Short Paper:
Secure Offline Payments in Bitcoin

Taisei Takahashi Akira Otsuka

INSTITUTE of INFORMATION SECURITY

WTSC'19: 3rd Workshop on Trusted Smart Contracts

Outline

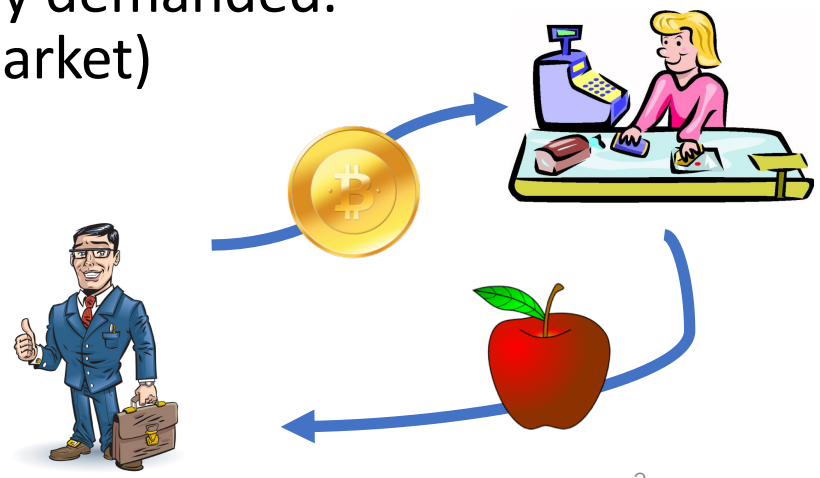
- Introduction
- Results
- Previous Research [DmitrienkoNY17]
- Our New Solution
- Conclusion

Introduction

- Bitcoin requires …
  - the payee to be online for sending a transaction to the Blockchain.
  - It takes a certain amount of time until the transaction is confirmed.

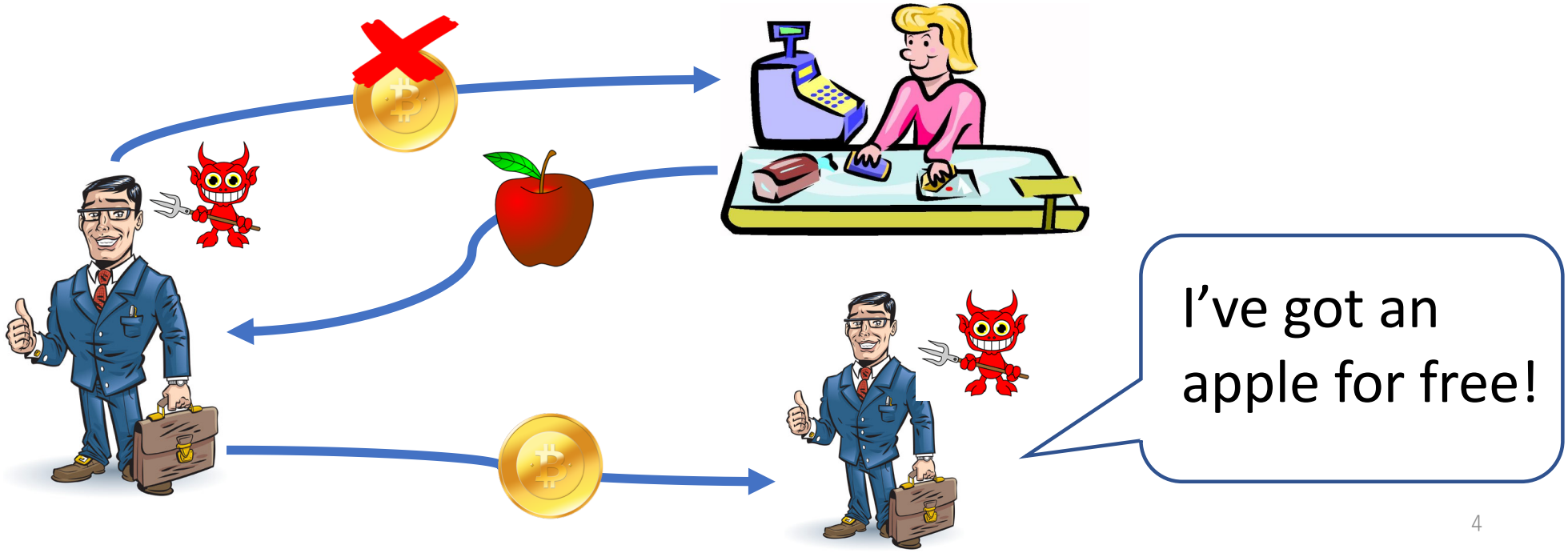
- In the real life scenario...
  - **Offline** and **Immediate** payment is greatly demanded.
    (e.g., Vending Machine, Digital Content Market)

- Fast payment : [Karame:2012]
  Vulnerable to **Double-spending attacks**.



Double-Spending Attacks on Fast Payments
[Karame:2012]

The malicious payer makes two payment transactions at the same time, one to the shop, and the other to the payer himself.

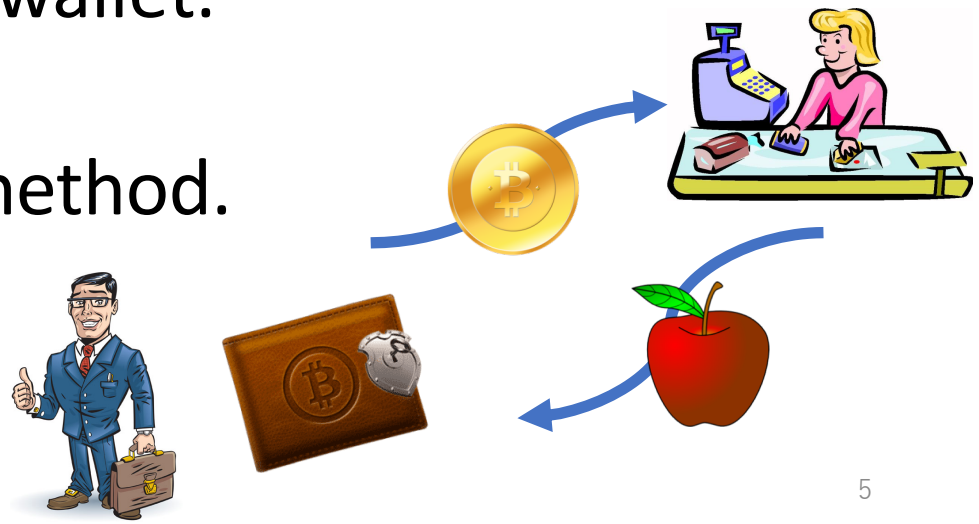


Results

- Completely decentralized **offline** and **immediate** payment scheme **without any modification to the existing Bitcoin network.**

- Only requires a tamper-proof wallet.

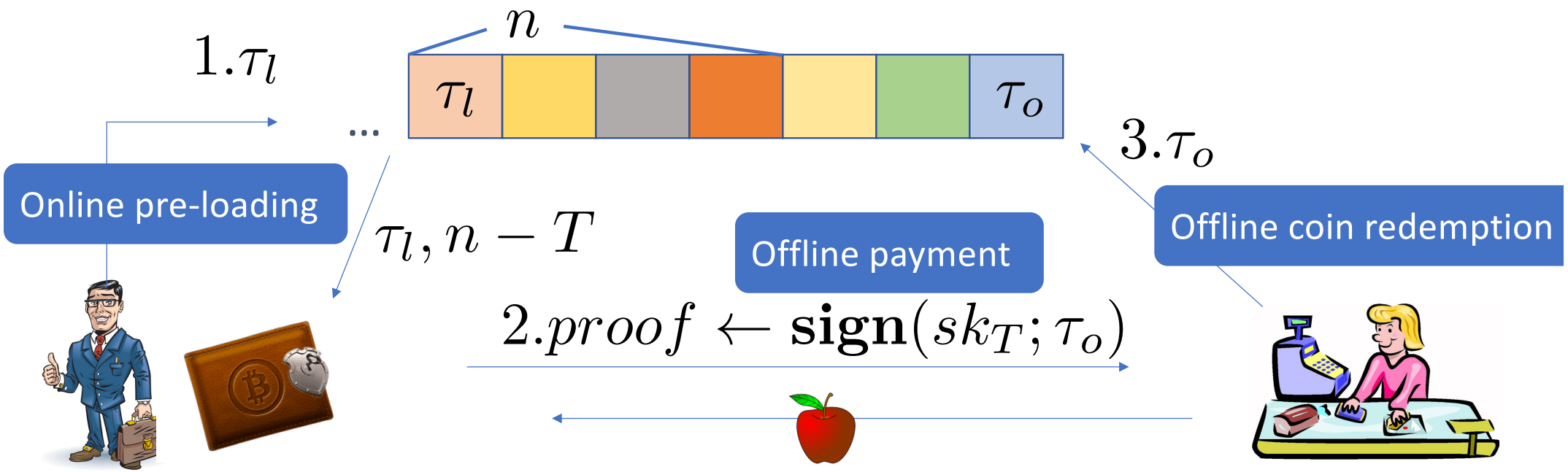
- Simplifies existing proposed method.



Previous Research [DmitrienkoNY17]

System Model (assume tamper-proof wallet)

1. Online pre-loading phase
2. Offline payment phase
3. Offline coin redemption and double-spender revocation

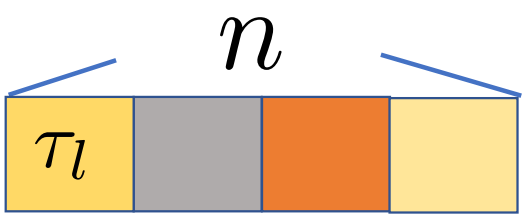


Previous Research [DmitrienkoNY17] - Security mechanisms

In order to ensure the wallet will not accept illegal pre-loading,

Dmitrienko17 proves it by showing **sufficiently large work is elaborated** on the fragment of blockchain **(Subchain)**

Online pre-loading

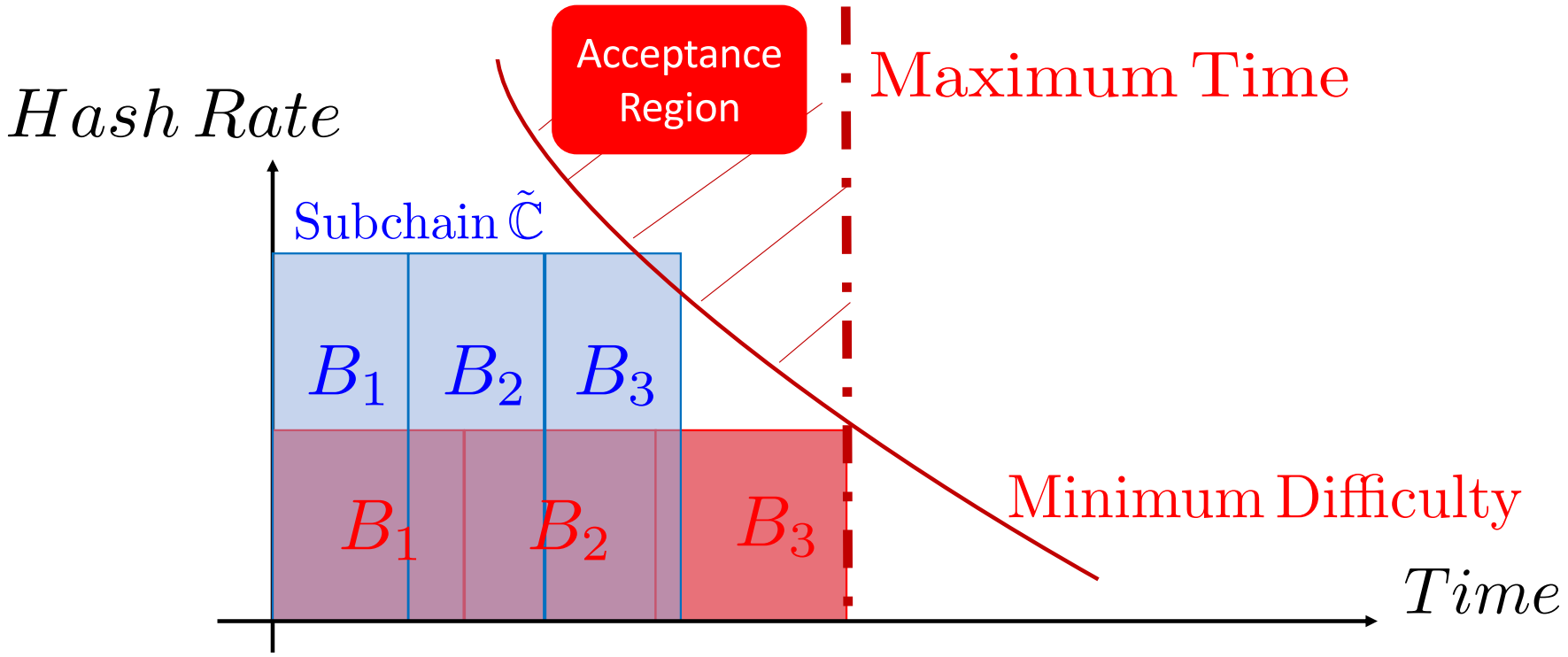


$\tau_l, n - T$

Previous Research [DmitrienkoNY17]

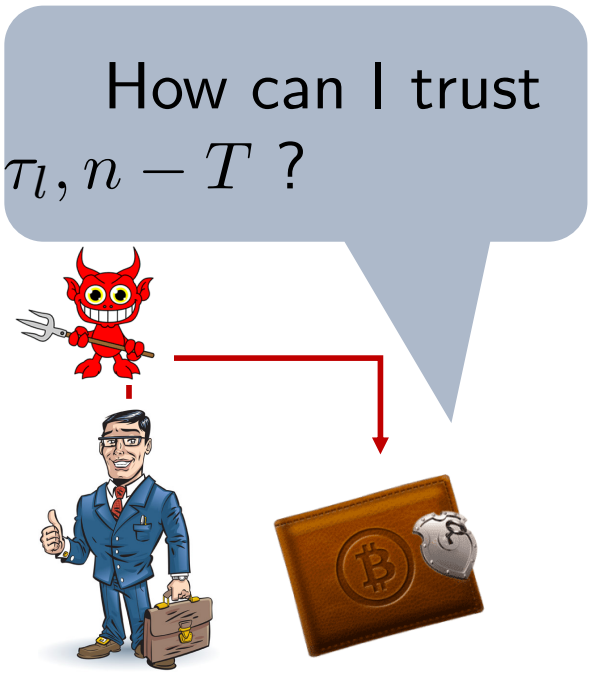
The wallet accepts the pre-loading transaction iff:

$$\text{Hash Rate} \times \text{Time} = \text{PoW} \geq \text{Minimum Difficulty}$$



Previous Research [DmitrienkoNY17]

It is necessary to prove the time taken to generate the fragments against the wallet objectively...



★**CHOICE**

A)Assume a trusted time-stamp server.

-> Additional assumption

B)Set the expiration time of the pre-loaded coins.

-> Sacrifices the usability

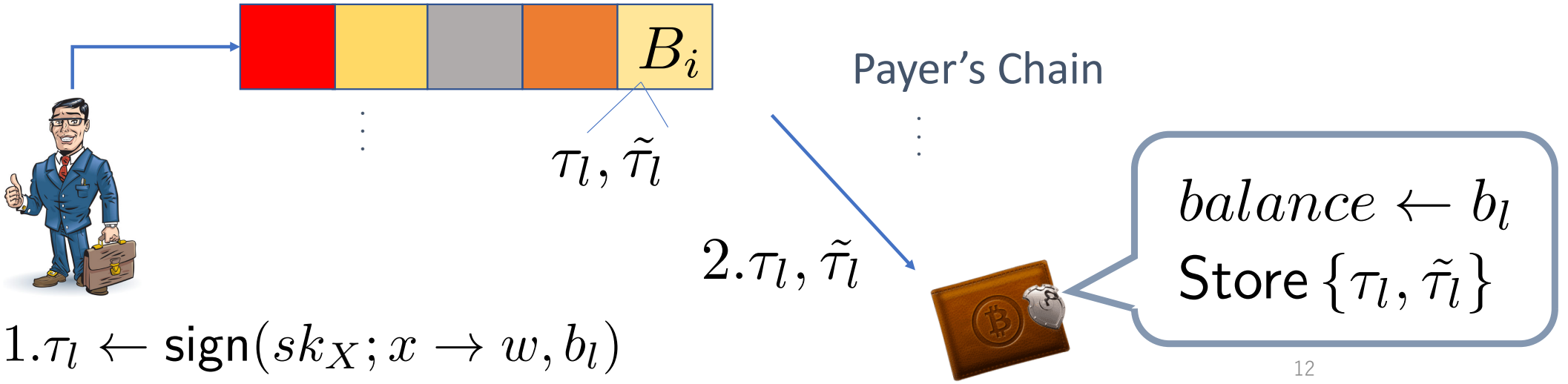
Our Construction

We do not require the external trusted time-stamp server and expiration time of the pre-loaded coins...

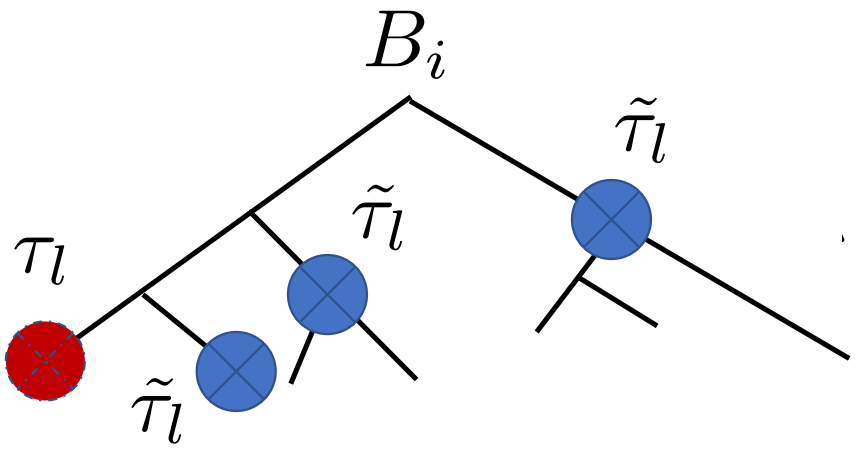
	[DmitrienkoNY17]	Our new solution
Pre-loading phase	Payer proves Wallet that **Money is Preloaded**	Payer only give a hint to Wallet (No Proof)
Offline payment phase	Payee accept the transaction **if Proof is verified**	Payee accept the transaction if **Proof is verified** AND **Money is Preloaded to Wallet**

Pre-loading Phase

1. Payer makes pre-load transaction.
2. After the pre-load transaction is into the block, the transaction is sent to the wallet.
3. The wallet accepts the transaction and increase *balance* and store the transaction.



Membership Proof on Merkle Tree



$$member(\tau_l, \tilde{\tau}_l, B_i) = 1$$

Membership Witness

$$(\tilde{\tau}_l : witness)$$

Payee Y_i does not have to record all past transactions.

Pre-loading Phase

1. Payer makes pre-load transaction.
2. After the pre-load transaction is into the block, the transaction is sent to the wallet.
3. The wallet accepts the transaction and increase *balance* and store the transaction.

$\tau_l, \tilde{\tau}_l$

Payer's Chain

$2.\tau_l, \tilde{\tau}_l$

$balance \leftarrow b_l$

Store $\{\tau_l, \tilde{\tau}_l\}$

$1.\tau_l \leftarrow \text{sign}(sk_X; x \rightarrow w, b_l)$

Offline Payment

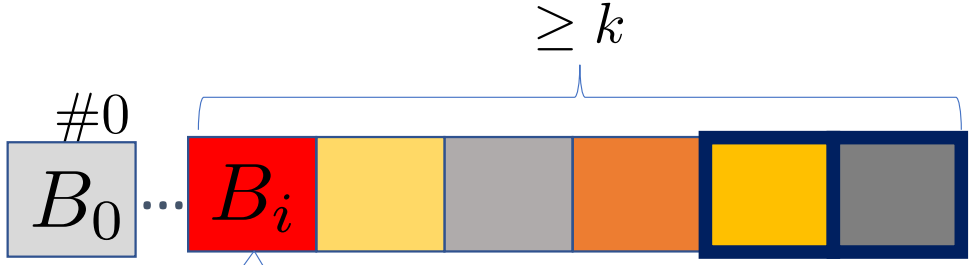
1. Payee charge b_o to Payer.

2. When τ_o is sent from the wallet, Payee checks...

   (a) τ_l is in the payee's chain.

   (b) τ_o is Valid w.r.t. Payee's chain.

Payee's Chain



if $(balance \geq b_o)$
$balance \leftarrow balance - b_o$
$\tau_o \leftarrow \mathsf{Sign}(sk_W; w \rightarrow y, b_o)$
$proof \leftarrow \mathsf{Sign}(sk_T; \tau_o, \tau_l, \tilde{\tau}_l)$
else $reject$

$1. PK_Y, b_o$

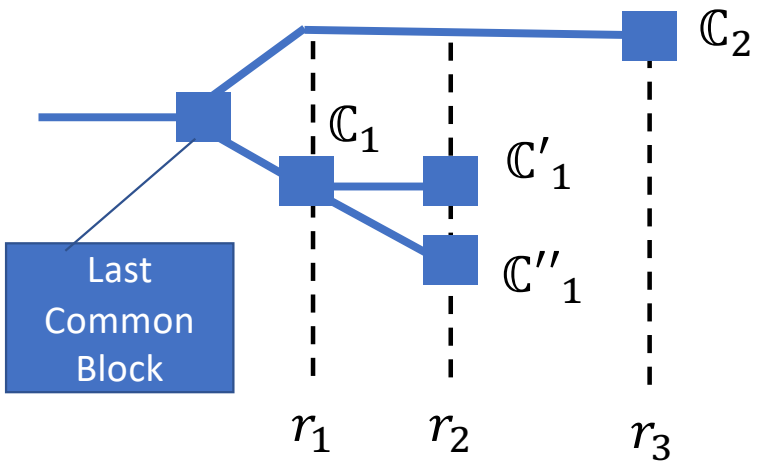
$2. \tau_o, proof, cert_T$

accept τ_o and $proof$ iff

$$\begin{cases} cert_T \text{ is trustworthy} \\ \mathsf{Verify}(PK_T; proof) = 1 \\ \tau_o \in (\mathcal{V}_{\mathbb{C}_Y} \cap \mathsf{Sign}(sk_W; w \rightarrow \cdot, b_o)) \\ \tau_l \in (\mathbb{C}_Y^{\lceil k} \cap \mathsf{Sign}(\cdot; \cdot \rightarrow w, b_l)) \end{cases}$$

$3. \mathsf{Sign}\ (sk_Y; status)$

Common-Prefix Property [GarayKL15]



- $\mathbb{C}^{\lceil k}$: Blockchain $\mathbb{C}$ with k blocks at the right end removed.
- $\mathbb{C}_1 \preceq \mathbb{C}_2$: $\mathbb{C}_2$ is a prefix of $\mathbb{C}_1$

Common-Prefix Lemma

(ϵ, η)-typical execution and consider two chains $len(\mathbb{C}_2) \geq len(\mathbb{C}_1)$

1. $\mathbb{C}_1$ is adopted by an honest party at round r.
2. $\mathbb{C}_2$ is either adopted by an honest party or diffused at round r.

$$\Rightarrow \mathbb{C}_1^{\lceil k} \preceq \mathbb{C}_2 \wedge \mathbb{C}_2^{\lceil k} \preceq \mathbb{C}_1, \text{ for } k \geq 2\eta\kappa f$$

Offline Payment

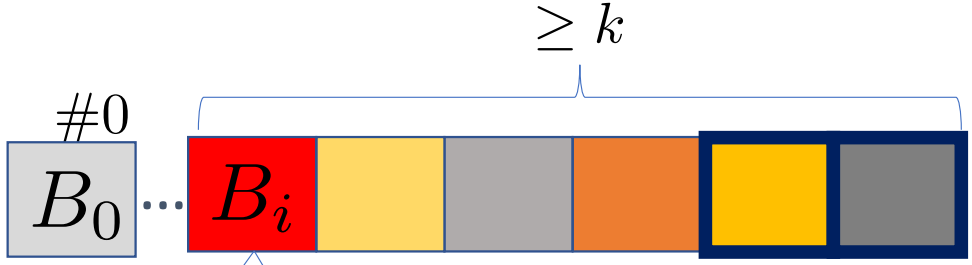
1. Payee charge b_o to Payer.

2. When τ_o is sent from the wallet, Payee checks...

   (a) τ_l is in the payee's chain.

   (b) τ_o is Valid w.r.t. Payee's chain.

Payee's Chain



if $(balance \geq b_o)$
$balance \leftarrow balance - b_o$
$\tau_o \leftarrow \mathsf{Sign}(sk_W; w \rightarrow y, b_o)$
$proof \leftarrow \mathsf{Sign}(sk_T; \tau_o, \tau_l, \tilde{\tau}_l)$
else $reject$

$1. PK_Y, b_o$

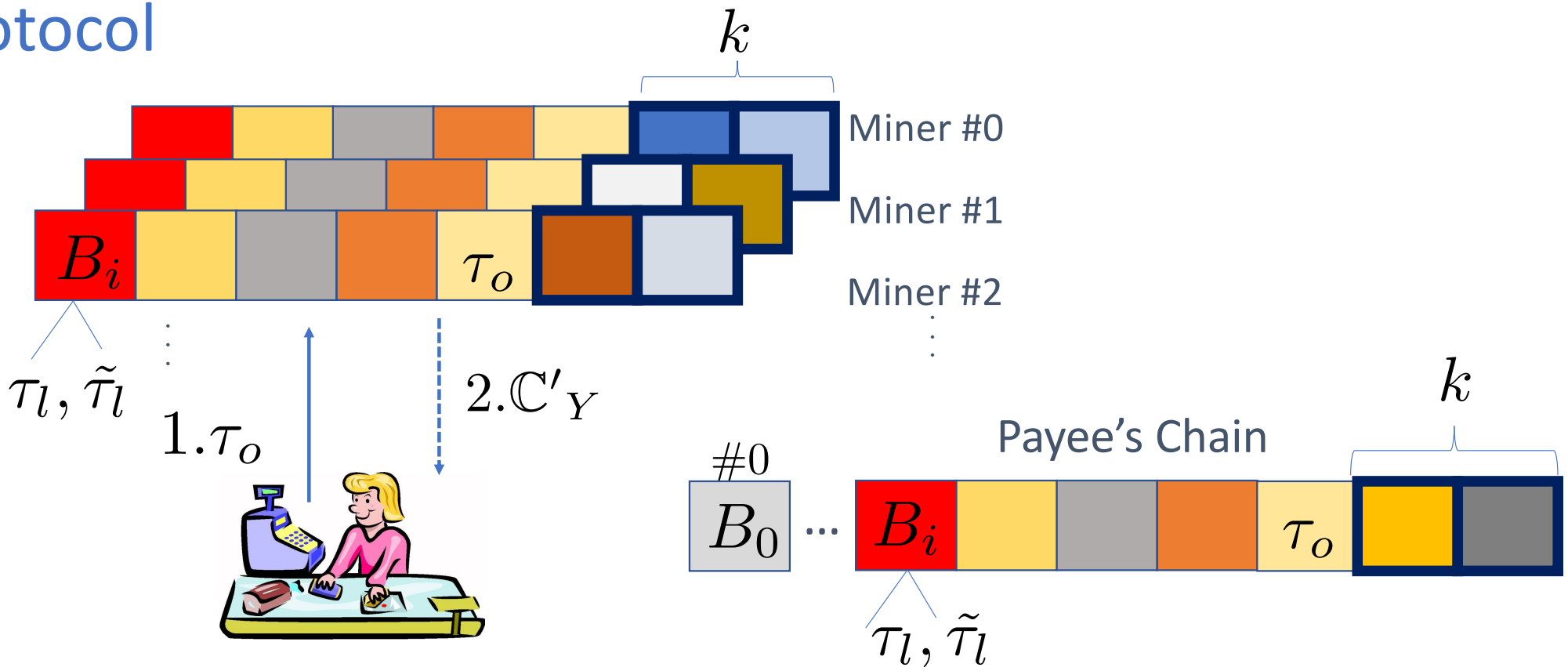
$2. \tau_o, proof, cert_T$

accept τ_o and $proof$ iff

$$\begin{cases} cert_T \text{ is trustworthy} \\ \mathsf{Verify}(PK_T; proof) = 1 \\ \tau_o \in (\mathcal{V}_{\mathbb{C}_Y} \cap \mathsf{Sign}(sk_W; w \rightarrow \cdot, b_o)) \\ \tau_l \in (\mathbb{C}_Y^{\lceil k} \cap \mathsf{Sign}(\cdot; \cdot \rightarrow w, b_l)) \end{cases}$$

$3. \mathsf{Sign}\ (sk_Y; status)$

Coin redemption and Double-spending wallet revocation protocol



Payee sends the offline transaction to the miners and wait until the transaction is confirmed.

Conclusion

- We proposed an efficient offline payment scheme for PoW blockchains such as Bitcoin.

- Advantages of our scheme are it requires...
  - No trusted time-stamp server.
  - No expiration time to the pre-loaded coins.
  - No modification to the existing Bitcoin network.

- **Open Problem** :
  - Offline payment schemes for PoS-type blockchain