Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

CrypTO CONFERENCE

Politecnico di Torino
1859

Telsy
A TIM ENTERPRISE BRAND

DISMA

Finanziato dall'Unione europea
NextGenerationEU

Italiadomani
PIANO NAZIONALE
DI RIPRESA E RESILIENZA

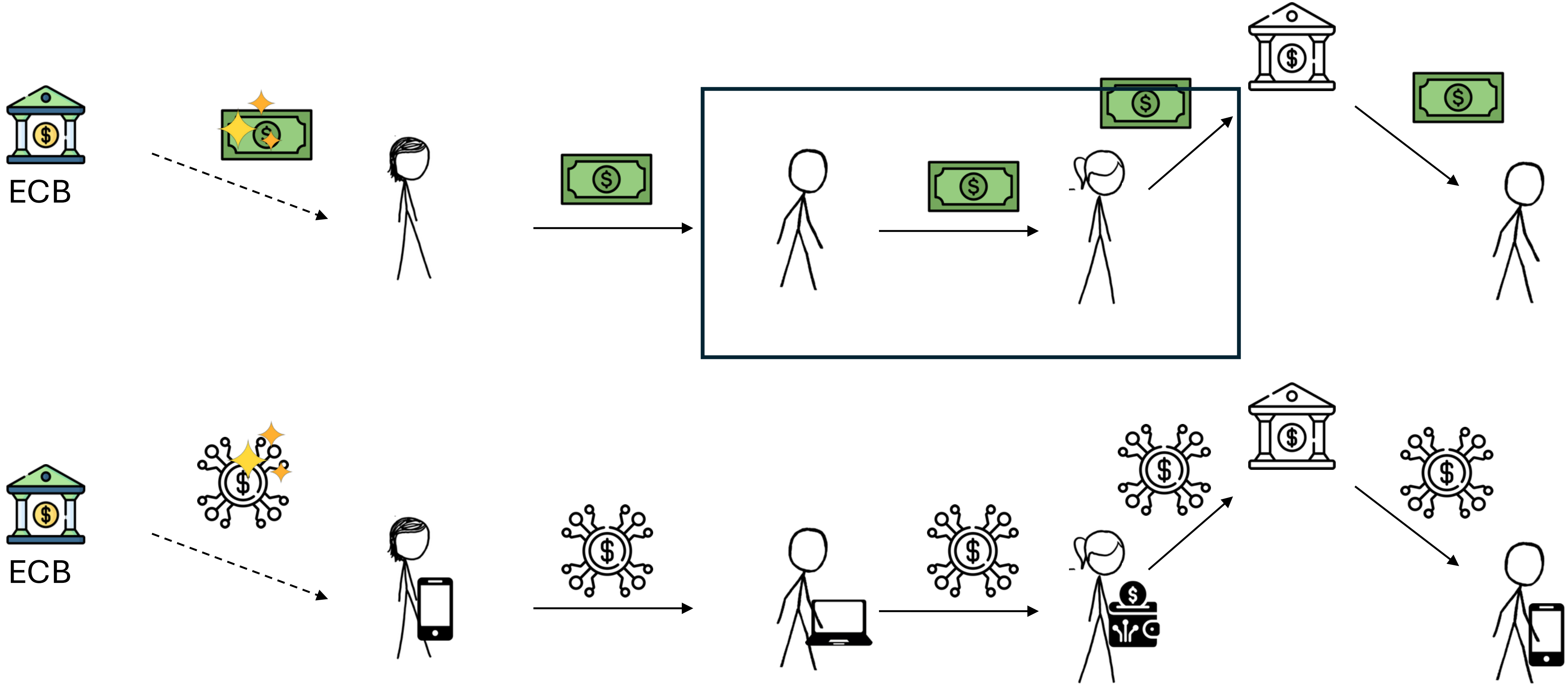
SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Private Electronic Payments with Self-Custody and Zero-Knowledge Verified Reissuance

Daniele Friolo[1], Geoffrey Goodell[2], Dann R. Toliver[3], and Hazem D. Nakib[2]

[1]Sapienza University of Rome, Rome, Italy
[2]University College London, London, UK
[3]TODAQ Finance

Fiat Money vs Digital Cash



Fungibility: a banknote is just a banknote, with no story behind!

Digital Cash Desiderata

- Consumer Privacy
- Compatibility with regulatory objectives
- No involvement of the issuer in the circulation of tokens
- Efficient procedure for reissuance of tokens
- Stateless issuer
- Modularity
- Auditability (with succinct audit log)
- **Transaction independence**

  «Consumers must not be expected to hold any secrets other than those related to the set of tokens that they currently hold»

Related Works

UTXO-based	***Account-based***
Androulaki et al. (AFT ‘20) ☑ Fast ❗ Auditable (expensive)	*PEReDI (Kiayias et al, CCS ‘22)* ☑ Universally Composable ☒ Complex design ❗ Traceable (trapdoor needed)
Wüst et al. (FC .19) ☑ Fast ☒ Property-based security	*Platypus (Wüst et al. CCS ‘22),* *KAIME (Dogan et al. ICISSP ‘24)* ☑ Simple design ☒ Property-based security
Tomescu et al. (ePrint) ☑ Universally Composable ☒ Complex design	

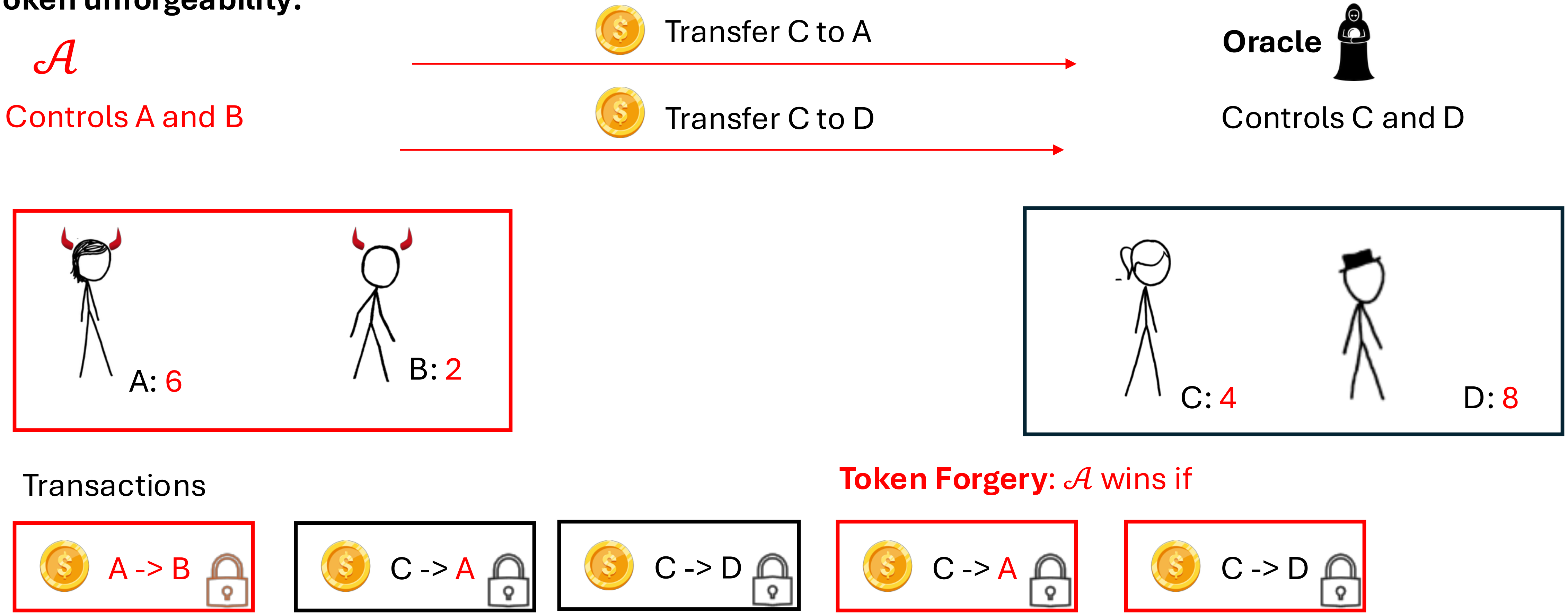
Related Works

UTXO-based	***Account-based***
Androulaki et al. (AFT '20) ☑ Fast ❗ Auditable (expensive)	*PEReDI (Kiayias et al, CCS '22)* ☑ Universally Composable ☒ Complex design eded)
Wüst et ☑ Fa ☒ Pr	☒ Property-based security
Tomescu et al. (ePrint) ☑ Universally Composable ☒ Complex design	

No transaction independence!

Desired properties – Token Integrity

Token unforgeability:



$\mathcal{A}$

Controls A and B

Transfer C to A

Transfer C to D

Oracle

Controls C and D

A: 6

B: 2

C: 4

D: 8

Transactions

A -> B

C -> A

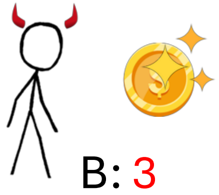
C -> D

Token Forgery: $\mathcal{A}$ wins if

C -> A

C -> D

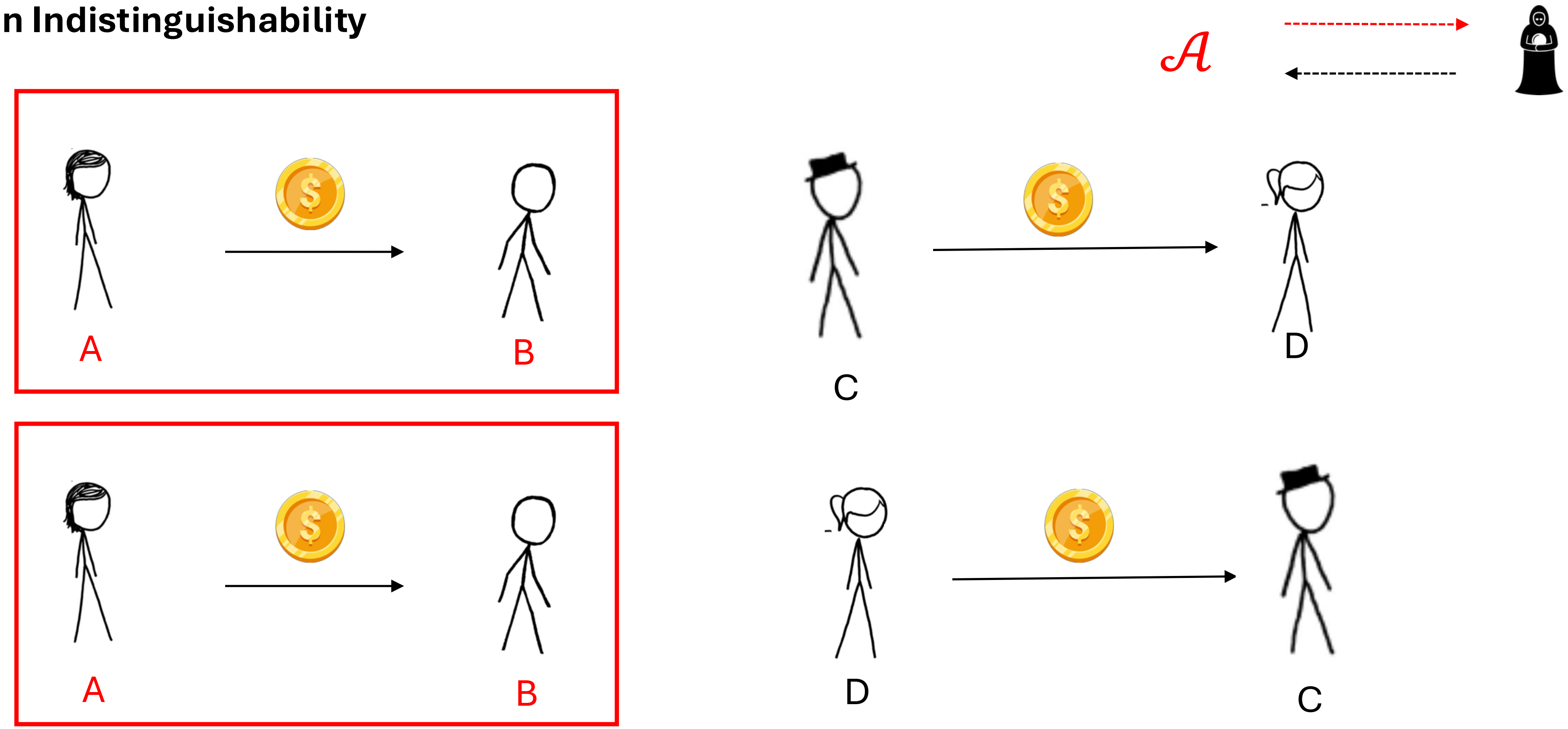
Balance invariance: the adversary wins if he mint new coins for A or B



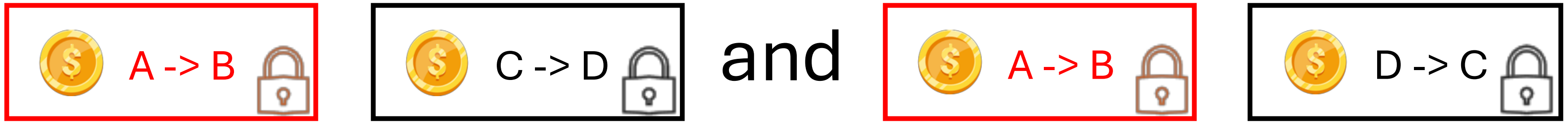
B: 3

Token Privacy

Token Indistinguishability

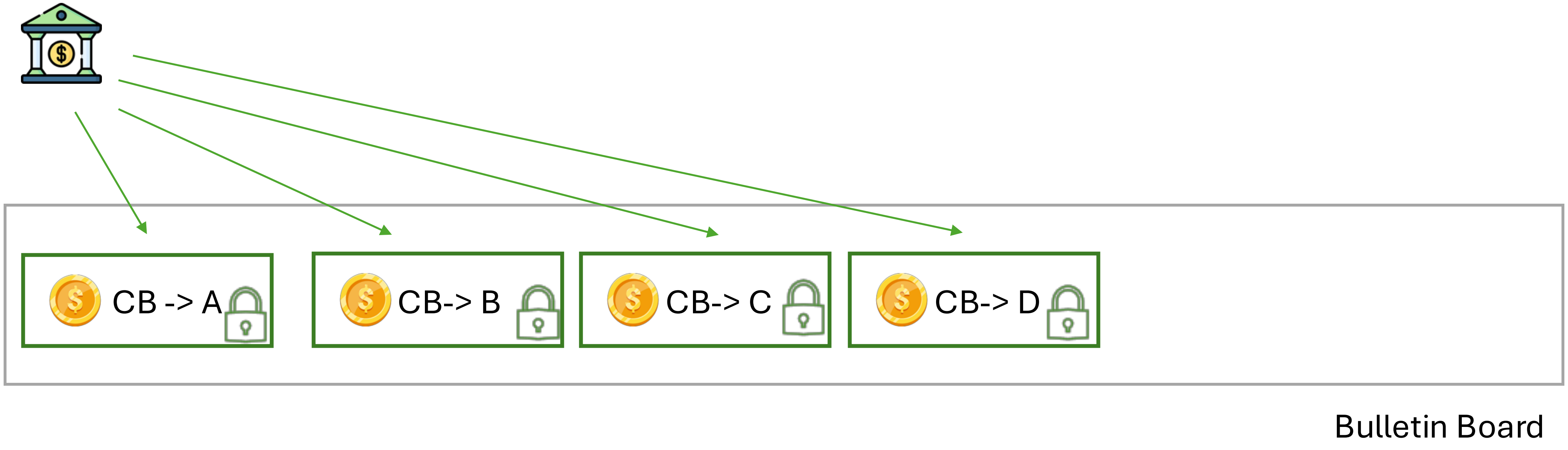


Token Forgery: $\mathcal{A}$ wins if he can distinguish between

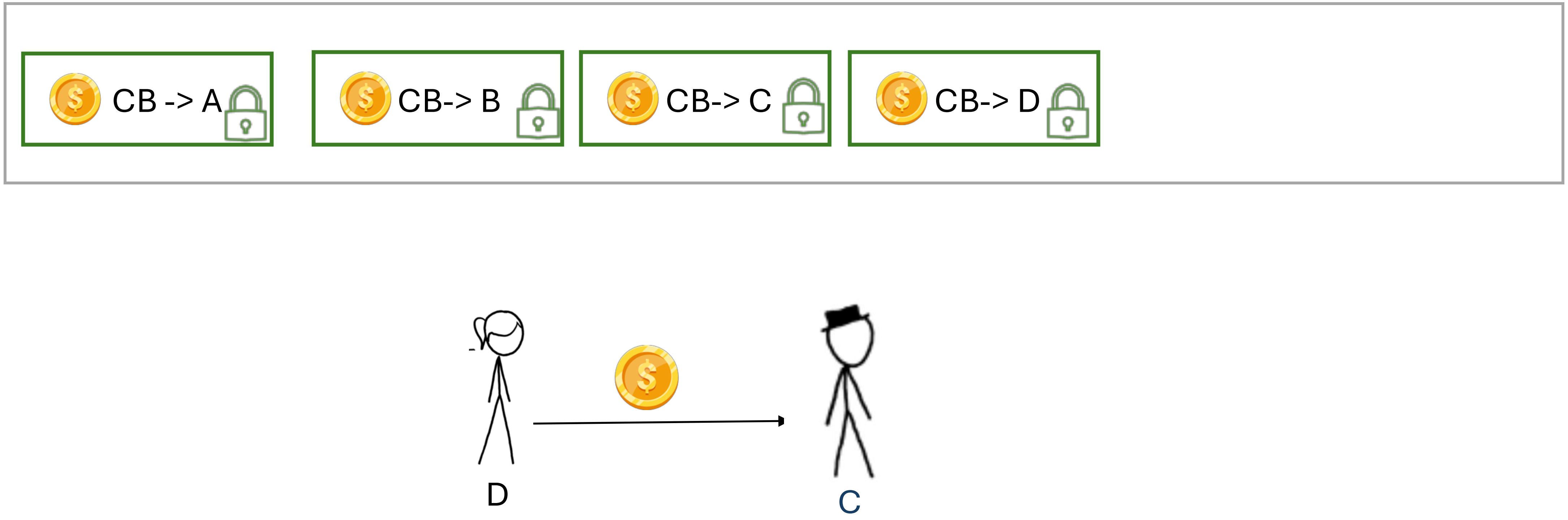


A -> B C -> D and A -> B D -> C

Protocol Idea



Protocol Idea



CB -> A

CB-> B

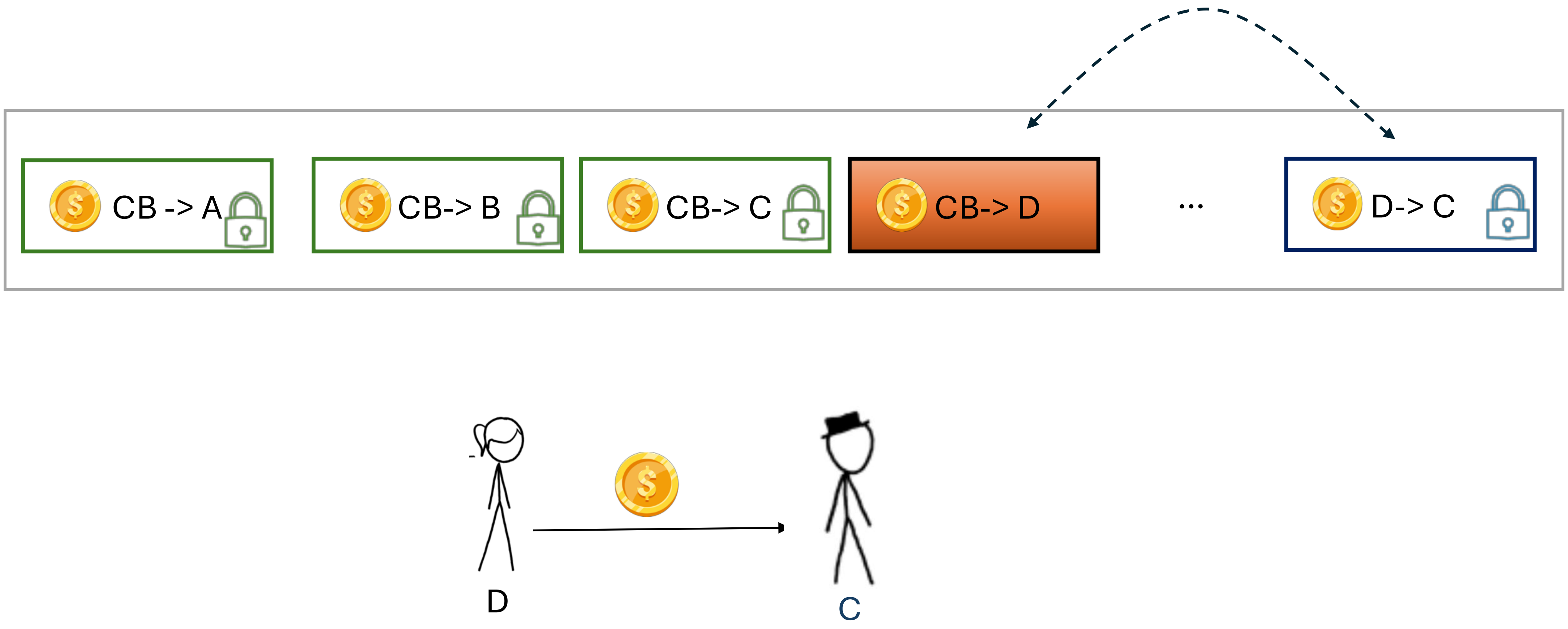
CB-> C

CB-> D

D

C

Protocol Idea



CB -> A

CB-> B

CB-> C

CB-> D

…

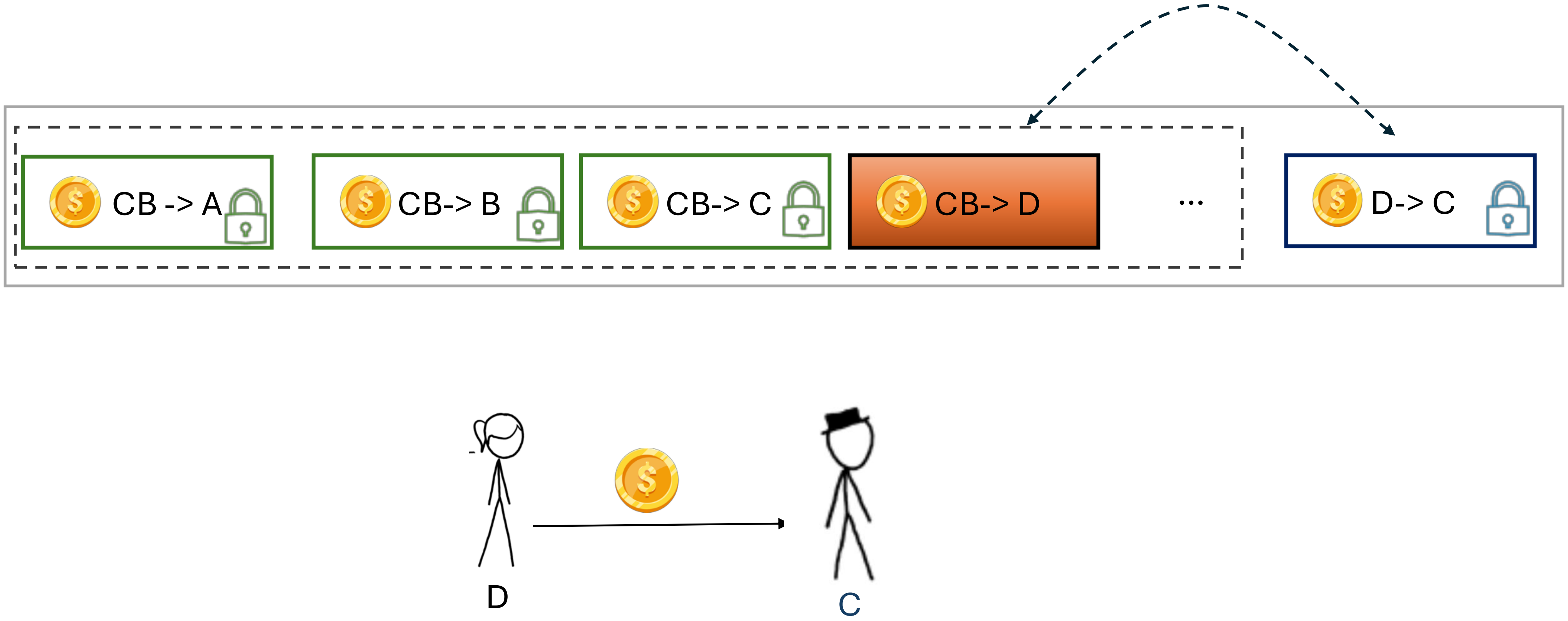
D-> C

D

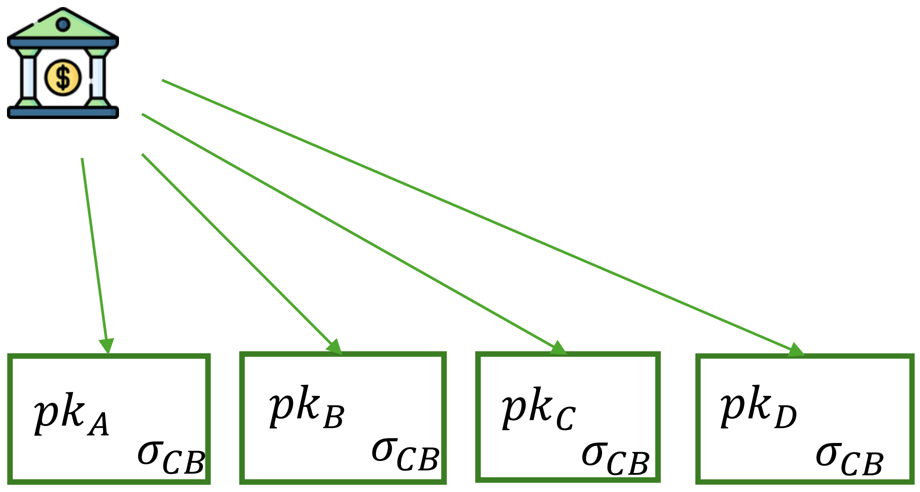
C

Protocol Idea

Proof: The sender burnt a token in this set



Our protocol



pk_A σ_{CB}

pk_B σ_{CB}

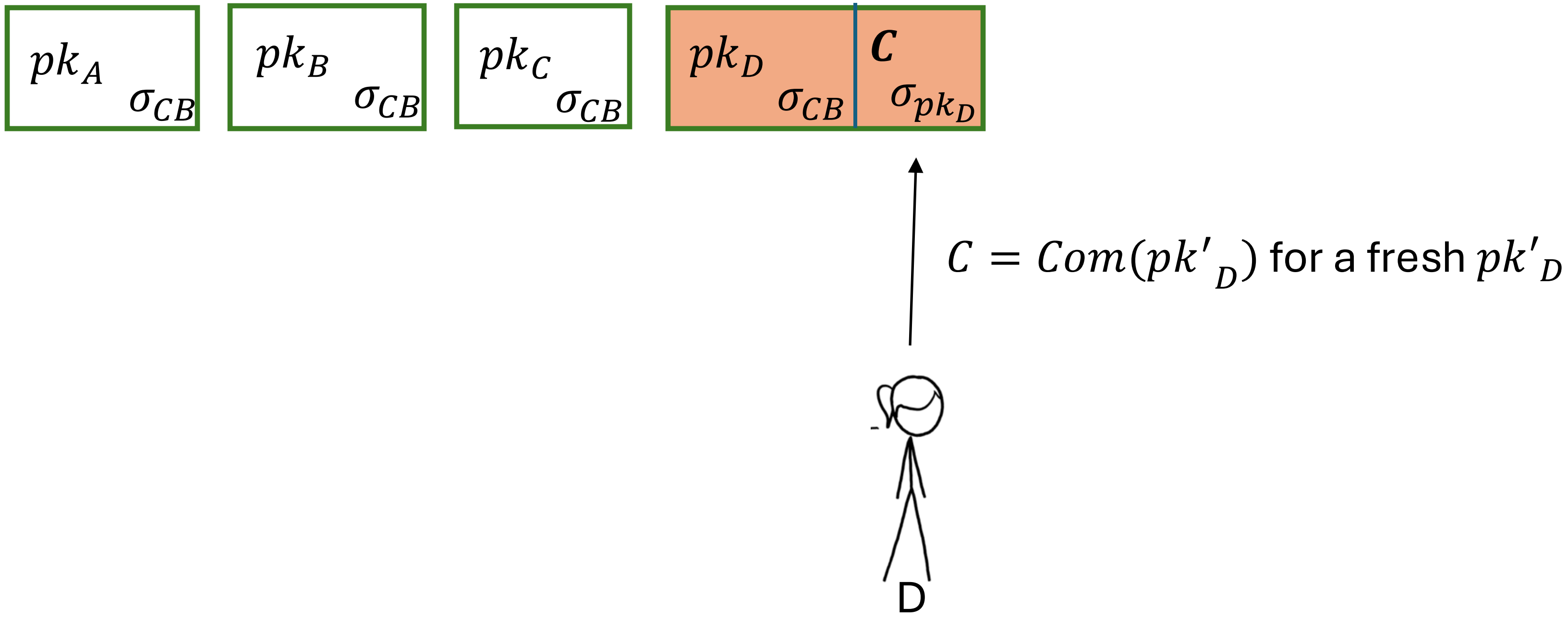
pk_C σ_{CB}

pk_D σ_{CB}

Further authenticated by the users through signatures

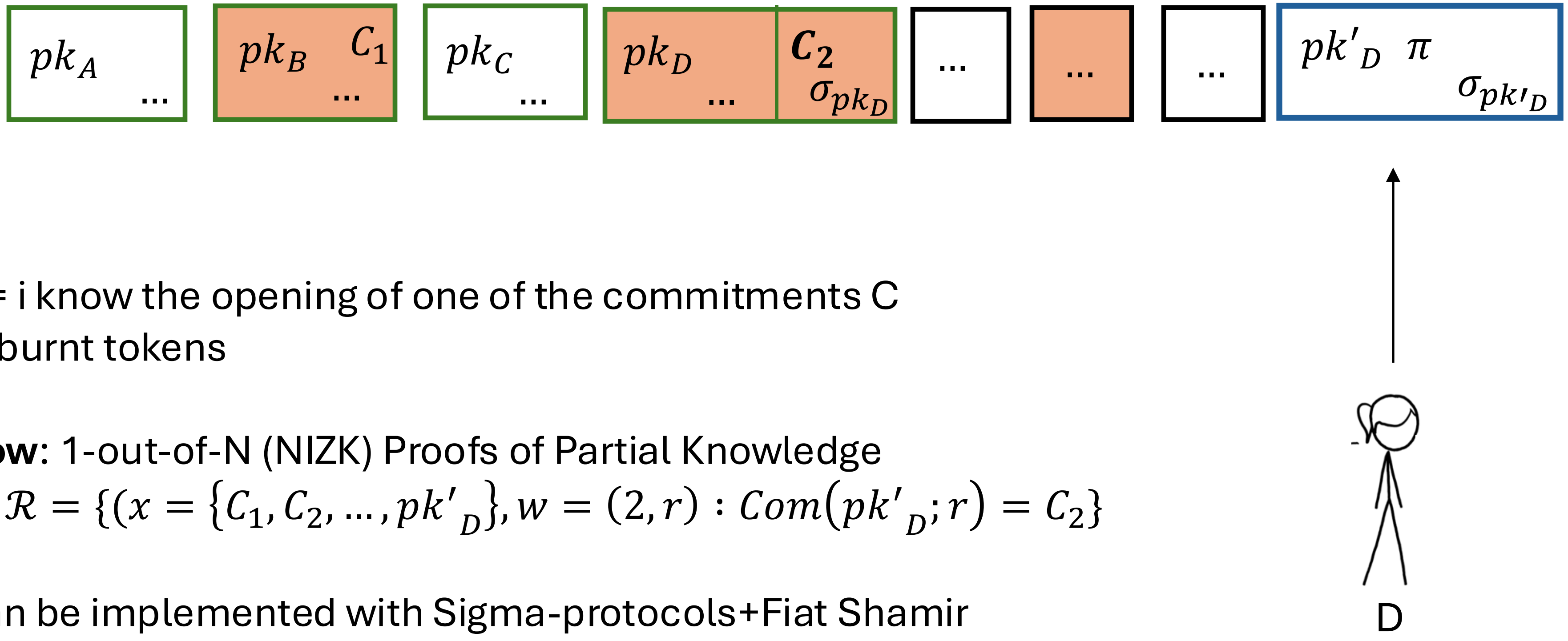
Our protocol

Step 1: Burn



Our protocol

Step 2: Mint with fresh pk'_D


pk_A …
pk_B C_1 …
pk_C …
pk_D …
$\boldsymbol{C_2}$ σ_{pk_D}
…
…
…
pk'_D π $\sigma_{pk'_D}$
D

π = i know the opening of one of the commitments C of burnt tokens

How: 1-out-of-N (NIZK) Proofs of Partial Knowledge

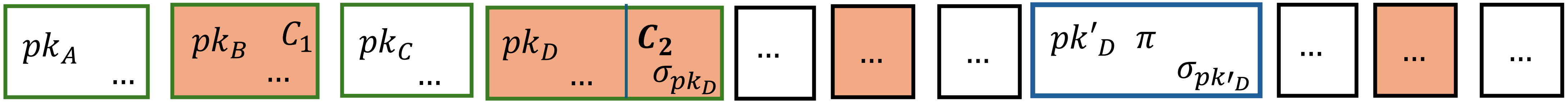
$$\mathcal{R} = \{(x = \{C_1, C_2, \dots, pk'_D\}, w = (2, r) : Com(pk'_D; r) = C_2\}$$

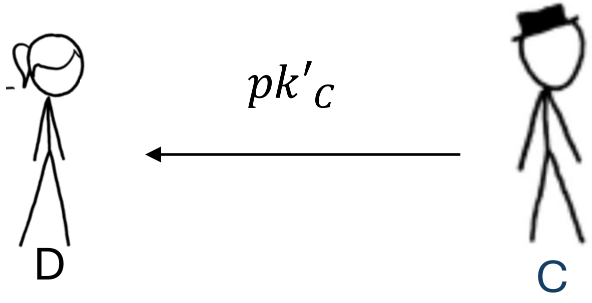
Can be implemented with Sigma-protocols+Fiat Shamir

Our protocol

$$\mathcal{R} = \{(x = \{C_1, C_2, \dots, pk'_D\}, w = (2, r) : Com(pk'_D; r) = C_2\}$$

Step 3.1: Payment to C, receive C's public key pk'_C



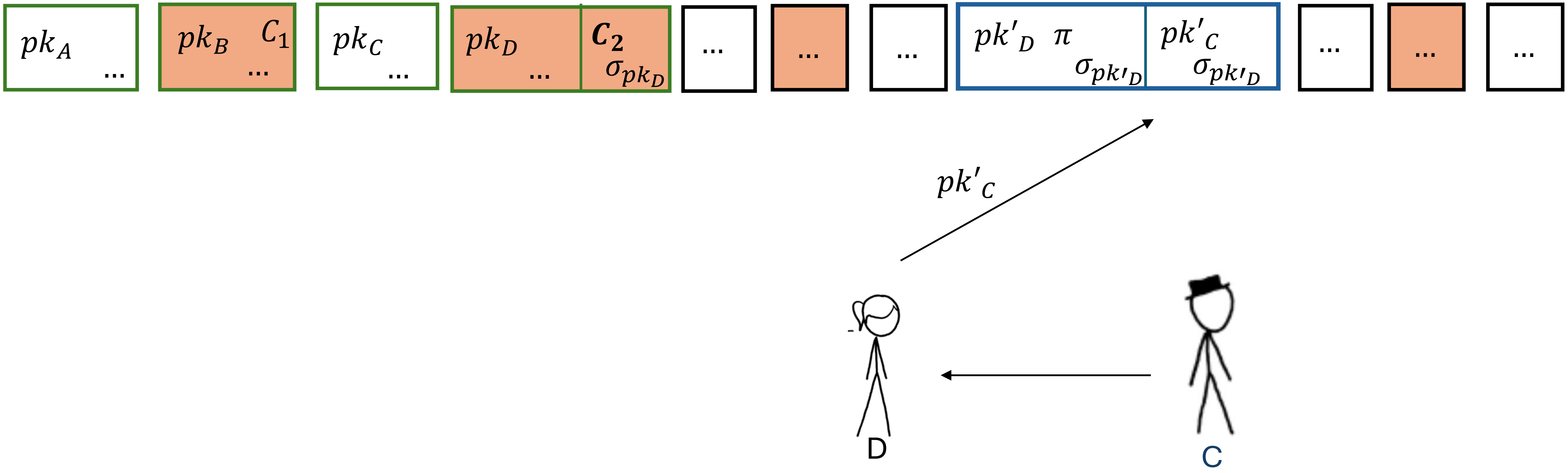


Sample a fresh pk'_C

Our protocol

$\mathcal{R} = \{(x = \{C_1, C_2, \ldots, pk'_D\}, w = (2, r) : Com(pk'_D; r) = C_2\}$

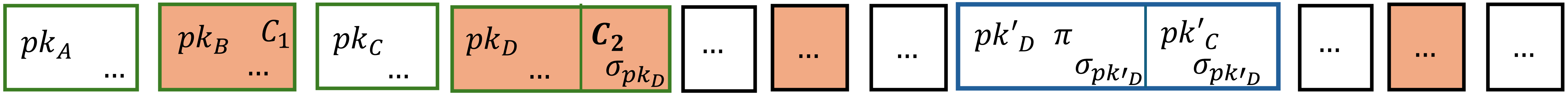
Step 3.2: Payment to C, D updates with new transaction with pk'_C, (authenticated with $\sigma_{pk'_D}$)



pk_A …
pk_B C_1 …
pk_C …
pk_D … $\boldsymbol{C_2}$ σ_{pk_D}
…
…
…
pk'_D π $\sigma_{pk'_D}$
pk'_C $\sigma_{pk'_D}$
…
…
…
pk'_C
D
C

Our protocol

$$\mathcal{R} = \{(x = \{C_1, C_2, \ldots, pk'_D\}, w = (2, r) : Com(pk'_D; r) = C_2\}$$



Accept the payment if

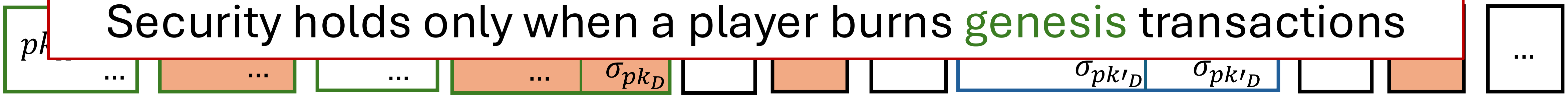
- All the signatures verify
- π verifies on $\{C_1, C_2, \ldots, pk'_D\}$
- pk'_D appears only once in the BB

Our protocol

$\mathcal{R} = \{(x = \{C_1, C_2, \dots, pk'_D\}, w = (2, r) : Com(pk'_D; r) = C_2\}$

Problem:

Security holds only when a player burns genesis transactions



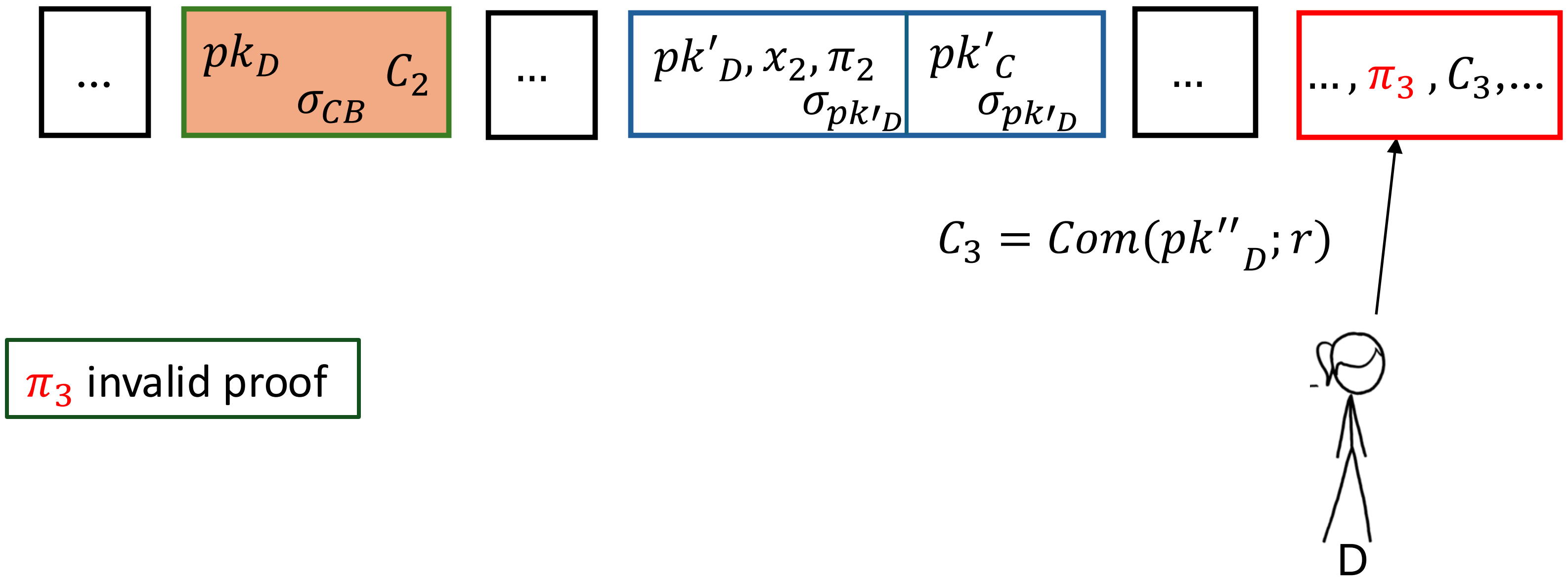
Accept the payment if

- All the signatures verify
- π verifies on $\{C_1, C_2, \dots, pk'_D\}$
- pk'_D appears only once in the BB

Our protocol

Problem:

- Security holds only when a player burns genesis transactions only

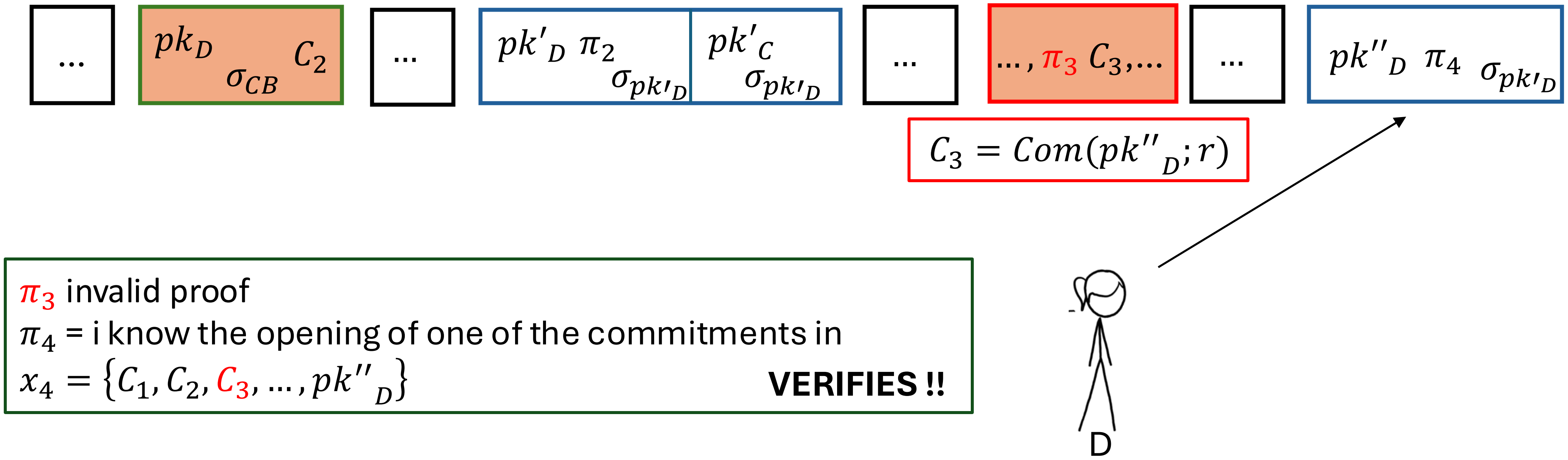

…
pk_D C_2 σ_{CB}
…
pk'_D, x_2, π_2 $\sigma_{pk'_D}$
pk'_C $\sigma_{pk'_D}$
…
$\ldots, \pi_3, C_3, \ldots$
$C_3 = Com(pk''_D; r)$
D

π_3 invalid proof

Our protocol

Problem:

- Security holds only when a player burns genesis transactions only


…
pk_D C_2 σ_{CB}
…
pk'_D π_2 $\sigma_{pk'_D}$
pk'_C $\sigma_{pk'_D}$
…
$\dots, \pi_3$ $C_3, \dots$
…
pk''_D π_4 $\sigma_{pk'_D}$
$C_3 = Com(pk''_D; r)$
D

π_3 invalid proof

π_4 = i know the opening of one of the commitments in

$x_4 = \{C_1, C_2, C_3, \dots, pk''_D\}$ **VERIFIES !!**

Our protocol: Workarounds

- The payee should also verify **all** the proofs
  - ☒ Computationally intensive and space-consuming for the user
- An antrusted aggregator aggregates all the proofs
  - ☑ Less work for the user
  - ☒ Requires computationally expensive zkSNARKs
- Use smart contracts to discard bad transactions
  - ☑ No work for the users
  - ☒ Complex blockchain systems (e.g., supporting EVMs)

Our protocol: Security

Token Integrity

- *Token forgery*:
  - Transactions and updated authenticated through signatures
  - NIZK-PPKs cannot be forged due to Knowledge Soundness
  - Binding of the commitment ensured that the adversary could not create proofs on wrong openings
- *Balance invariance*:
  - No double spending: Public keys cannot be reused

Token privacy:

- *Token indistinguishability*: Hiding of the commitment scheme and Zero-Knowledge of the NIZK-PPK ensure that the adversary cannot link new transactions to burnt transactions

Conclusions and future works

- Novel protocol allowing private electronic payments with self-custody and zero-knowledge verified assurance
- Satisfies digital cash desiderata, including transaction independence
- Future work:
  - Optimistic protocol where zero-knowledge proofs are produced only when a central bank-aided fail-safe mechanism must be put in place