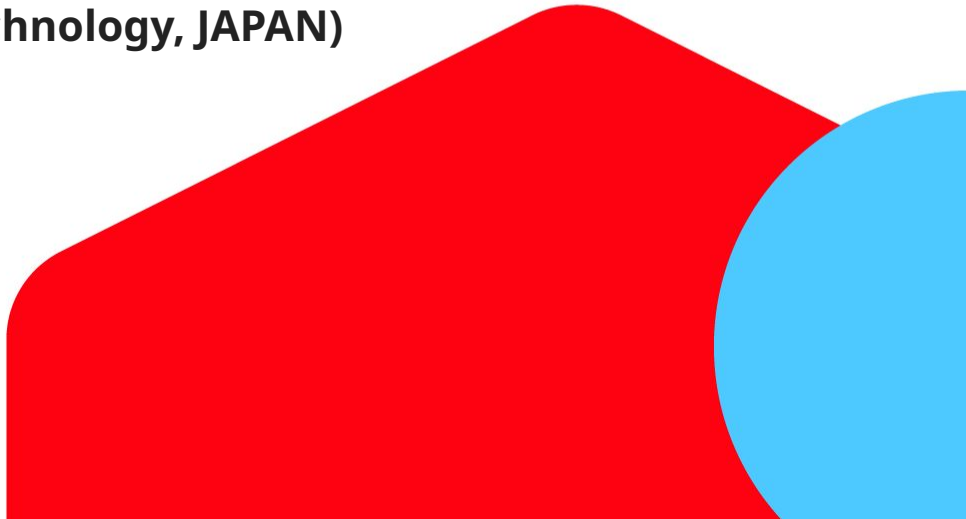
May 29, 2024. 9:30am – 9:45am
2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)

Pragmatic Analysis of Key Management for Cryptocurrency Custodians

Yuto TAKEI
(Mercari, Inc. and Tokyo Institute of Technology, JAPAN)

Kazuyuki SHUDO
(Kyoto University, JAPAN)

mercari



Outline of the presentation

1. Research motivation
2. Related work
3. Risk analysis on signing system
4. Conflict of security measures
5. Consideration with hardware or custody wallets
6. Introducing EXTREME-COLD
7. Conclusion

mercari

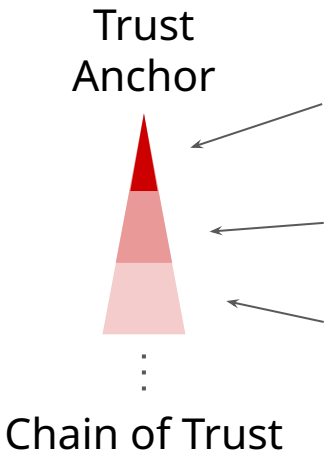
Research Motivation

- Cryptocurrency exchanges have to secure funds in custody.
- Cyber attacks happens against cryptocurrency exchanges:
  - Mt. Gox lost 740,000 bitcoins (2014).
  - Bitfinex lost 120,000 bitcoins (2016).
  - Coincheck lost around 58 billion yen worth of NEM (2018).
  - KuCoin lost 28 billion yen equivalent multiple assets (2020).
- Many researchers focus on wallets, while only a few focus on integration to exchanges as a system.
  - Exchanges are subject to regulations and audits.
    (e.g. rule of 95% cold in Japan)

Related Work

Key management has been widely studied.

DNSSEC's Root KSK management



Root KSK (Key Signing Key)
managed by IANA and PTI

Root ZSK (Zone Signing Key)
managed by Verisign

Sub-domain's KSK and ZSK

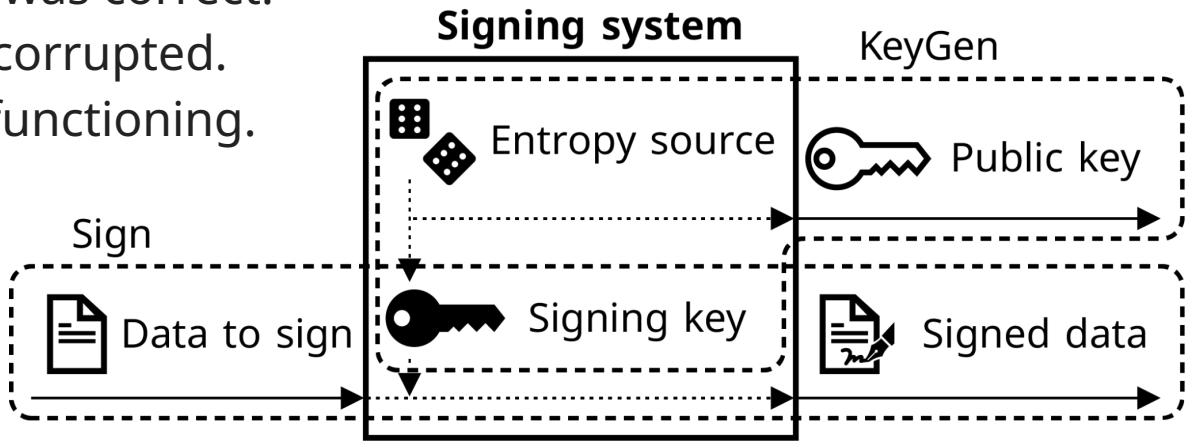
Recordings publicly available:
iana.org/dnssec/ceremonies

Cryptocurrency Context

- Management methods:
  - Software wallets
    - Smartphone-based
    - QR-code
  - Hardware wallets
    - Trezor, Ledger, etc.
    - Raspberry Pi
- Attack methods
  - Attacking weak keys
  - Decrypting wallets
  - Side-channel attacks

Risk Analysis on Signing System

- The key is not compromised. (Confidentiality)
  - The key is securely generated.
  - The key is not exposed.
- The key is usable. (Availability and Integrity)
  - The public key was correct.
  - The key is not corrupted.
  - The system is functioning.



Definition of risk

$$\text{risk} = \mathbf{f}\,(\,\text{impact}\,,\,\text{likelihood}\,)$$

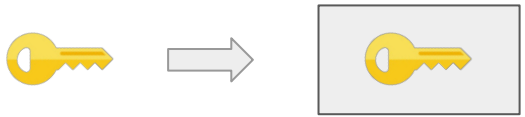
risk *: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.*
(https://csrc.nist.gov/glossary/term/risk)

Conflict of Security Measures

Measures for Confidentiality and Availability are often in conflict.

To enhance confidentiality:

- Encrypt the key
- Requires additional authentication



Hardened

To enhance availability:

- Increase the number of backups
- Add more operators

Duplicated

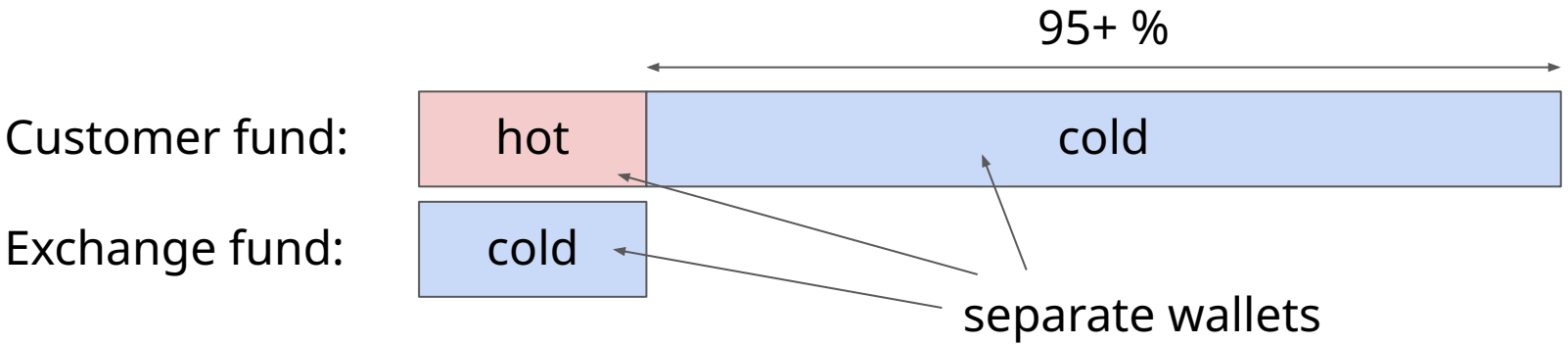
Consideration with Hardware or Custody Wallets

- Transparency
  - Implementation details are often blackboxed.
  - Security audit and assessment may vary.
- License
  - Cryptocurrency related functions are not included in FIPS 140-3.
- Internet Connectivity
  - Some products require operating online.

Largely depends on the risk management policy of exchanges.
Hardware or custody wallets also come with many benefits!

(Example) Japan's regulatory requirement

- Keep 95+ % of customer funds in the cold wallet.
  (Cold wallet = never connected to the Internet, not even once)
- Isolate customer and exchange fund.
- Keep equal or more amount in cold than the hot wallet.



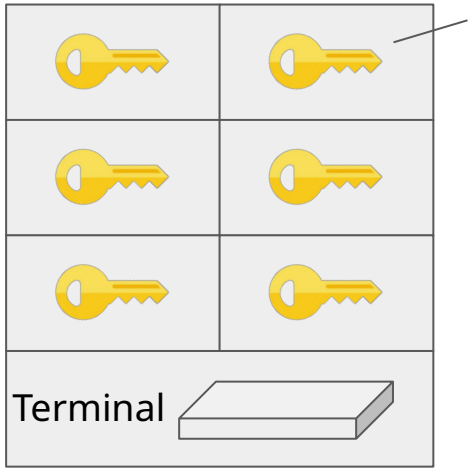
mercari

Introducing Extreme-Cold

- Keys are completely offline-managed.
- Resistant to side channel attacks.
- Maximum transparency (reproducible architecture).

Design of KMF

Metal detector



Key media (e.g. USB sticks)
Duplicated for availability

N+1 lockers

Key Management Facility (KMF)

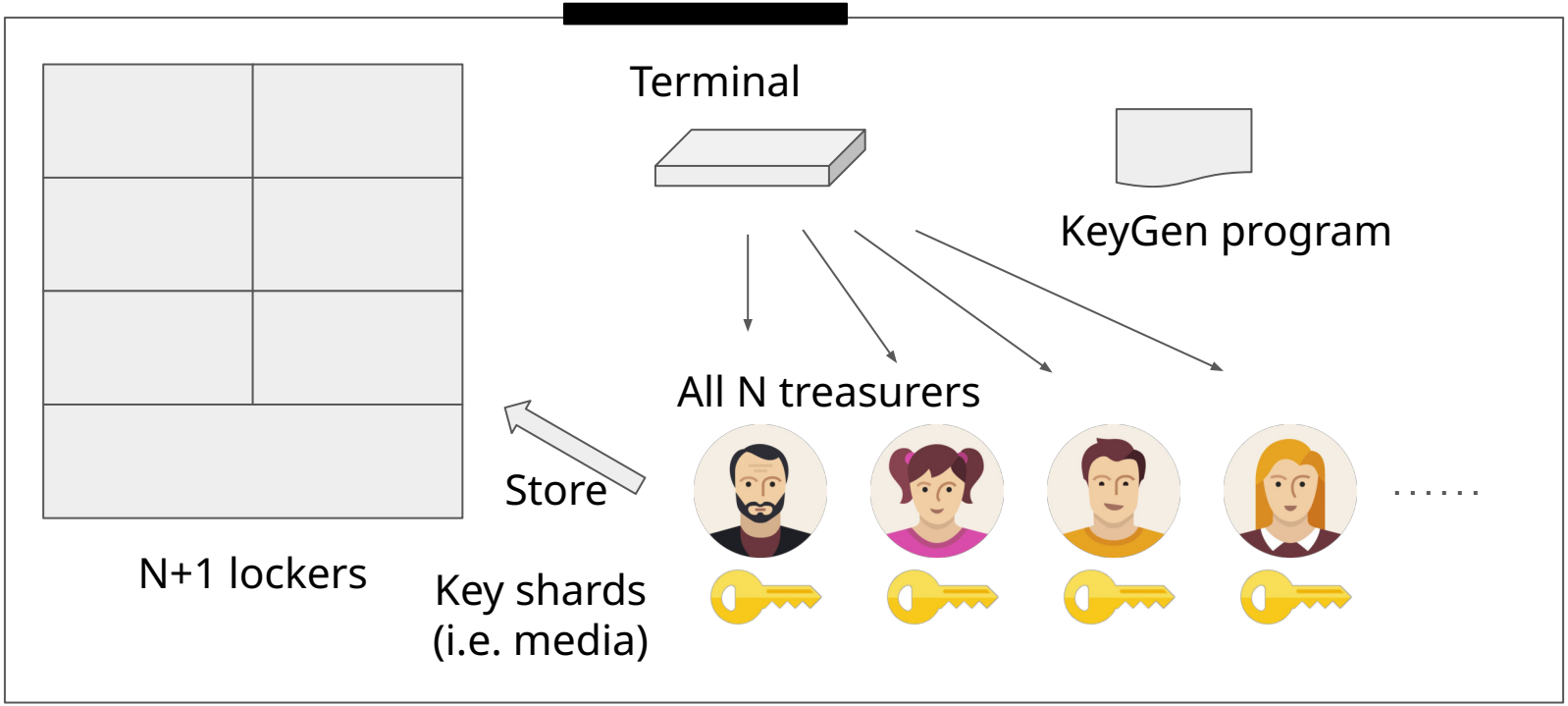
Treasurers and Assumptions

- M treasures (= operator) among N can activate and use the key.
- Treasurer may behave incorrectly.
  - They may bring out the key.
  - They may sabotage the key.

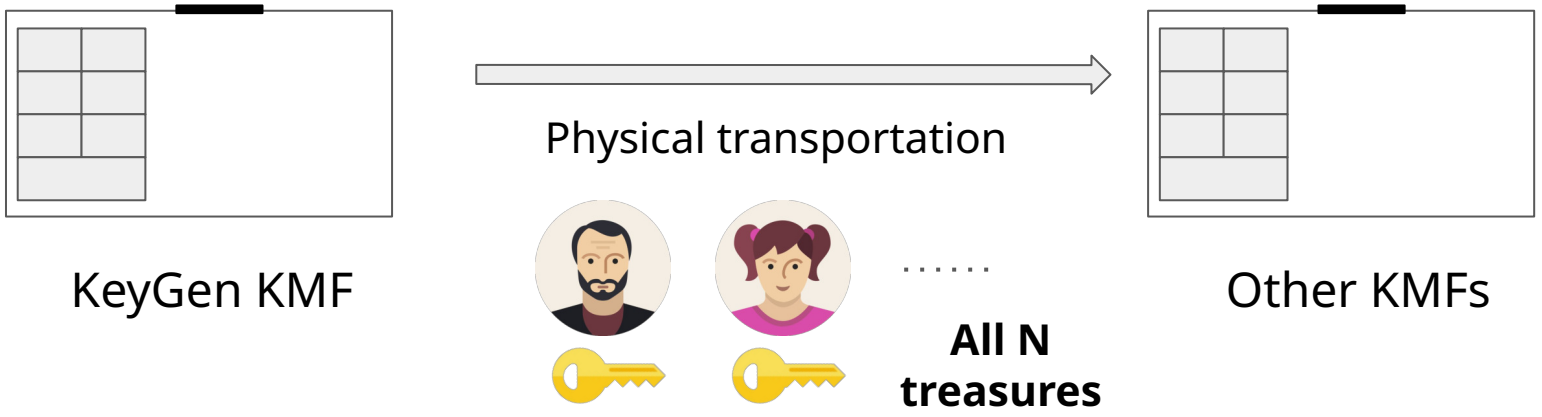
Key splitting technique:

- Multi-signature addresses (BIP-16)
- Shamir’s Secret Sharing (SSS)
- Threshold Signature Scheme (TSS)

Generating New Key (KeyGen)

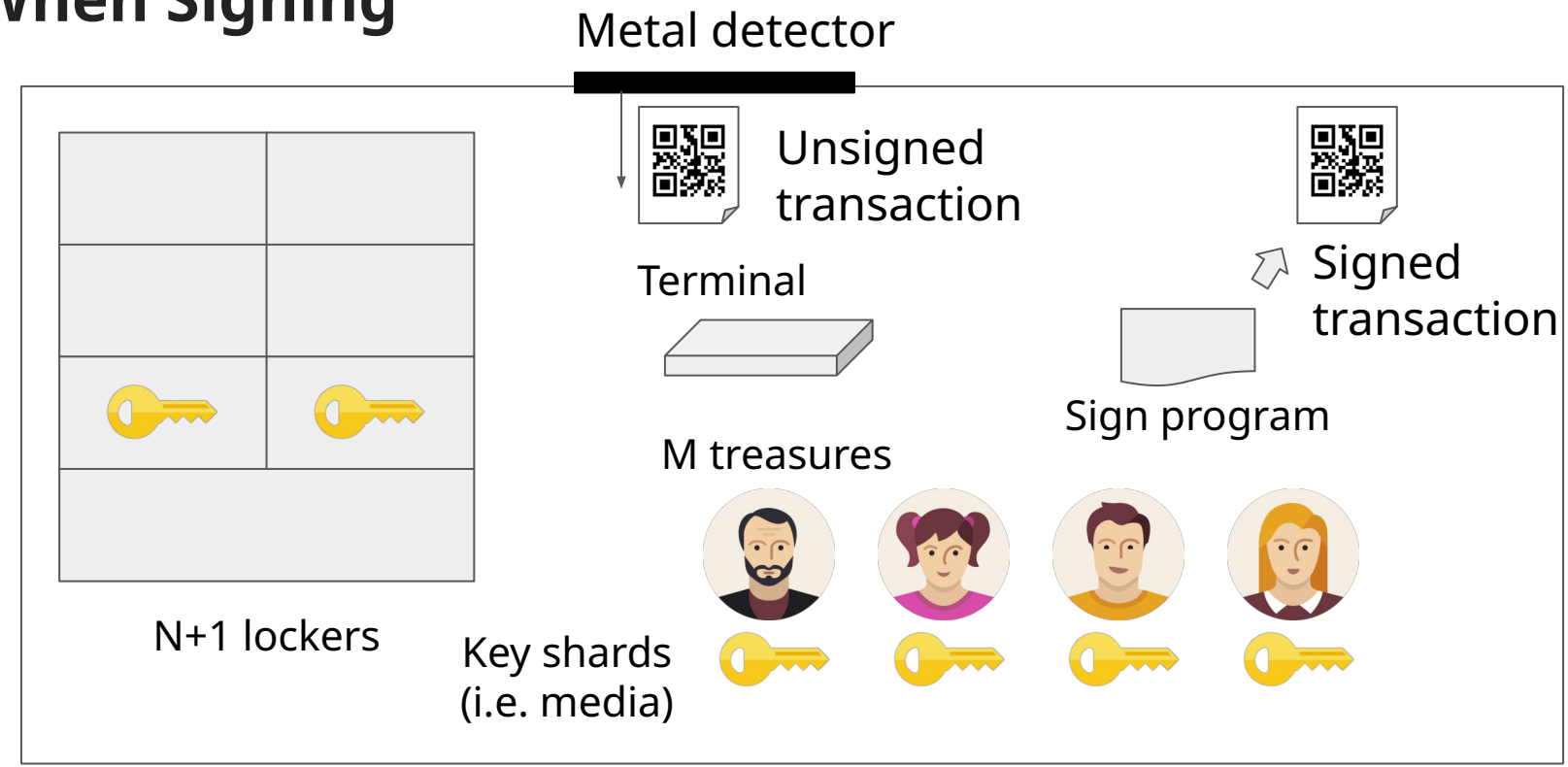


Transportation of New Key



- Deploy all key shards before start operation.
- All keys are go when shards are free of defects.

When Signing



Software of KeyGen and Sign

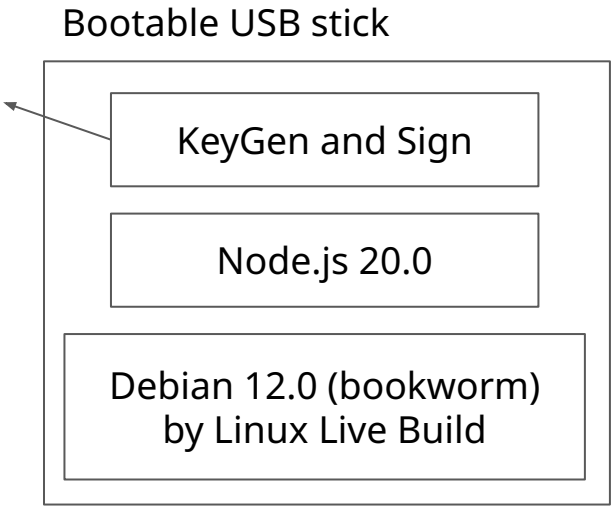
- Completely self-contained offline programs written in TypeScript.
- Deterministic Random Bit Generator (DRBG) is used as CSPRNG.

```
# Wallet secret key generator

This program generates the private key t
as a hierarchical wallet based on BIP32.

We will proceed with the following steps

1. Input a random string.
2. Generate a secure password.
3. Provide the number of treasurers.
4. Save the generated private key.
```



Evaluation of Extreme-Cold

- Security
  - Resistant to side channel attacks (including BeatCoin’s methods)
- Operability
  - Daily performances: ~ 30 minutes to complete signing session.
- Scalability
  - Number of transactions can be scalable (as long as printable).
  - Adding new key requires heavy operation by design.
- Maintainability
  - Update treasurer : Change of N is easy. Change of M requires KeyGen.
  - Update software : Old media should be destroyed
- Cost : 3,000+ USD / KMF

Conclusion

- Research on key management for exchanges is necessary.
- Regulatory requirements may apply.
- Proper risk control needs to be in place.
- Extreme-Cold is proposed as a reference cold wallet implementation for cryptocurrency exchanges.
- Proven attack resistance and feasibility.