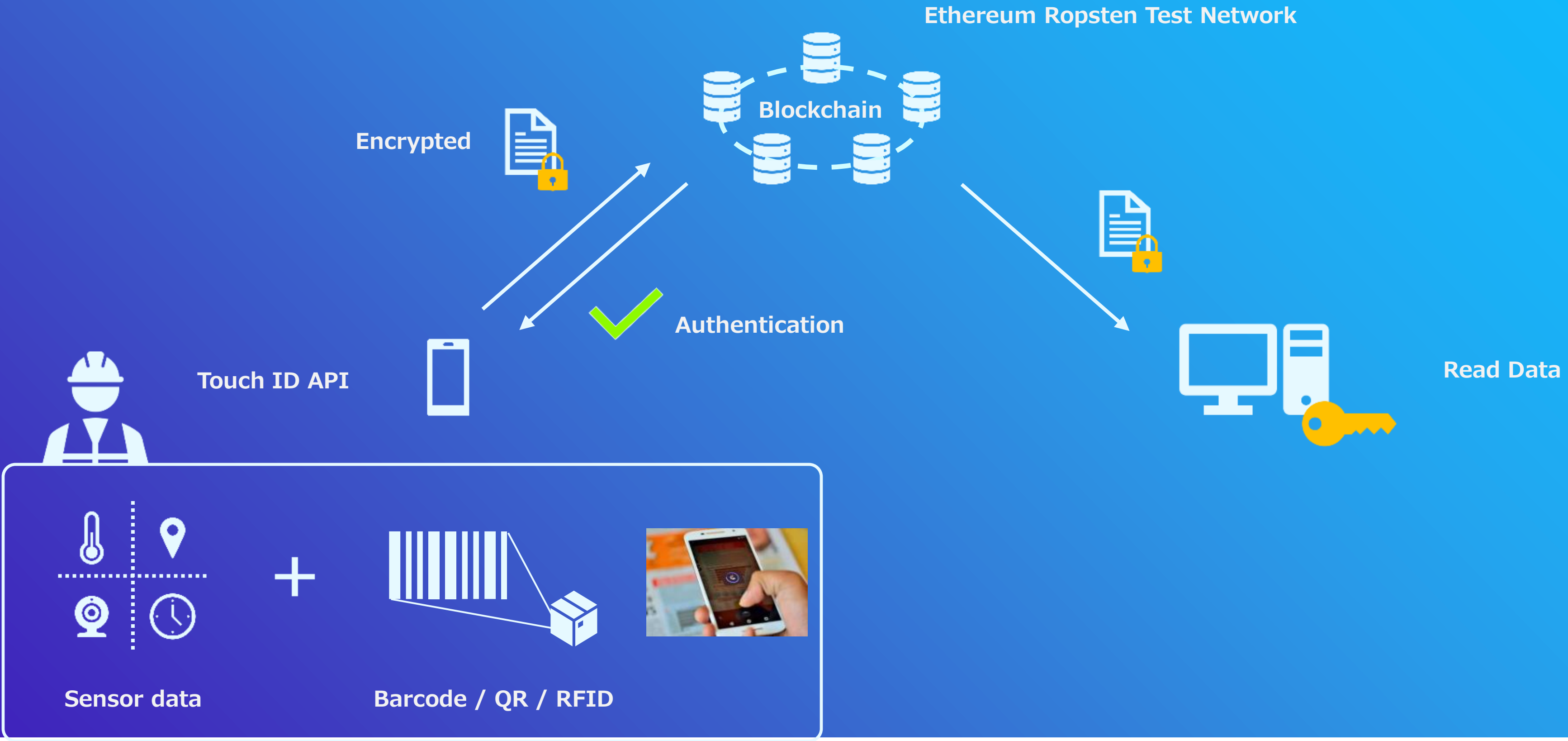
- In the GSN (Gas Station Network) a parameter of 20 bytes called msg.data is used as the proven sender address, instead of msg.sender.

- However, only msg.sender can execute or run setData in ERC725.

ERC725’s Transition and Future

1. Current state of ERC725
2. Examination of ERC725’s issues
3. **Possibility of application in IoT**

Application in IoT



Ethereum Ropsten Test Network

Blockchain

Encrypted

Authentication

Touch ID API

Read Data

Sensor data

Barcode / QR / RFID

Application in IoT

Verifying and Tracking Quality Inspections

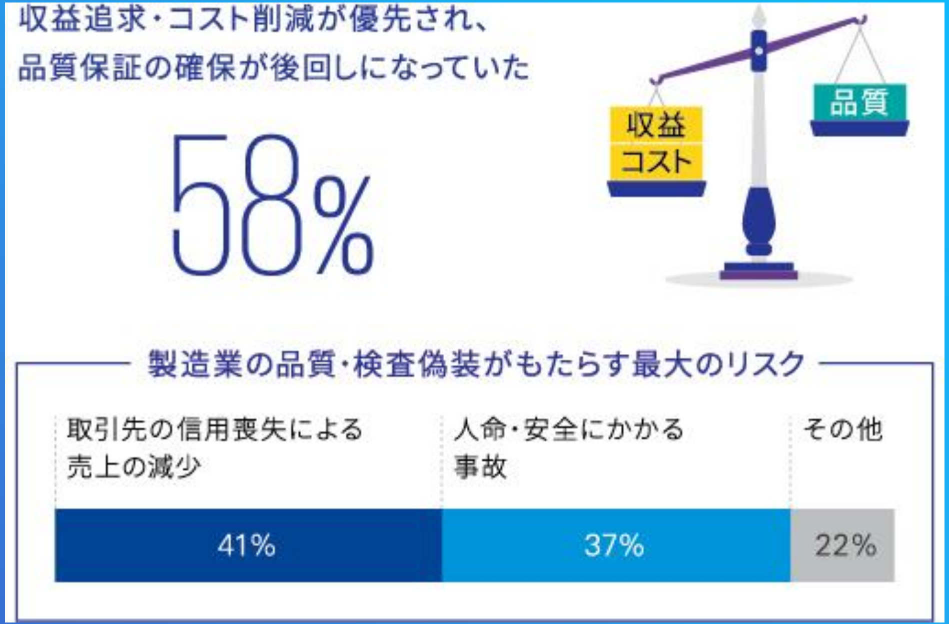
Issues

Inspection Costs and Fraud Risks②

The most common cause for disguising quality inspection among companies was “the pursuit of profit and reduction of costs.” The most common risk among companies was “decreased sales due to the loss of trust from partners.”

Although there are hopes for using AI (artificial intelligence) to handle fraud, there are few cases of actual utilization at present.

In a study by KPMG (2019), approximately half of companies responded that the utilization of AI to prevent or detect fraud is “effective.” Meanwhile, approximately 40% of companies responded that the effectiveness of AI in handling fraud is “unclear.” This can be considered to be caused by the lack of specific case examples of AI utilization, as only 2% of companies had actually introduced AI to handle fraud.



収益追求・コスト削減が優先され、
品質保証の確保が後回しになっていた

58%

製造業の品質・検査偽装がもたらす最大のリスク

取引先の信用喪失による売上の減少	人命・安全にかかる事故	その他
41%	37%	22%

https://home.kpmg/jp/ja/home/insights/2019/03/fraud-survey-6.html

Issues

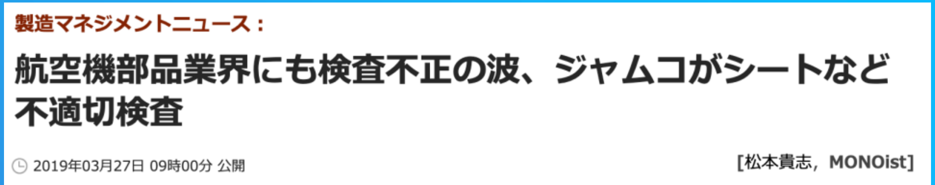
The discovery of **unqualified inspections** occurs repeatedly in the aircraft parts industry

JAMCO announced on March 26th, 2019 that inappropriate inspections were being carried out in its business to manufacture parts used inside aircraft. This was found both for this company and Miyazaki JAMCO, its manufacturing subsidy, as there were inspections by unqualified personnel and failure to conduct acceptance inspections.

Blockchain can only ensure the information that is registered to blockchain. If the information itself is incorrect, nothing can be done.

Also, a system to objectively ensure “human fairness (whether the data was entered correctly),” which serves to relay the data, does not exist at present, and humans also conduct the checks.

https://monoist.atmarkit.co.jp/mn/articles/1903/29/news010_2.html



製造マネジメントニュース：

航空機部品業界にも検査不正の波、ジャムコがシートなど不適切検査

2019年03月27日 09時00分 公開 [松本貴志，MONOist]

https://monoist.atmarkit.co.jp/mn/articles/1903/27/news045.html

Focus on Manufacturing Inspections and Conduct Tracking

Inspection of parts and quality is carried out repeatedly at each location.

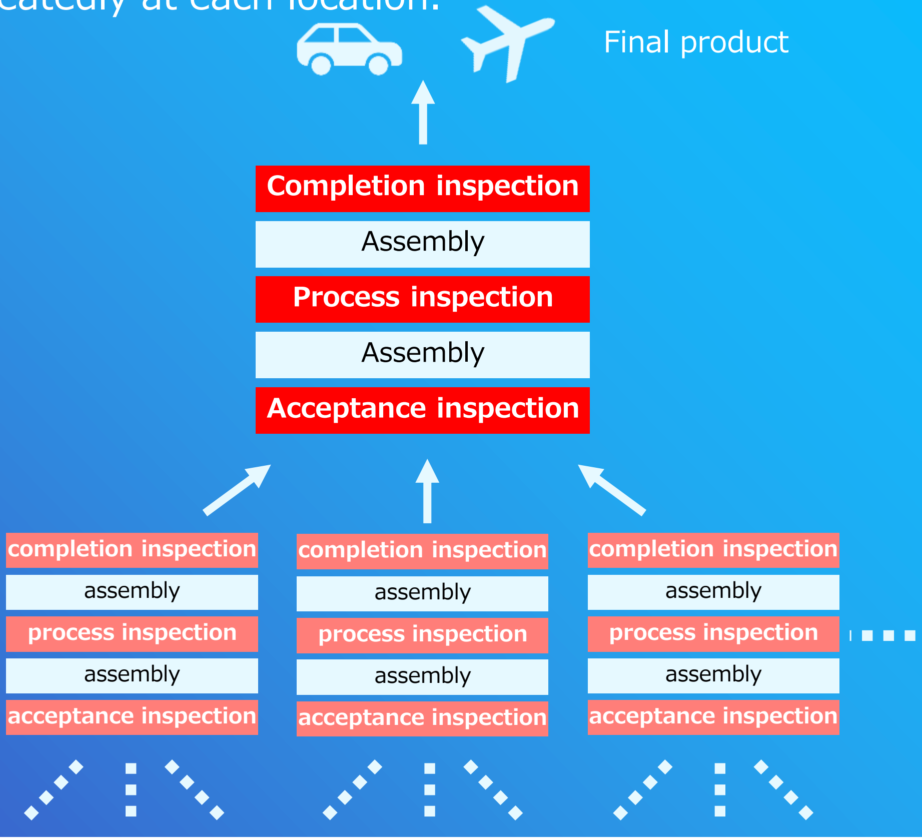
1. **Repeated inspections are needed**

   → Opportunity to reduce costs

2. **Lack of systems and regulations that ensure inspections**

3. **Manual inspections tend to lead to fraud**

4. **Information about the lack of inspections is hard to share**



Thank You