Ring Signatures for Blockchain

Eiichiro Fujisaki
（藤崎 英一郎）

JAIST（北陸先端科学技術大学院大学）

Nov. 19, 2018 @ ECC 2018

What I am talking today.

- Bitcoin: Blockchain-based cryptocurrency
  - Overview
- Ring signature and its variants
  - Linkable / Traceable ring signatures
- About Monero
  - Application of Linkable / Traceable ring signature to blockchain-based cryptocurrency.
- Traceable ring signature
  - Techniques, and extensions
- Recent progress on ring signatures
- Conclusion

Bitcoin: A peer-to-peer electronic cash system [Nakamoto2008]

Key Ingredients:

- Transactions,
- Blockchain,
- Mining (proof of work (POW))

Transaction (取引)

"Goal: Send 1 BTC from Alice to Bob"

Address: A (made from Alice's pk)

Address: B(made from Bob's pk)

Ex.: 1G2jt5WeGhqWtDKEkcKY2GrZKjfYsuiVxX (A Bitcoin Address is the hash of public-key.)

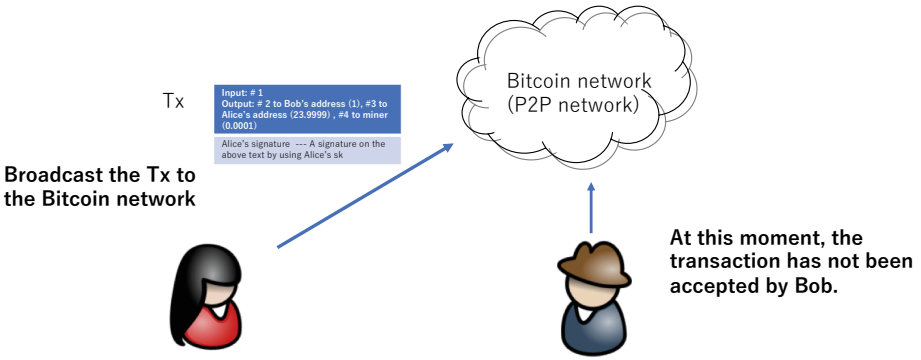
Tx

Input: # 1
Output: # 2 to Bob's address B (1), #3 to Alice's address A (23.9999) , #4 to miner (0.0001)

Alice's signature --- the signature on the above text by using Alice's sk

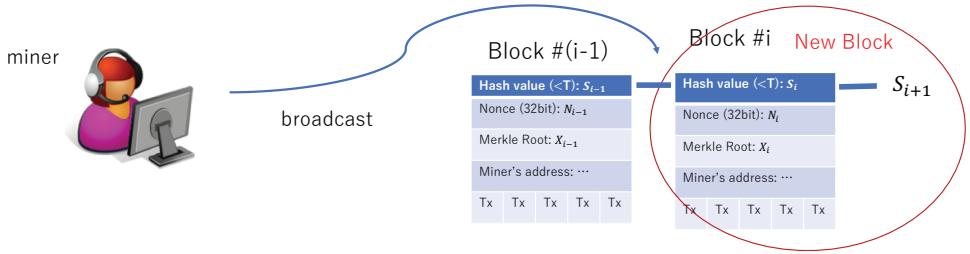
Transaction (Tx) =The text + signature (made by A's secret key)

Broadcast transaction

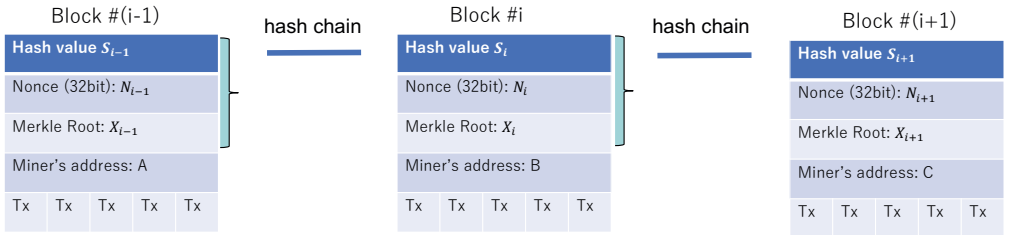


What the miners do ?

1. Choose a miner's preferable Tx's in the Bitcoin network.
2. Bundle the chosen Tx's (after verifying the validity of all).
3. Find nonce N_i, called Proof of Work.
4. Make new Block #i as it connects to Block #(i-1), and broadcast it in the Bitcoin network.



Blockchain -- chain of blocks



$S_i = H(S_{i-1}|X_{i-1}|N_{i-1}) <$T

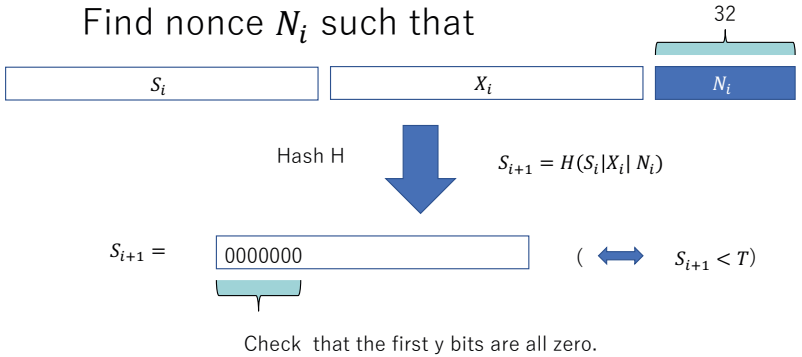
$S_{i+1} = H(S_i|X_i|N_i) < T$

Merkle root = hash value of miner's address and Tx's in the block

Proof of Work (POW): Work of finding nonce N such that hash value S <T.

Proof of Work (POW)

Find nonce N_i such that

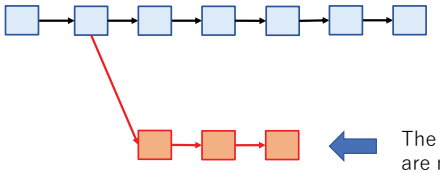


Check that the first y bits are all zero.

It takes 10 min to find a nonce on average (Bitcoin).

Longest chain rule

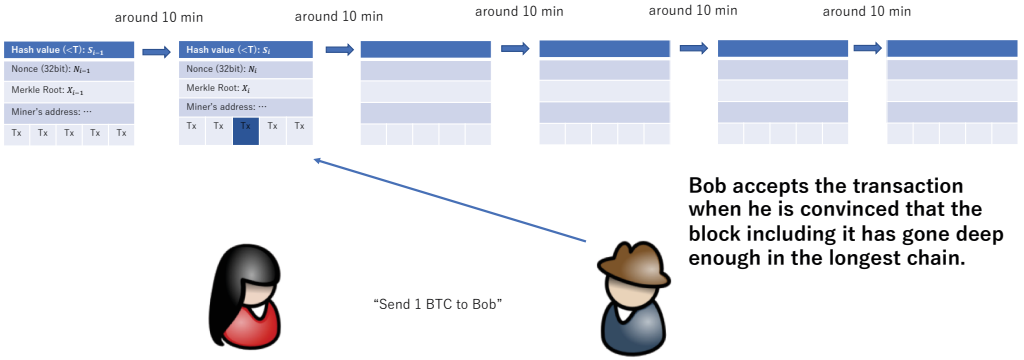
The longest chain = the legitimate chain



The transactions in these blocks are not accepted.

The “longest chain rule”:
If you see multiple competing valid chains, believe the one with more blocks.

When Bob accepts transaction ?

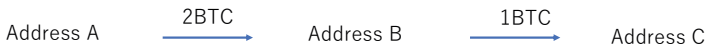


Bob accepts the transaction when he is convinced that the block including it has gone deep enough in the longest chain.

Bitcoin recommends that a merchant should accept when it goes 6 blocks deep from the end of the chain.

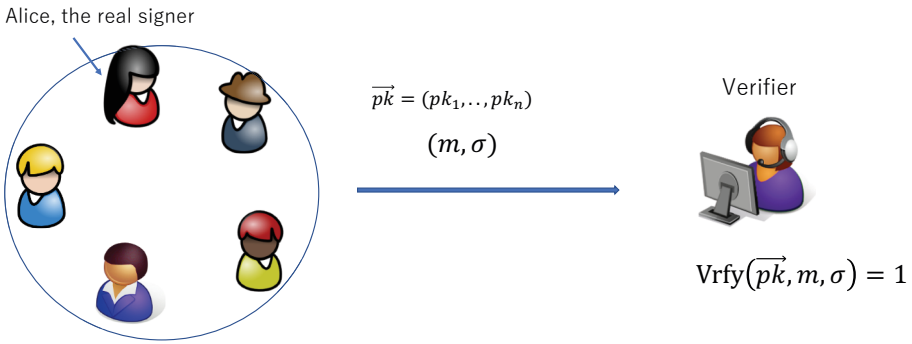
Notes on Bitcoin

- Address: The hash value of the owner’s public key.
  - A money (BTC) moves from address to address in the P2P network.
- Anonymity: (In principal) The link between a public-key (an address) and the owner is unknown (unless he makes it public).
  - A (public) bitcoin address of Mr. 堀江貴文 (Hori-emon)
    - 1G2jt5WeGhqWtDKEkcKY2GrZKjfYsuiVxX
- Traceability: A money flow is publicly traceable.
  - Otherwise, the miners cannot verify overspending.



Ring signature and Its variants

Ring Signature [How to leak a secret (RST2001)]



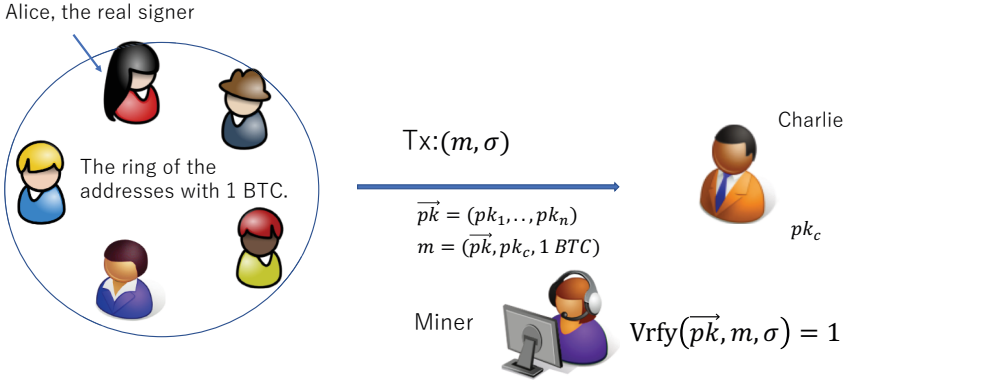
1. Alice, the real signer, can arbitrary choose a "ring" including herself.
2. Alice can convince the verifier that the signature σ is made by one of the ring members, without revealing who among them.

Applications: Whistle-blowing, Deniable signature.

Linkable / Traceable Ring Signatures

- Linkable Ring Signature [J. K. Liu, V. K. Wei, and D. S. Wong ACISP2004 (LWW04)]
  - Linkability: Two signatures generated by the same signer on the same ring are linked.
  - Applications: one-time E-voting, On-line electronic cash system
  - Followed by [TWCA04,LW05, TW05..]
- Traceable Ring Signature [F-Suzuki PKC2007 (FS07)]
  - Introduce a tag, composed of a ring and an issue, to control anonymity more delicate.
  - (Tag-)Linkability: Two signatures by the same signer on the same tag are linked.
  - Public Traceability: If two signatures of the same tag are made on different messages, the signer is revealed.
  - Applications: E-voting, Off-line electronic cash system
  - Followed by [F CT-RSA 2011] .

Linkable / Traceable ring signatures can provide untraceability to a blockchain-based cryptocurrency (e.g., Monero)



Miner is convinced that 1 BTC has moved from one of the addresses to Charlies' address.

If double spending, the two signatures are linked, so the miner can reject.

About Monero

- An untraceable blockchain-based cryptocurrency,
- Initially, used a simplified version of traceable ring signature [FS07], to achieve untraceability of money flow.
- Now, adopts so-called multi-layered linkable spontaneous anonymous group signature, by applying Ring Confidential Transaction [Noether 2015] to linkable ring signature [LWW04].
- Monero now hides not only money flow, but the amount of a transaction, as does Zcash.
- Concern about money-laundering. This problem is not settled.
  - Monero is substantially banned in Japan.

Monero's (initial) Linkable Ring Signature

A simplified version of TRS [FS07] (called **One-Time Linkable Ring Signature**)

$y_1 = g^{x_1}$

$y_a = g^{x_a}$

The real signer

$y_j = g^{x_j}$

$y_n = g^{x_n}$

Chaum's undeniable signature

$\sigma = h^{x_a}$ where $L = (y_1, .., y_n)$ and $h = H(L)$

+ **(1,n)- HVZK proof [CDN94]** to prove that, given $(g, h, y_1, .., y_n, \sigma)$

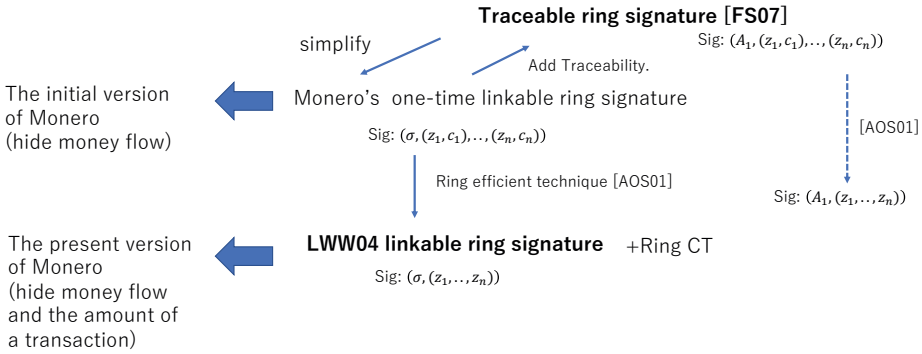
$\exists\, i \in [n]: \log_g (y_i) = \log_h(\sigma)$

Signature on m: $(\sigma, (z_1, c_1), .., (z_n, c_n))$

where $\sigma \in G,\ z_i, c_i \in Z_q$

[CDN94] Cramer, Damgaard, and Shoenmaker, Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols, Crypto 1994.

Monero: Relation to Linkable / Traceable Sig



[AOS01]: Abe, Ohkubo, and Suzuki, 1-out-of n Signature from a Variety of Keys, Asiacrypt 2001.

Traceable Ring Signature

The technique of [FS07] and some extension

Traceable Ring Signature [FS07]

$y_1 = g^{x_1}$

$y_a = g^{x_a}$

The real signer

$y_j = g^{x_j}$

$y_n = g^{x_n}$

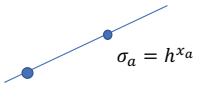
(1,n)- HVZK proof [CDN94]

given $(g, h, (y_1, .., y_n), (\sigma_1, .., \sigma_n))$

$\exists\, i \in [n]: \log_g (y_i) = \log_h(\sigma_i)$

+

(1,n)-Secret Sharing



$A_0 = H(L, m)$

where $L = ((y_1, .., y_n), \text{issue})$

$\forall i:\ \sigma_i = A_0 A_1^i$

$\log \sigma_i = \log A_0 + (\log A_1) i$

Signature: $(A_1\ (z_1, c_1), .., (z_n, c_n))$

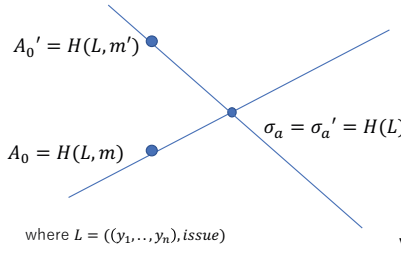
where $A_1 \in G,\ z_i, c_i \in Z_q$

Traceable Ring Signature (Signing)

1. Alice picks up the ring including herself $\vec{y} = (y_1, .., y_a, .. y_n)$.
2. Sets up tag $L = (\vec{y}, issue)$ where, for instance, ***issue*** = "2018 IACR election".
3. Computes $\sigma_a = h^{x_a}$ and $A_0 = H(L, m)$, where $h = H(L)$.
4. Sets $A_1 = \left(\frac{\sigma_a}{A_0}\right)^{\frac{1}{a}}$, i.e., $\sigma_a = A_0 A_1^a$, and computes $\sigma_i = A_0 A_1^i$ for all $i \neq a$.
5. Produces the FS based signature of (1,n)-HVZK proof [CDN94] that, given $(g, h, \vec{y}, \vec{\sigma})$, $\exists i$ such that $\log_g y_i = \log_h \sigma_i$.
6. Outputs $\left(A_1, (z_1, c_1), .., (z_n, c_n)\right)$.

If two signatures of different messages on the same label L

Signature of m: $(A_1, (z_1, c_1), .., (z_n, c_n))$, Signature of m': $(A_1', (z_1', c_1'), .., (z_n', c_n'))$



$\forall i$: $\sigma_i = A_0 A_1^i$

$\log \sigma_i = \log A_0 + (\log A_1) i$

$\forall i$: $\sigma_i' = A_0' A_1'^i$

Then, the signer is revealed.

Note: Traceable Ring Signature [FS07]

- v.s. Monero's one-time linkable ring signature.
  - The signature size is ***the same.***
- v.s. LWW linkable ring signature
  - When applying the ring efficient technique of [AOS01] to TRS[FS07], the signature size is ***the same.***
  - Note: The AOS01 technique can be applicable to *all* discrete-log (over prime order group) type (1,n)-HVZK CDS proof.
- [Strong security] Traceable ring signature requires ***exculpability,*** where even the ring member cannot produce a forged signature such that a honest signer is accused of signing twice on the same tag.

Efficiency Improvement

- Can reduce the signature size, by applying the ring efficient technique of [AOS01] to TRS [FS07].

Sig: $(A_1, (z_1, c_1), .., (z_n, c_n))$ —AOS01→ Sig: $(A_1, (z_1, .., z_n))$

|G| +2n |q| bits — |G| +n |q| bits

- [F11] With the technique of [CGS07], $O(\sqrt{n})$ size traceable ring signature (in the common reference string model).

[CGS07] Chandran, Groth and Sahai, Ring Signatures of Sub-linear Size without Random Oracles, ICALP07.

[F11] Fujisaki, Sub-Linear Size Traceable Ring Signatures without Random Oracles, CT-RSA11.

Threshold Version

- A recent trend on blockchain-based cryptocurrency.
  - Threshold ECDSA signature.
  - A countermeasure against the stolen secret-key problem. To sign, the secret keys of plural addresses are needed.
- Threshold traceable ring signature
  - Combination of (t,n)-proof [CDS94] and (t,n)-secret sharing yields (t,n)-traceable ring signature (See [FS07])
  - Compared to the ordinary traceable ring signature, (t,n)-TRS requires additional (t-1) group elements for signing.

Standardization Progress about (linkable/Traceable) Ring Signature

- ISO/IEC 20008-3: Mechanisms using multiple public keys
  - Status: Study Period
  - Linkable ring signature (based on [LWW04])
  - Traceable ring signature (based on [FS07])

Recent progress on ring signatures

Thanks to Keita Emura

- Short ring signature
  - [BCGGP15]: Short Accountable Ring Signatures Based on DDH. ESORICS 2015.
  - [LPQ18] Logarithmic-Size Ring Signatures with Tight Security from the DDH Assumption, ESORICS 2018
  - [MS17] Efficient Ring Signatures in the Standard Model. ASIACRYPT2017 (knowledge exponent assumption)
- Unique ring signature
  - [FZ13] Unique Ring Signatures: A Practical Construction, Financial Cryptography 2013 (a generalization of linkable /traceable ring signatures)

Recent progress on ring sig (2)

- Post-Quantum ring signature
  - David Derler, Sebastian Ramacher, and Daniel Slamanig: Post-Quantum Zero- Knowledge Proofs for Accumulators with Applications to Ring Signatures from Symmetric-Key Primitives. PQCrypto 2018
  - Muhammed F. Esgin, Ron Steinfeld, Amin Sakzad, Joseph K. Liu and Dongxi Liu: Short Lattice-based One-out-of-Many Proofs and Applications to Ring Signatures. Cryptology ePrint Archive: Report 2018/773
  - Wilson Abel Alberto Torres, Ron Steinfeld, Amin Sakzad, Joseph K. Liu, Veronika Kuchta, Nandita Bhattacharjee, Man Ho Au, and Jacob Cheng: Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT v1.0). ACISP 2018: 558-576

Recent progress on ring sig (3)

- Accountable ring signature (implying group signature)
  - Xu, S., Yung, M.: Accountable ring signatures: A smart card approach. CARDIS 2004
  - Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth, and Christophe Petit: Short Accountable Ring Signatures Based on DDH. In ESORICS (1) 2015, pp. 243-265.
  - Russell W. F. Lai, Tao Zhang, Sherman S. M. Chow, and Dominique Schröder: Efficient Sanitizable Signatures without Random Oracles. In ESORICS 2016. pp. 363–380.
  - Sudhakar Kumawat and Souradyuti Paul: A New Constant-size Accountable Ring Signature Scheme Without Random Oracles. Inscrypt 2017

Conclusions

- Linkable / Traceable ring signature can provide untraceability to a blockchain-based cryptocurrency.
- Monero, untraceable cryptocurrency, utilizes linkable / traceable ring signatures. It has now very strong anonymity and untraceability. Currently, too strong, I think.
- As for signature size, that of traceable ring signature is *the same* as that of linkable ring signature, in spite of additional property, *public-traceability.*