ICCCN 2017
Workshop on Privacy, Security and Trust in Blockchain Technologies

Long-term public blockchain: Resilience against Compromise of Underlying Cryptography

August 3 2017

Masashi Sato

SECOM Co., Ltd.
Intelligent Systems Laboratory
Email: masas-sato@secom.co.jp

Shin'ichiro Matsuo

MIT Media Lab.
Email: matsuo@media.mit.edu

Background

- Security of blockchains replies on cryptographic technologies such as digital signature and hash algorithm.
- Compromise of cryptographic technologies may cause destruction of assets and a currency on a blockchain.
- It is very important to prepare a mechanism to transition of underlying cryptographic technologies.
- We consider a transition mechanism of digital signature and hash algorithm on a blockchain.

Underlying cryptographic technologies

For example, Bitcoin relies on the following cryptographic technologies:

- Digital signature to transaction
  - used with (Cryptographic) Hash Function
- Hash function used for generating transaction ID
- Hash function used in Hash tree of transaction
- Hash function used in chain of block

Impact analysis of blockchain protocol when these algorithms are broken was proposed:

I. Giechaskiel and C. Cremers and K. Rasmussen, “On Bitcoin Security in the Presence of Broken Crypto Primitives,” IACR ePrint Archive, 2016/167

Impacts when cryptographic technologies are broken

- Digital signature
  - Malicious user can duplicate a signing key and steal assets of a valid user.

- Hash function
  - Transaction stored in past block can be altered by collision of hash value of transaction.
    - Example: double spending, transfer unspent coins to another address
  - A set of block which is generated before a past certain time can be replaced by collision of hash value of block.
    - Example: double spending , erase history of transactions

Our proposal

We propose a method to extend the validity of data on the blockchain even when the underlying cryptographic algorithm is compromise.

- Transition of Digital Signature
  - Key length or digital signature algorithm used in software need to be upgraded.
  - Each user must create new key pair and transfer assets to the new key.
- Transition of Hash Function
  - Software needs to be changed to use new hash function, but also old weak blocks must be protected by new hash function.
  - We propose the mechanism of protecting old blocks, Basic Transition Procedure.

Basic Transition Procedure

- Basic Transition Procedure is a transition mechanism of hash function in order to maintain authenticity of transactions recorded in past blocks.
- This method has similar concept of ETSI long-term signature scheme.
  - But this method does not requires any centralized server.

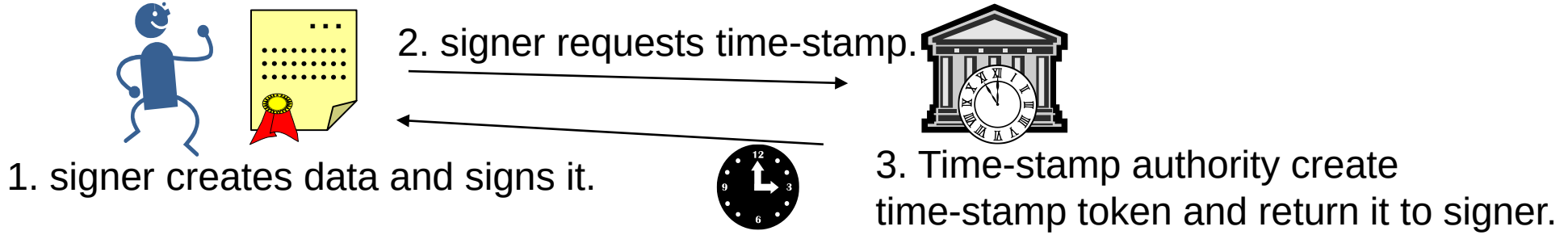
ETSI Long-term signature

- ETSI (European Telecommunications Standards Institute)
- ETSI provides the standards regarding long-term signature.
  - EN 319 122-1 V1.1.1, Electronic Signatures and Infrastructures (ESI);CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures, ETSI, 2016
- This mechanism is based on PKI (Public Key Infrastructure).

What is the concept of ETSI Long-term signature?

There are 2 important concepts: Signature time-stamp and Archive time-stamp

Signature time-stamp provides a proof of existence of digital signature and signing data.

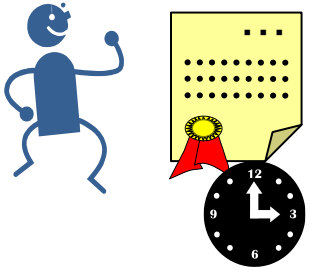


- Signature time-stamp token contains time information which is provided by time-stamp authority.
- Signature time-stamp token also relies on cryptographic technologies (signature and hash). Therefore, signature time-stamp become weak in future.

What is the concept of ETSI Long-term signature?

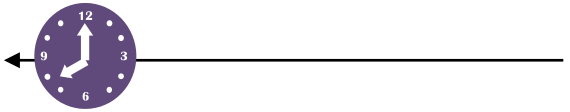
There are 2 important concepts: Signature time-stamp and Archive time-stamp

Archive time-stamp enhances cryptographic algorithms of signature and signature time-stamp.



1. send signature data and Signature time-stamp

2. Time-stamp authority create new Time-stamp token on these data with more secure cryptographic algorithms.



The property of ETSI long-term signature

- ETSI long-term signature needs trusted third party.
- ETSI long-term signature proves the time information.

Public blockchain doesn't have these properties.

Proof of Existence (PoE) and Secure transition

- From the core concept of ETSI long-term signature, we define PoE and Secure transition of hash function regarding public blockchain.

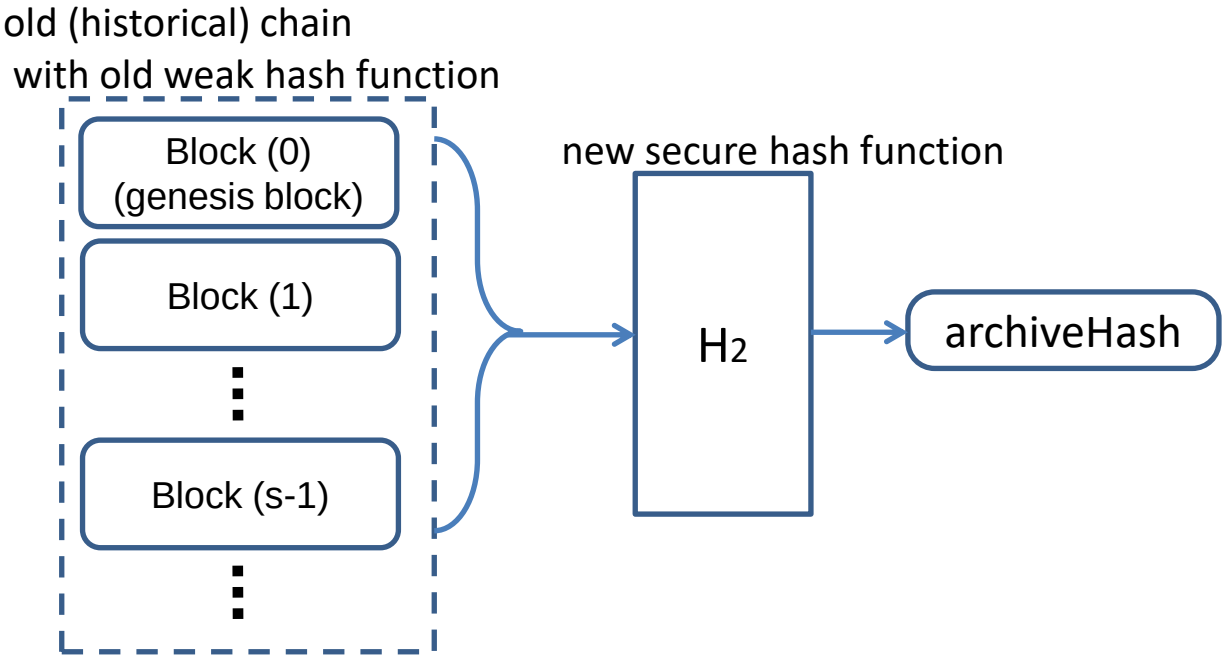
- PoE provides a proof of time or time-wide order when a transaction is generated. (Definition 4.1, 4.4 in detail)
  - With regard to public blockchain, a sequence of hash value of block is functioned as PoE of transaction.

- Secure transition is to provide transition without altering signature, transaction and PoE. (Definition 4.2 in detail)
  - In order to perform secure transition, it is necessary to ensure sequence of hash value of block.

Process of Basic Transition Procedure (step 1)

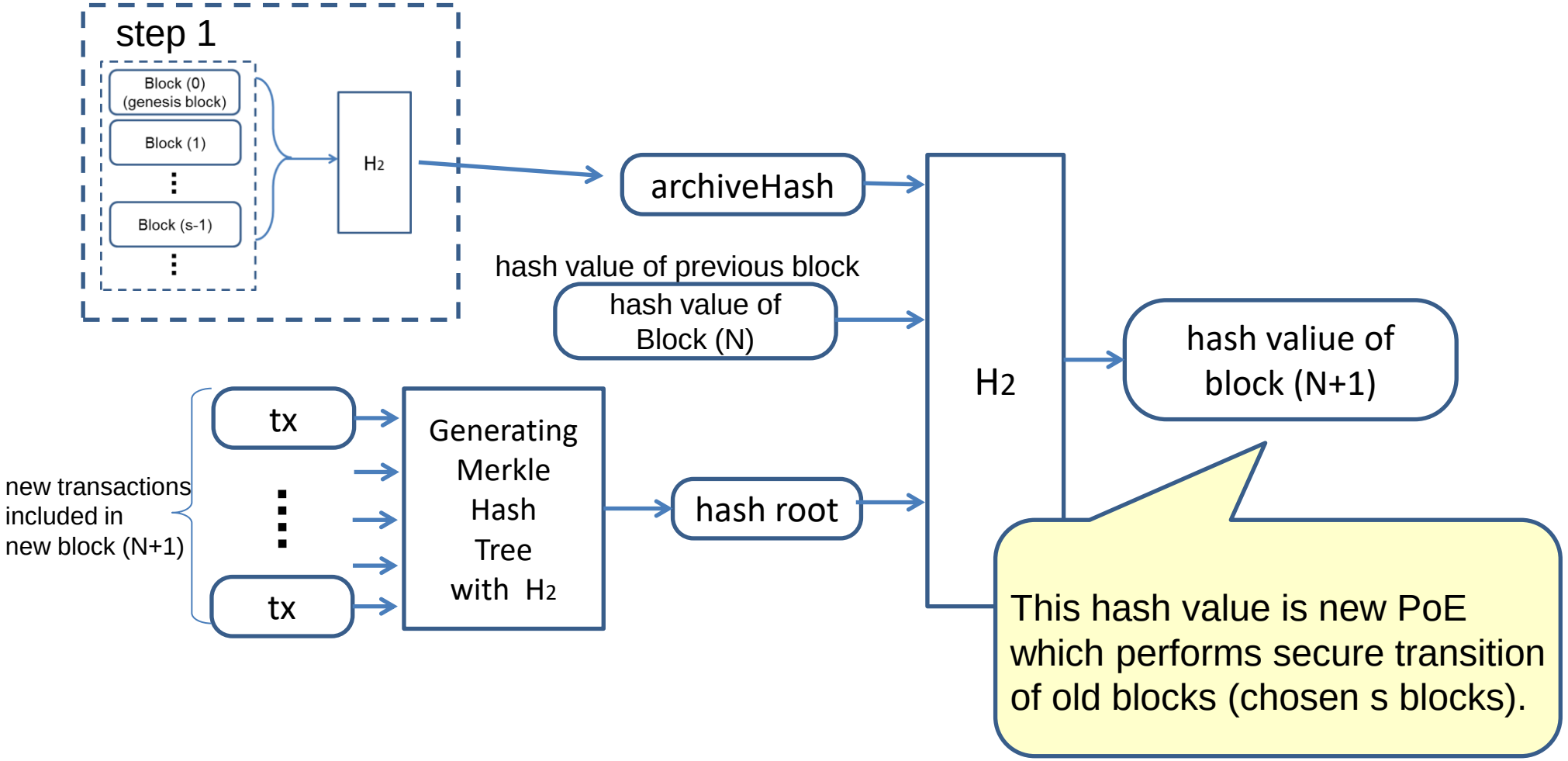
- Basic Transition Procedure is executed at time of generating new block which uses new hash function.
- 1st step of this procedure is to generate archiveHash.

- Transition procedure starts after number N (= r * s) block.
- This process is a part of generating new block (number N+1)
- .A sequence of s blocks is chosen from old chain.



Process of Basic Transition Procedure (step 2)

- 2nd step of this procedure is to generate new block including archiveHash.



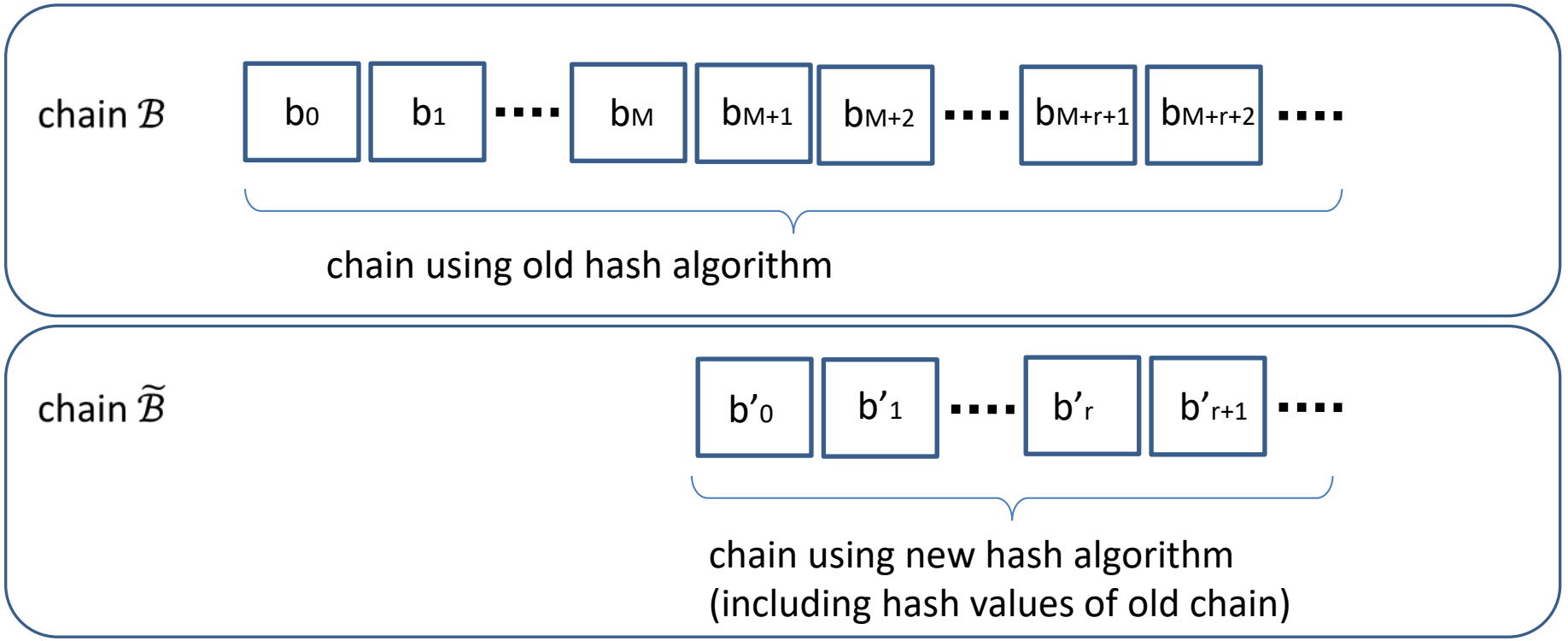
Process of Basic Transition Procedure (next)

- For generating new block (N+2), old blocks between s and 2s-1 are chosen from old chain. Step1 and 2 are executed.
- By repeatedly executing this procedure, secure transition of all old blocks (from 0 to N) are completed at the time when new block (N+r) is generated.

Feature of Basic Transition Procedure

- Basic Transition Procedure is a method of secure transition regarding hash function of block.
  - This method ensures authenticity of transactions and proof of existence of transactions for long-term.
- This method can be performed without trusted third party.
  - Steps of transition are integrated to new block generation.

Extension of Basic Transition Procedure



Conclusion

- We propose a scheme of transition of digital signature and hash function regarding public blockchain.
- We utilize similar concept of long-term signature scheme standardized by ETSI, but our proposal can be performed without trusted third party.
- Basic Transaction Procedure can make a transition with a certain amount of time (e.g. several years).

Thank you.