

# Glimpse

On-Demand PoW Light Client with Constant-Size Storage for DeFi

Giulia Scaffino

giulia.scaffino@tuwien.ac.at

Lukas Aumayr

lukas.aumayr@tuwien.ac.at

Zeta Avarikioti

georgia.avarikioti@tuwien.ac.at

Matteo Maffei

matteo.maffei@tuwien.ac.at

TU Wien

USENIX Security Symposium  
August 9-11, 2023



# Glimpse: Contributions



✓ Trustless

✓ Secure

✓ Constant-Size Storage

✓ DeFi Applications

✓ Compatible with as many chains as possible

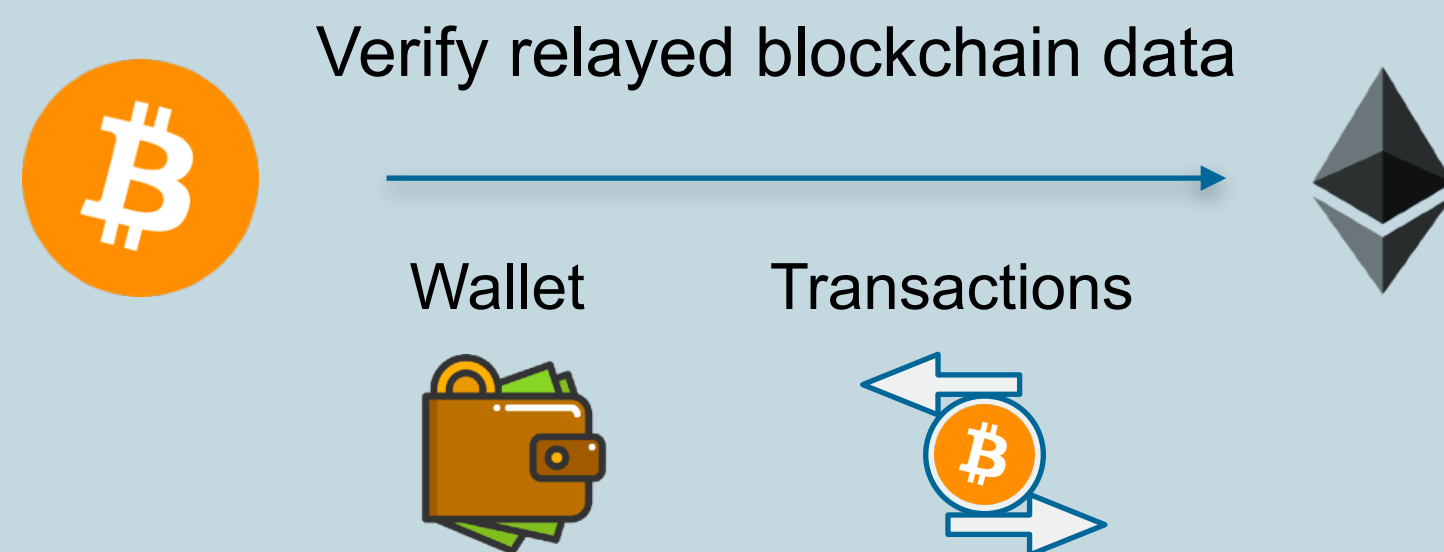
# Trustless Cross-Chain Communication



# Trustless Cross-Chain Communication



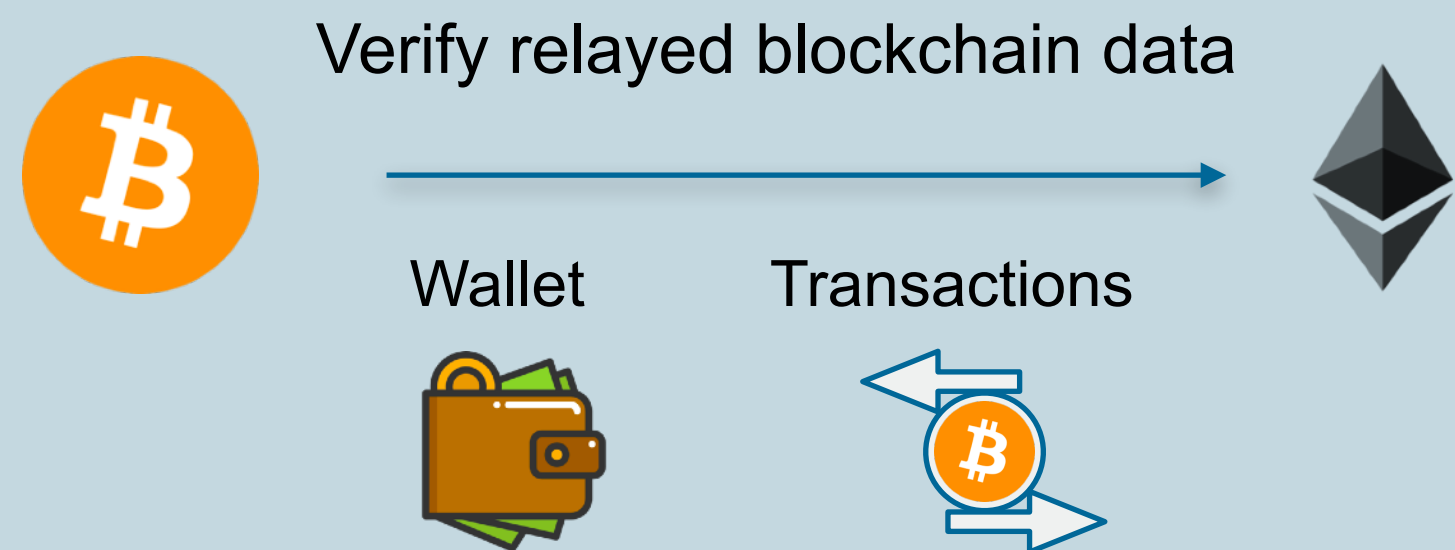
## Transaction Verification



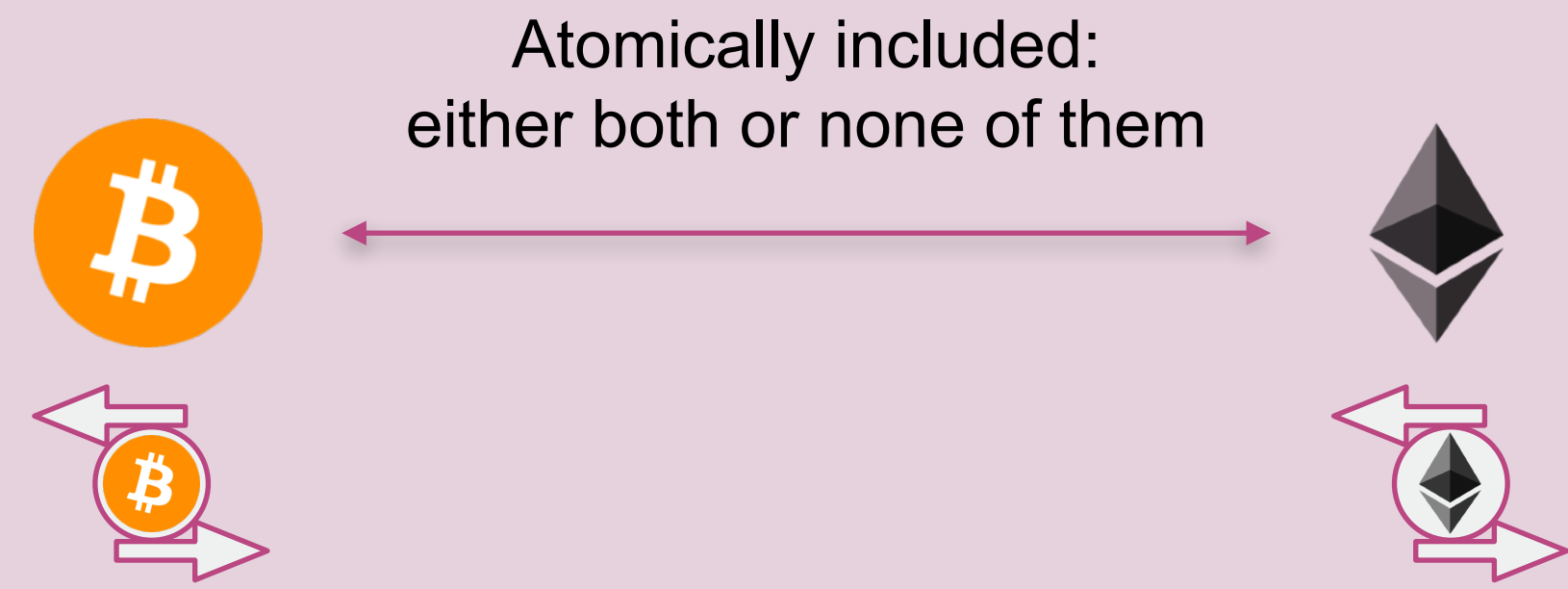
# Trustless Cross-Chain Communication



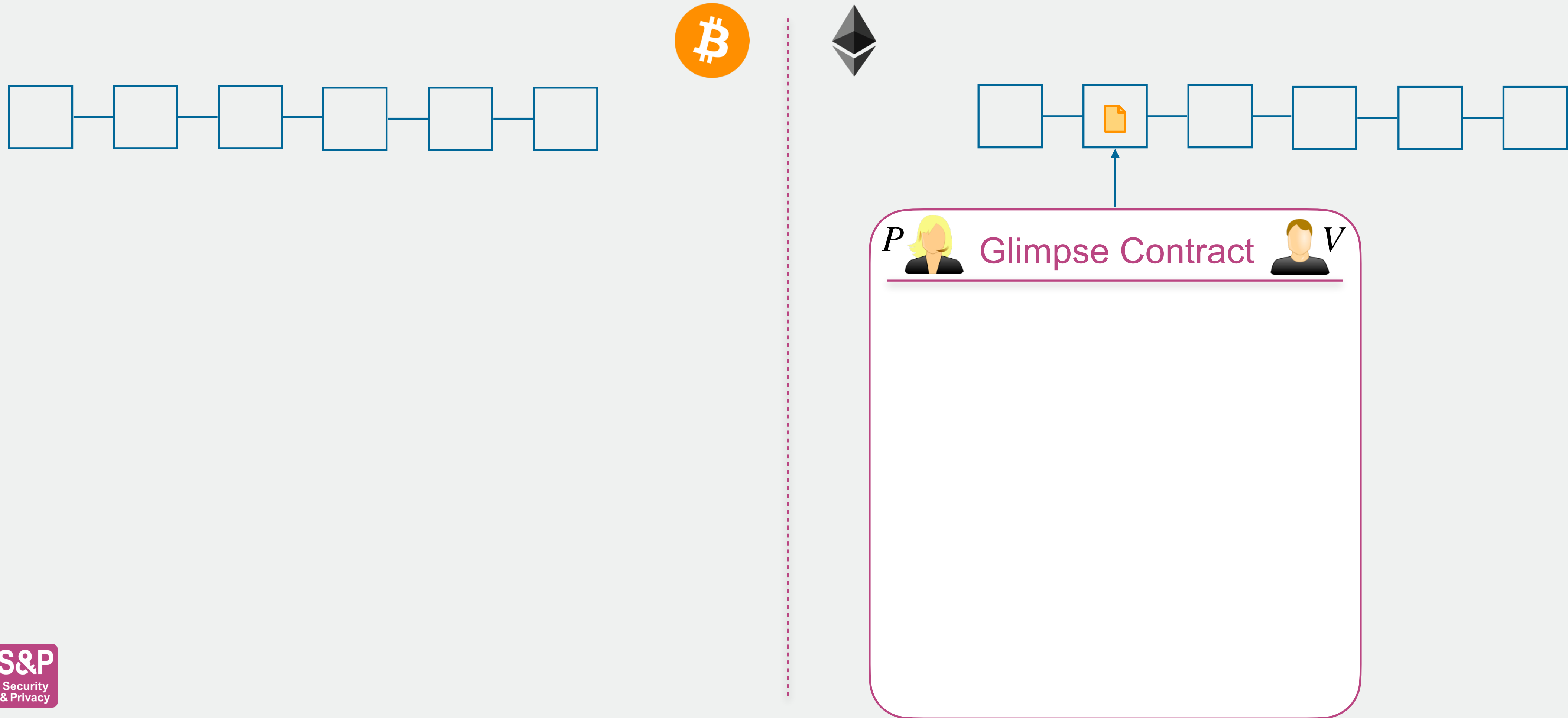
## Transaction Verification



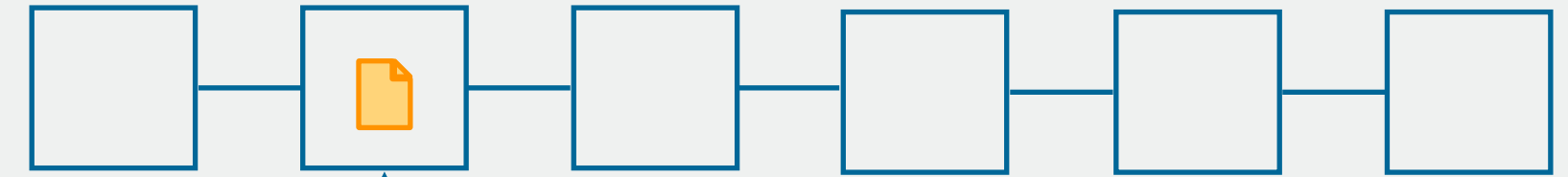
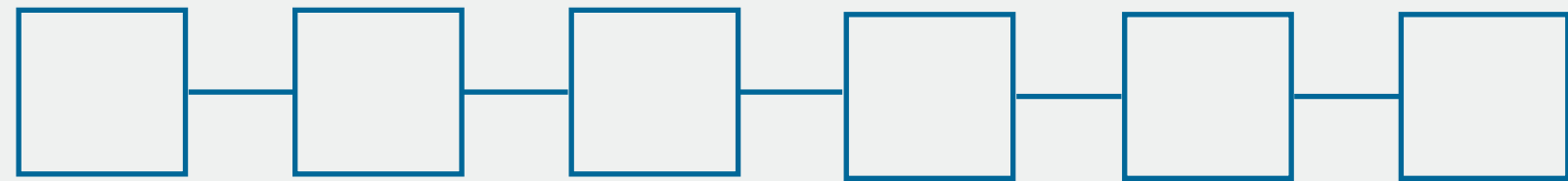
## Transaction Synchronisation





# Glimpse: Overview




# Glimpse: Overview




*P*  **Glimpse Contract**  *V*

“If  included in ,

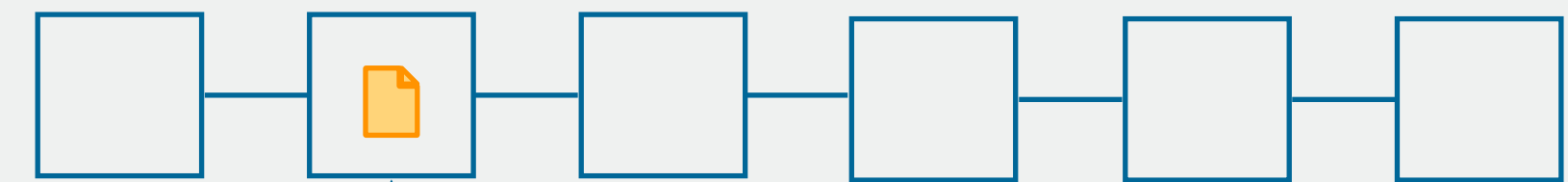
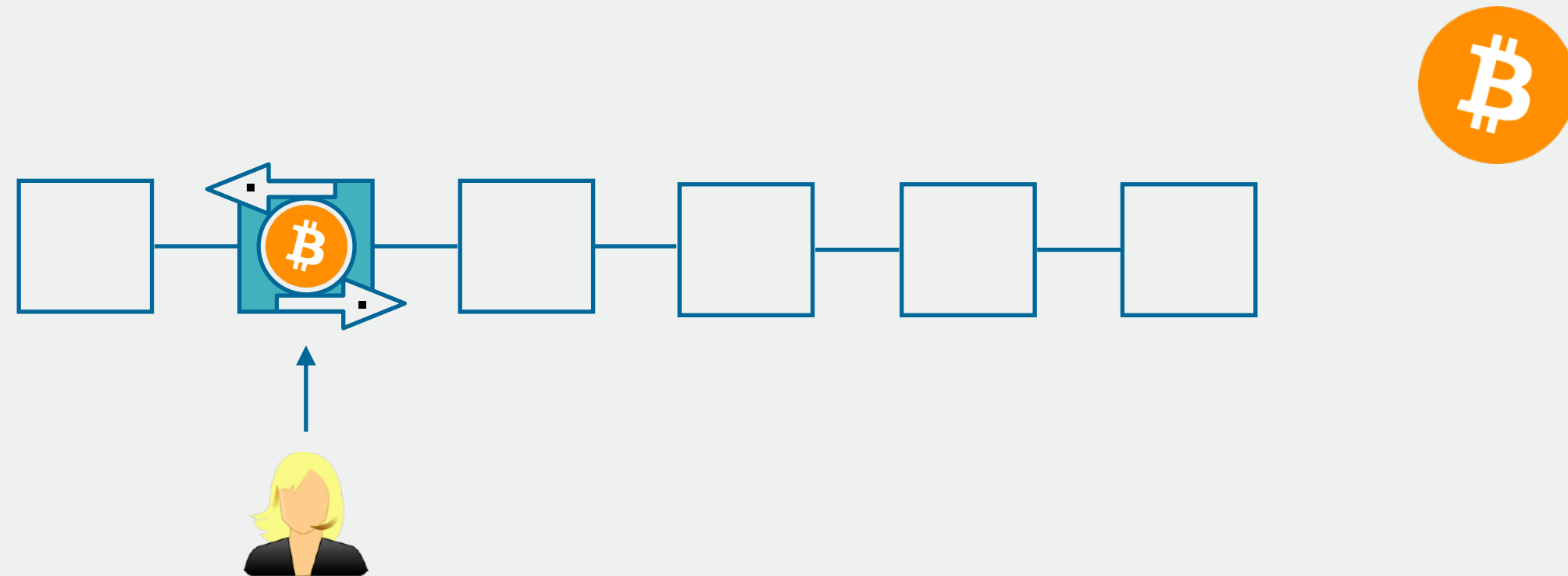
publish  <sup>*X*</sup>, upon verifying

**Proof**

[Empty box for proof]

Else, after *T* publish  <sup>*Y*</sup>.”

# Glimpse: Overview




*P*  **Glimpse Contract**  *V*

“If  included in ,

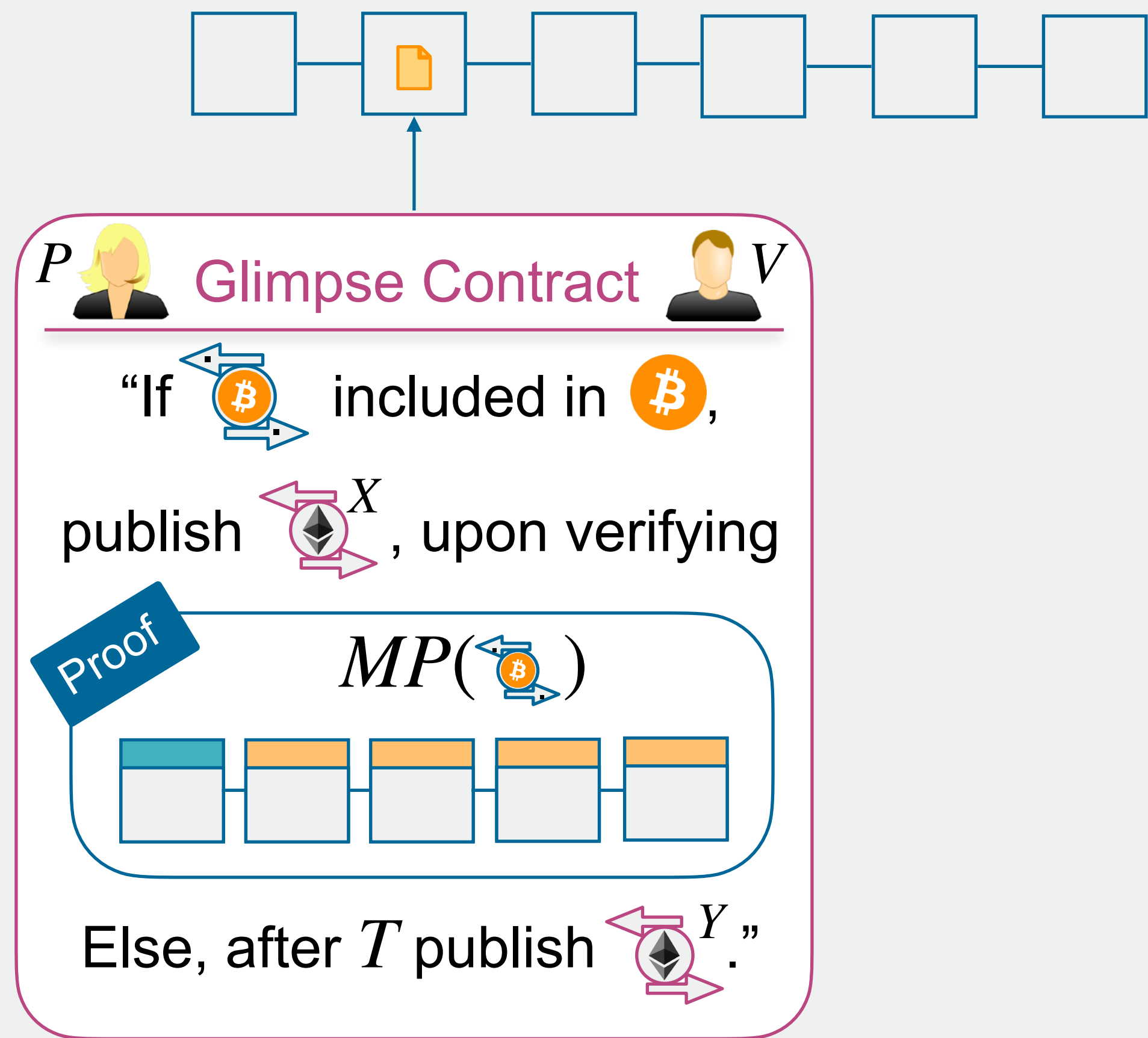
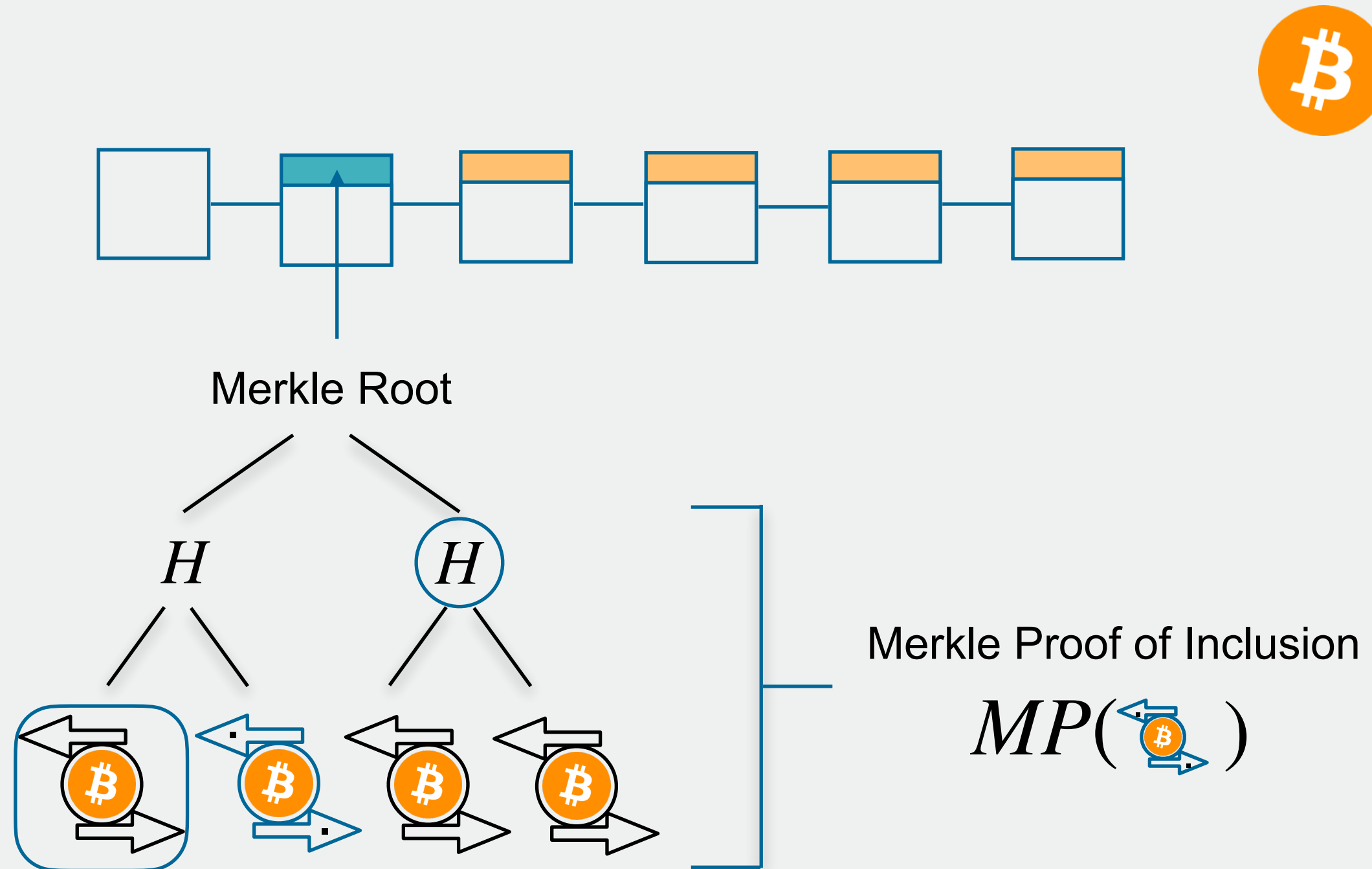
publish <sup>*X*</sup>, upon verifying

**Proof**

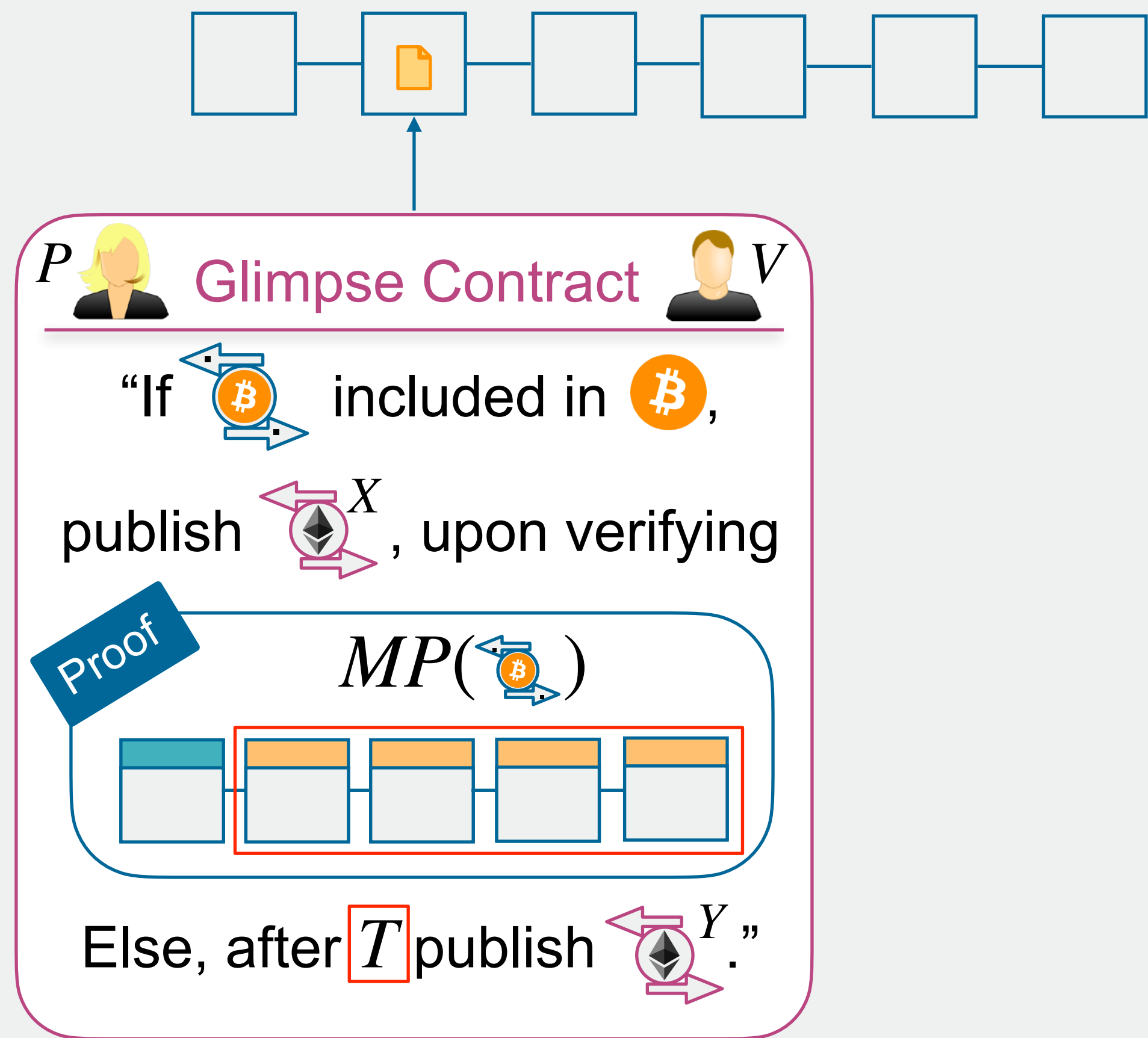
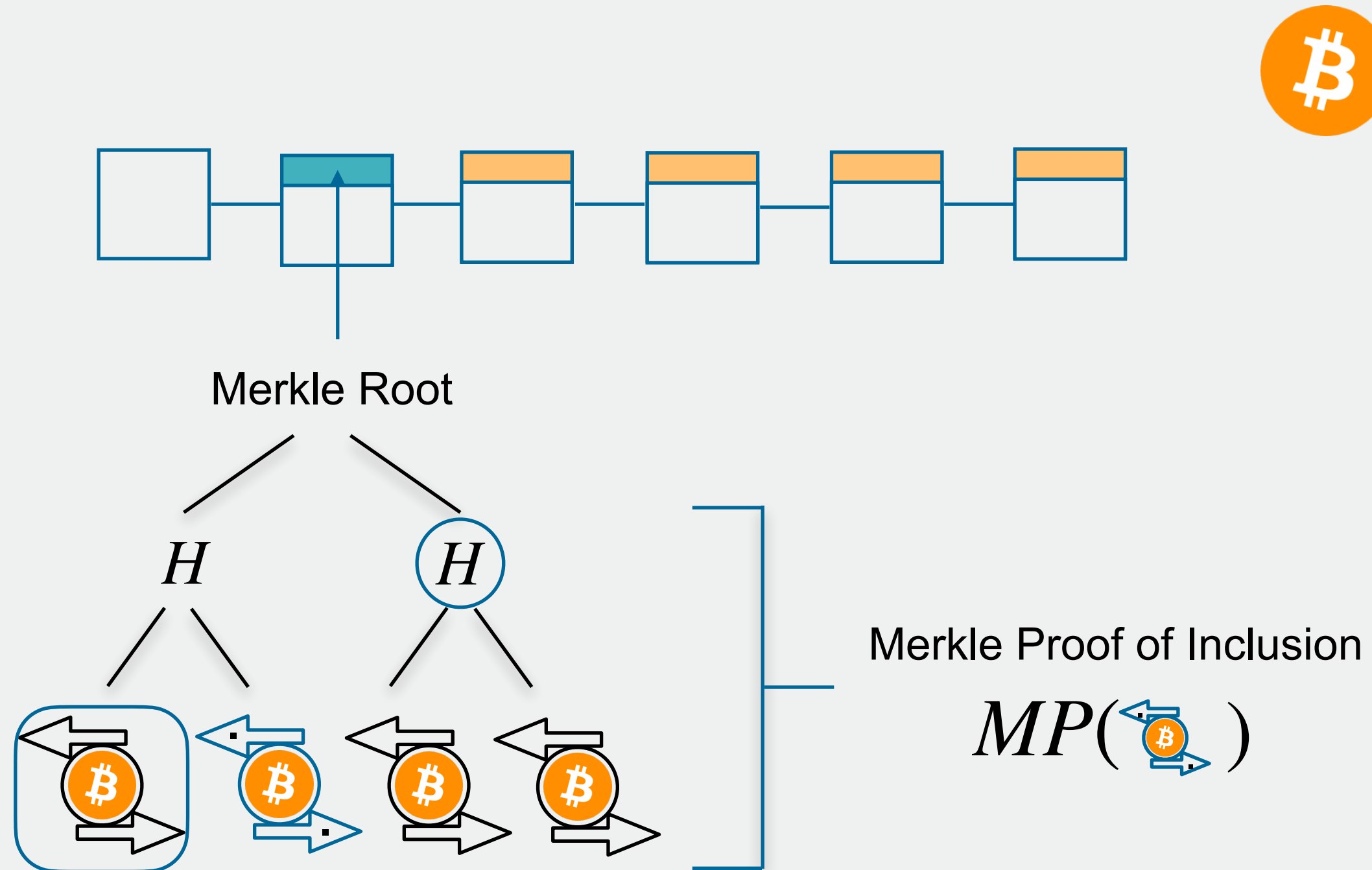
Else, after *T* publish <sup>*Y*</sup>.”



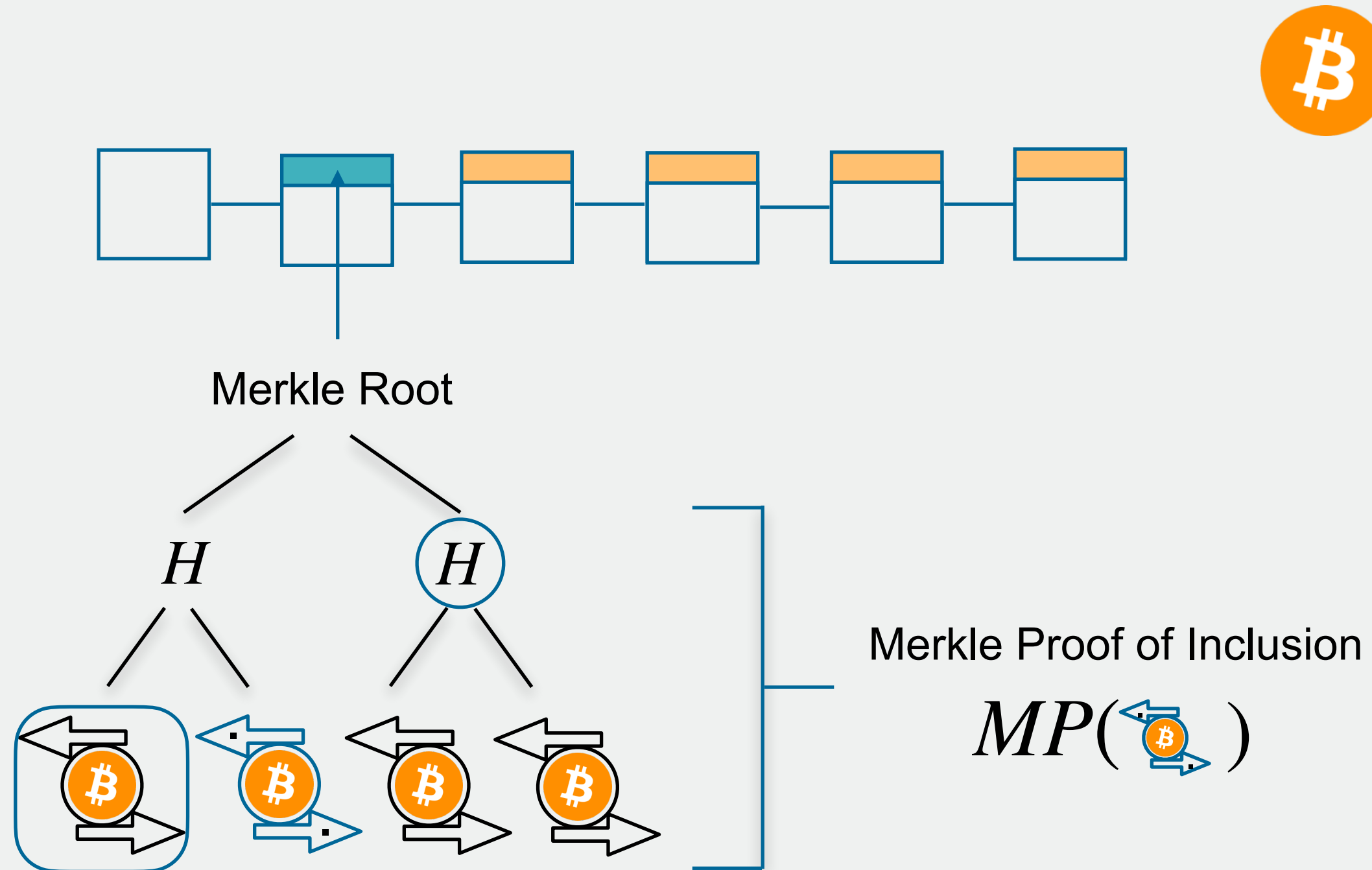
# Glimpse: Proof Construction

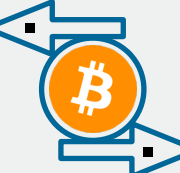



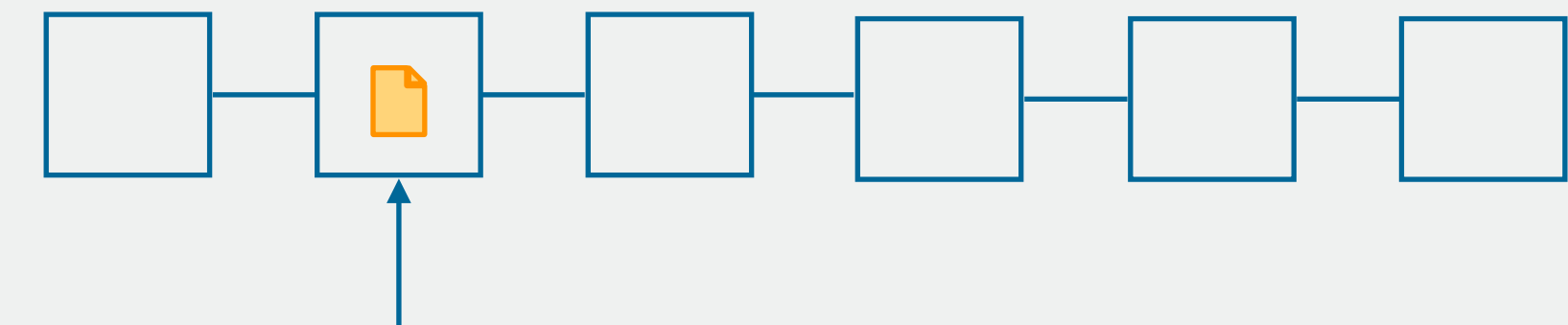
# Glimpse: Proof Construction







# Glimpse: Proof Construction

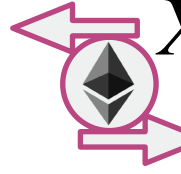


By fully knowing  upfront,  can forge a proof beforehand!

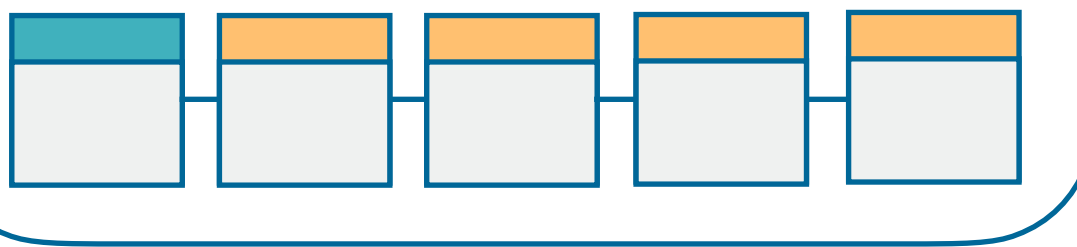


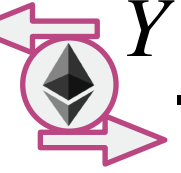
*P*  **Glimpse Contract**  *V*

“If  included in ,

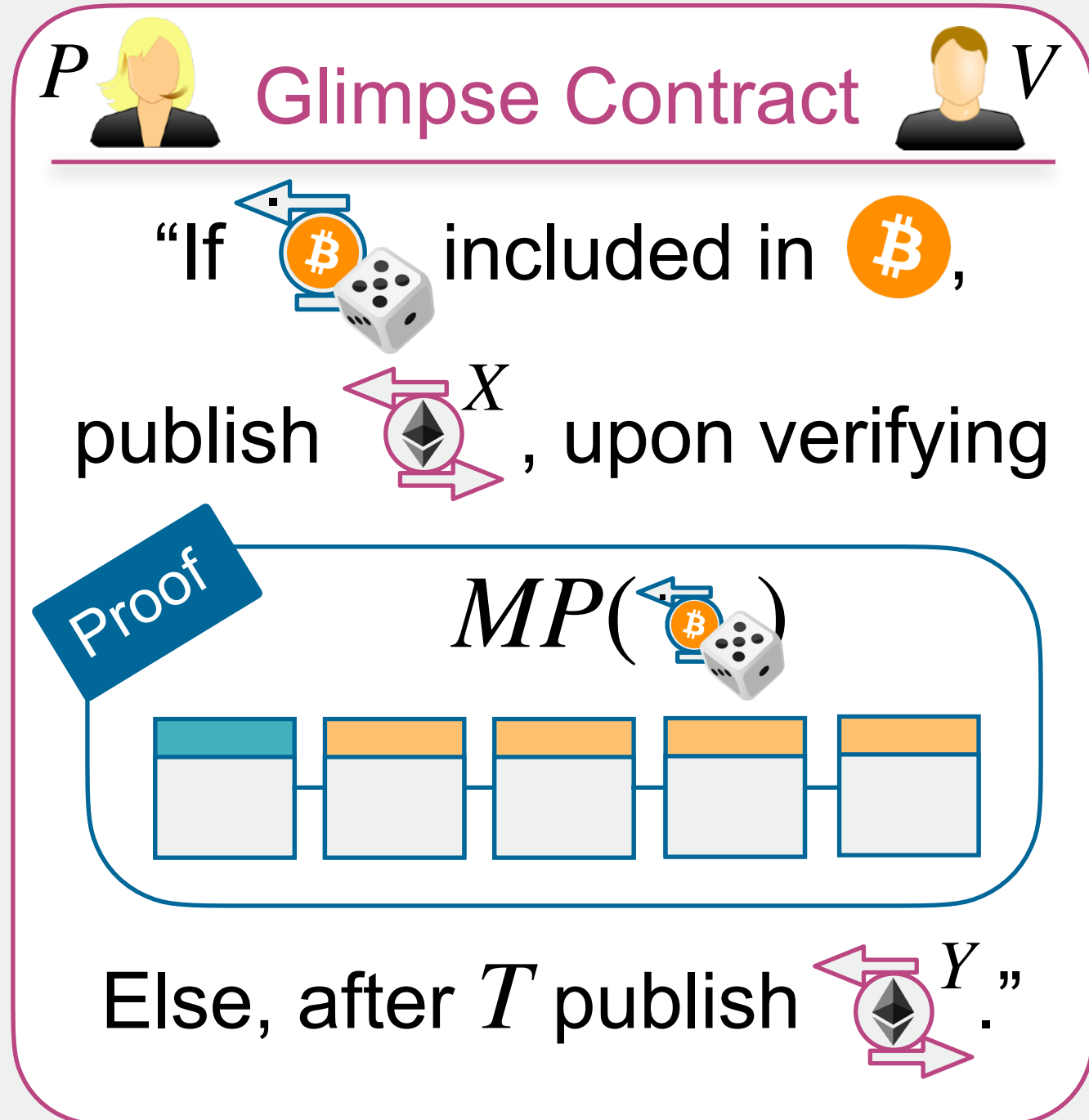
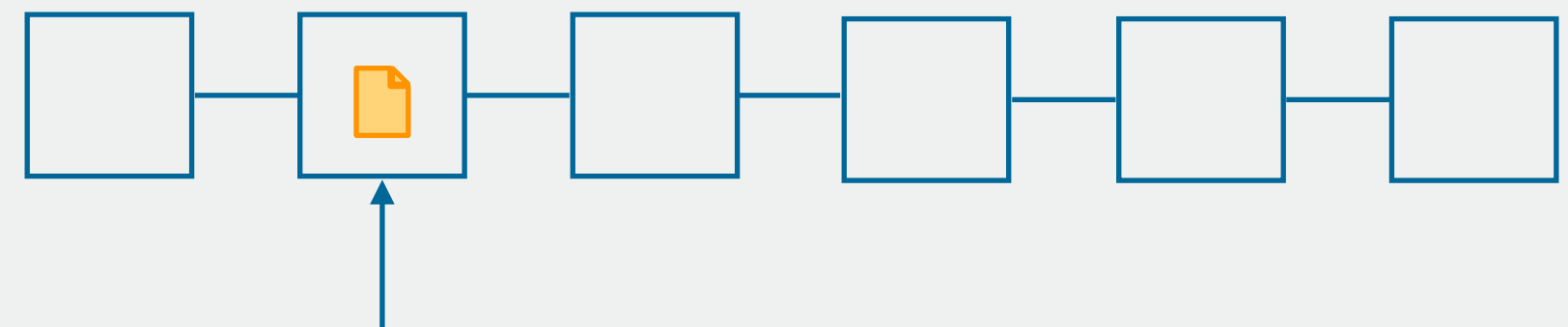
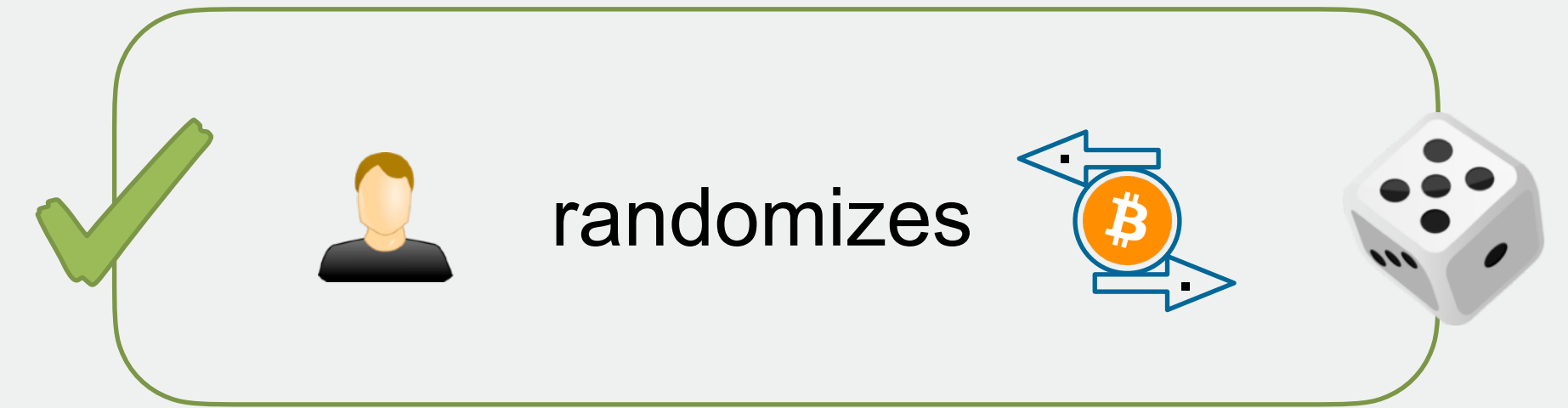
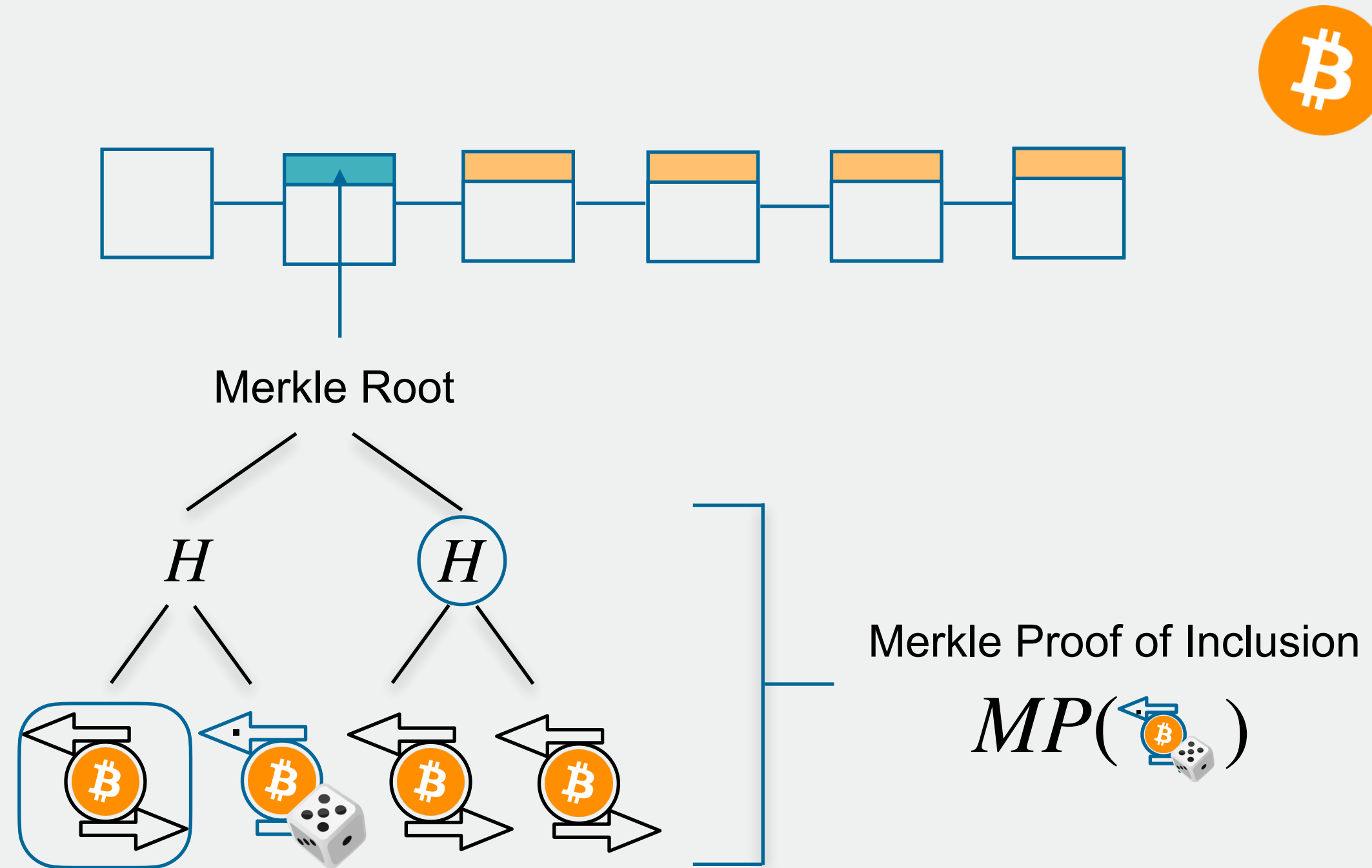
publish <sup>*X*</sup>, upon verifying

**Proof**  $MP(\text{⚡️})$

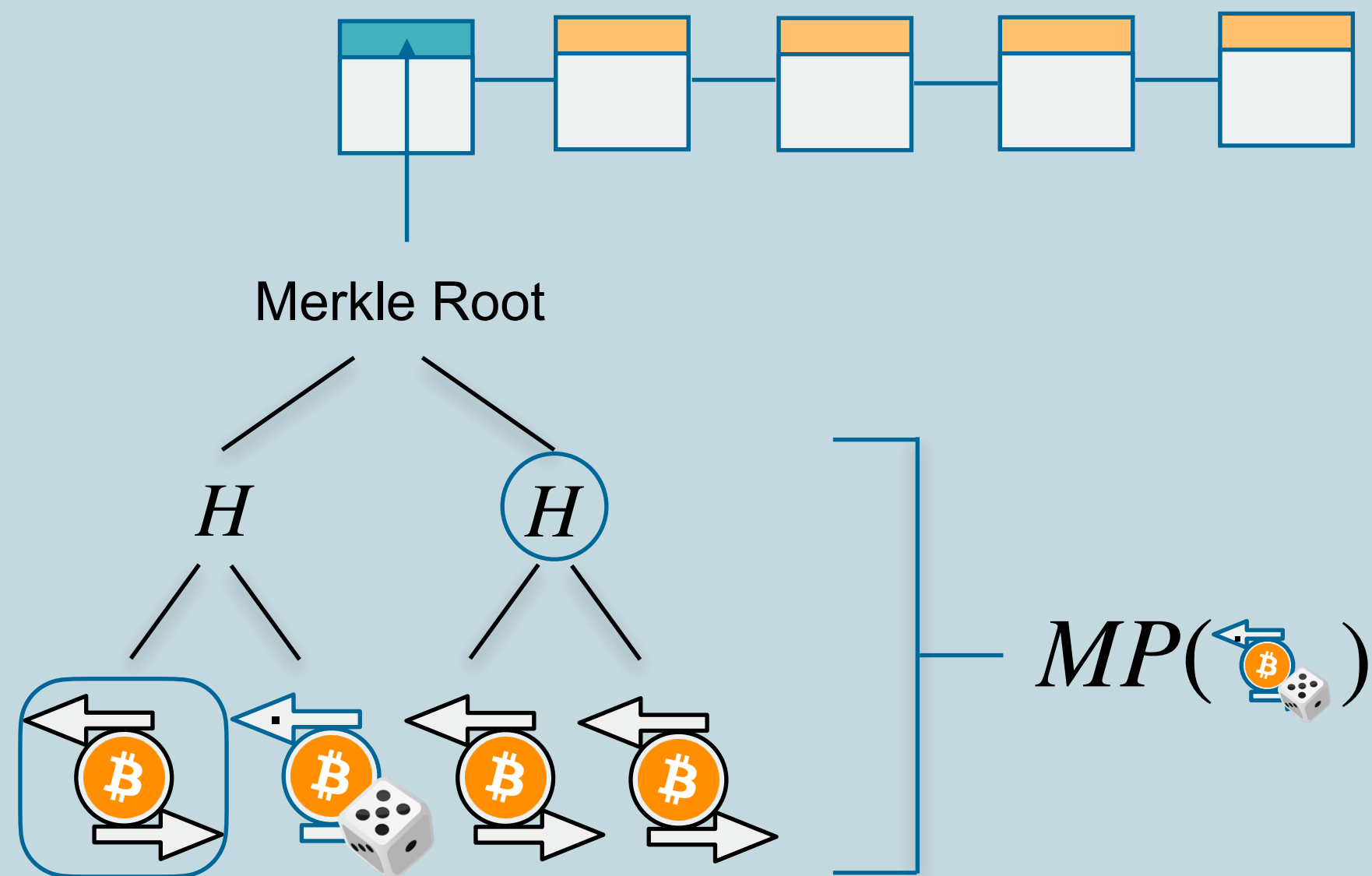


Else, after *T* publish <sup>*Y*</sup>.”




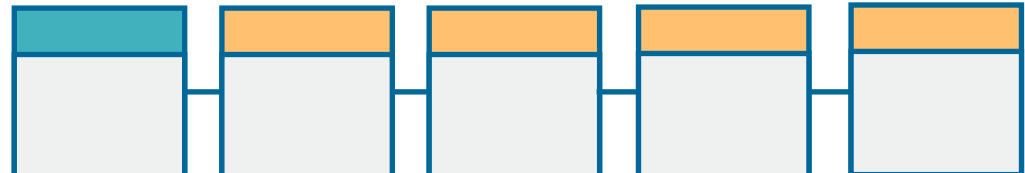

# Glimpse: Proof Construction

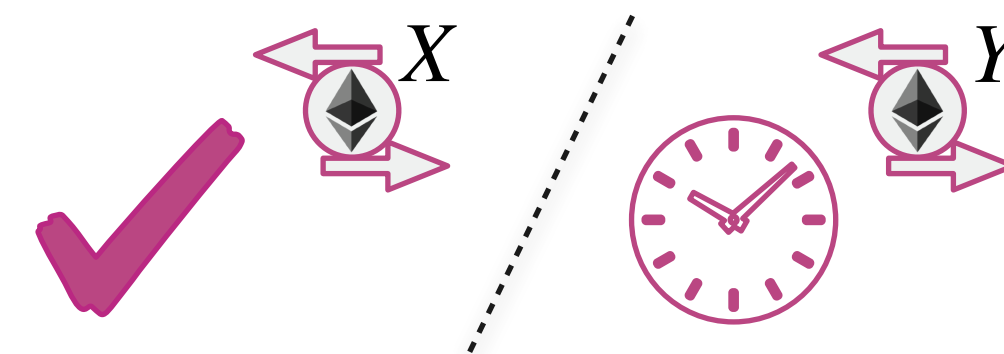


# Glimpse: The Contract



*P*  Glimpse Contract ( $d_S$ )  *V*

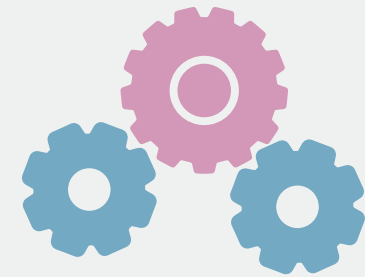
- Check that  includes the random string
- Check that  $MP(\text{$ ) hashes to the Merkle root in 
- Check that  are properly chained together
- Check that the hashes of  are smaller than the difficulty  $d_S$  of the source chain



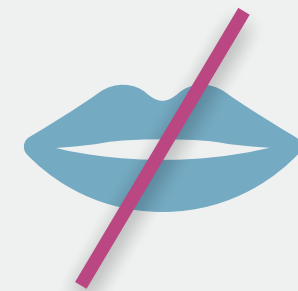
# Glimpse: Economic Security

We have defined the secure parameter space for Glimpse with respect to:

- Proof Forgery Attacks

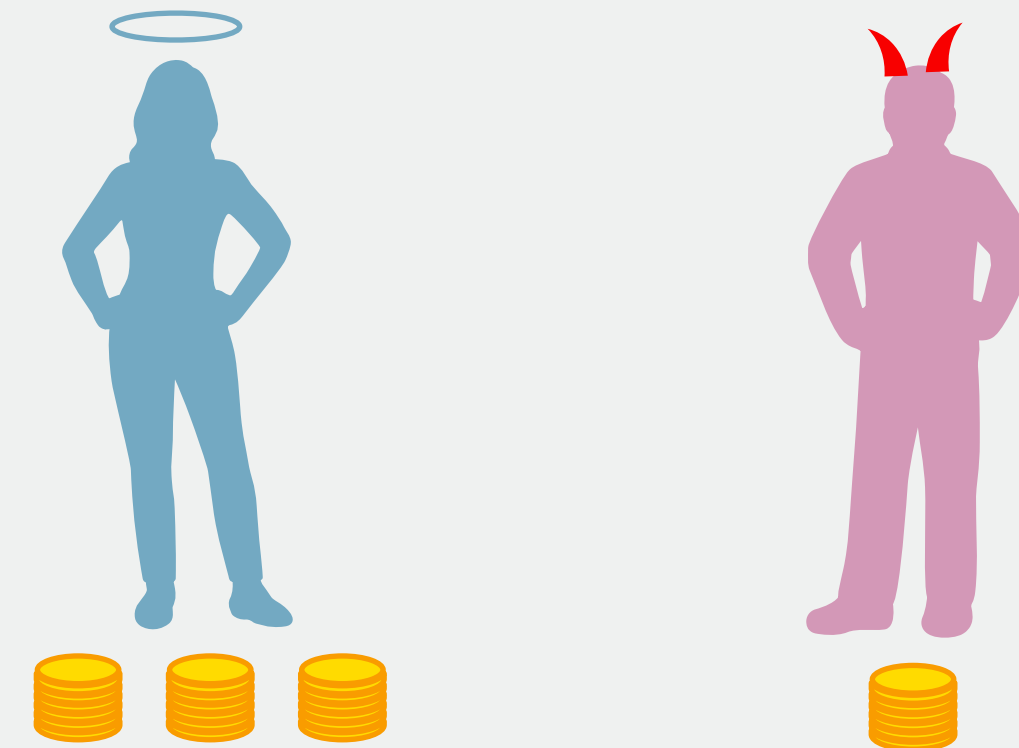


- Censorship Attacks

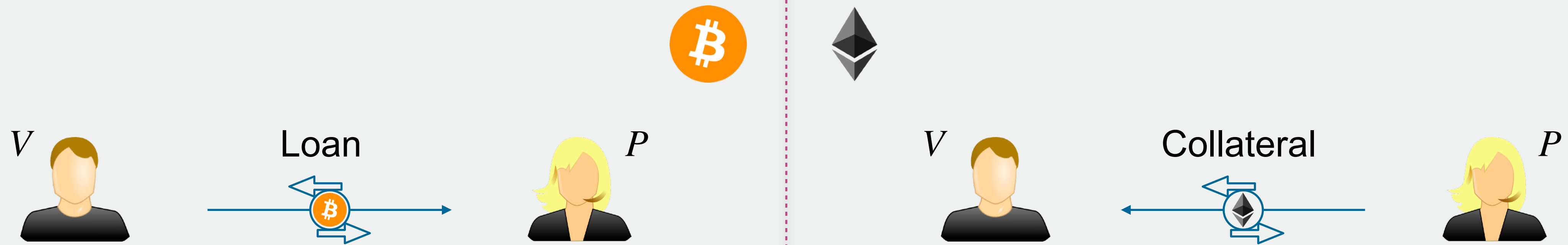


## Take Away

It has to be more profitable to behave honestly than attacking the bridge!

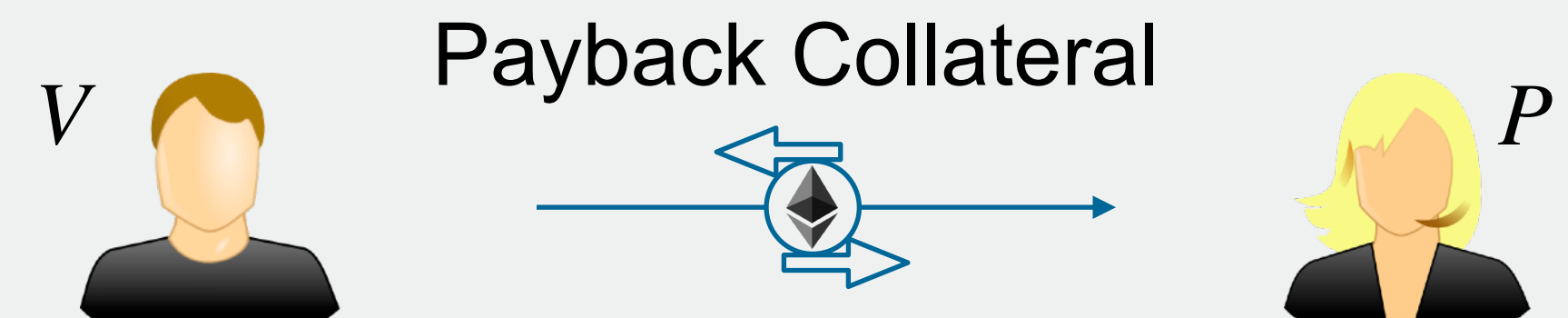
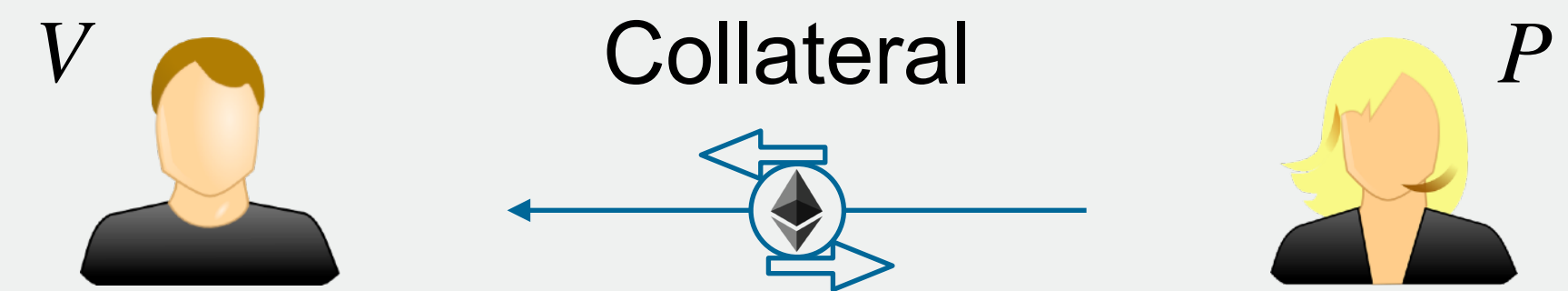
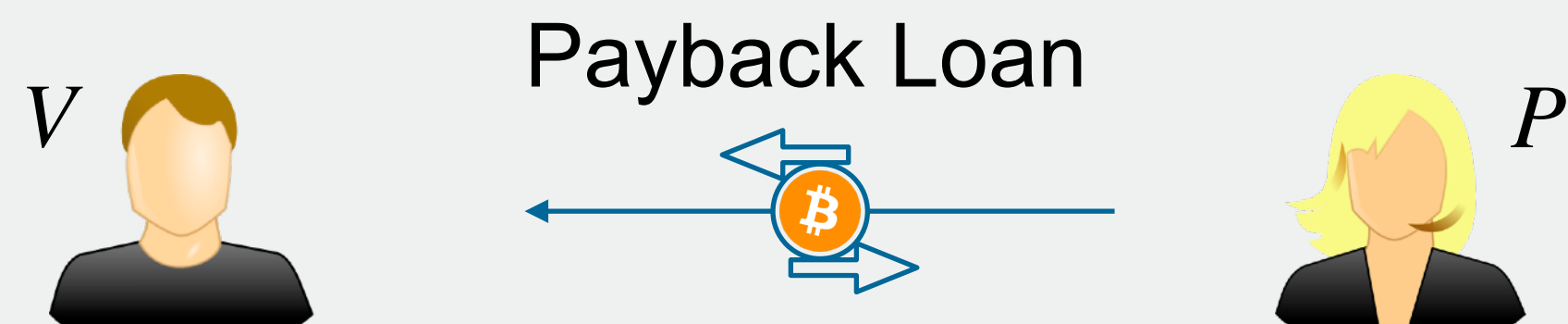
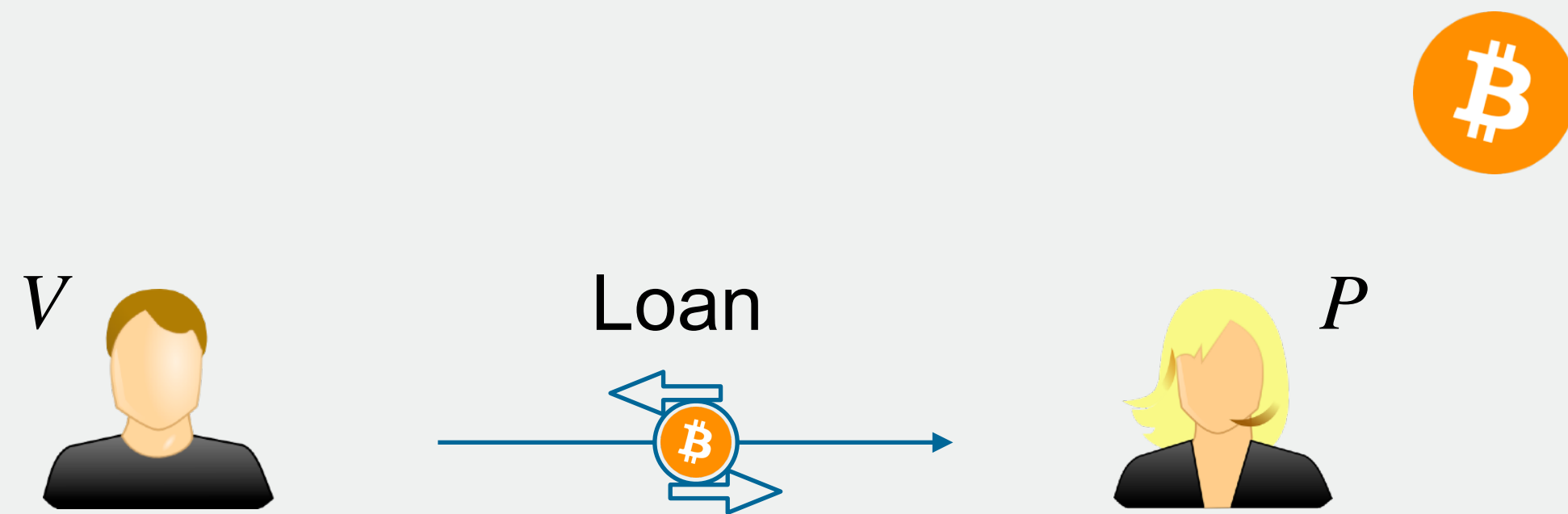


# Glimpse for Cross-Chain Lending



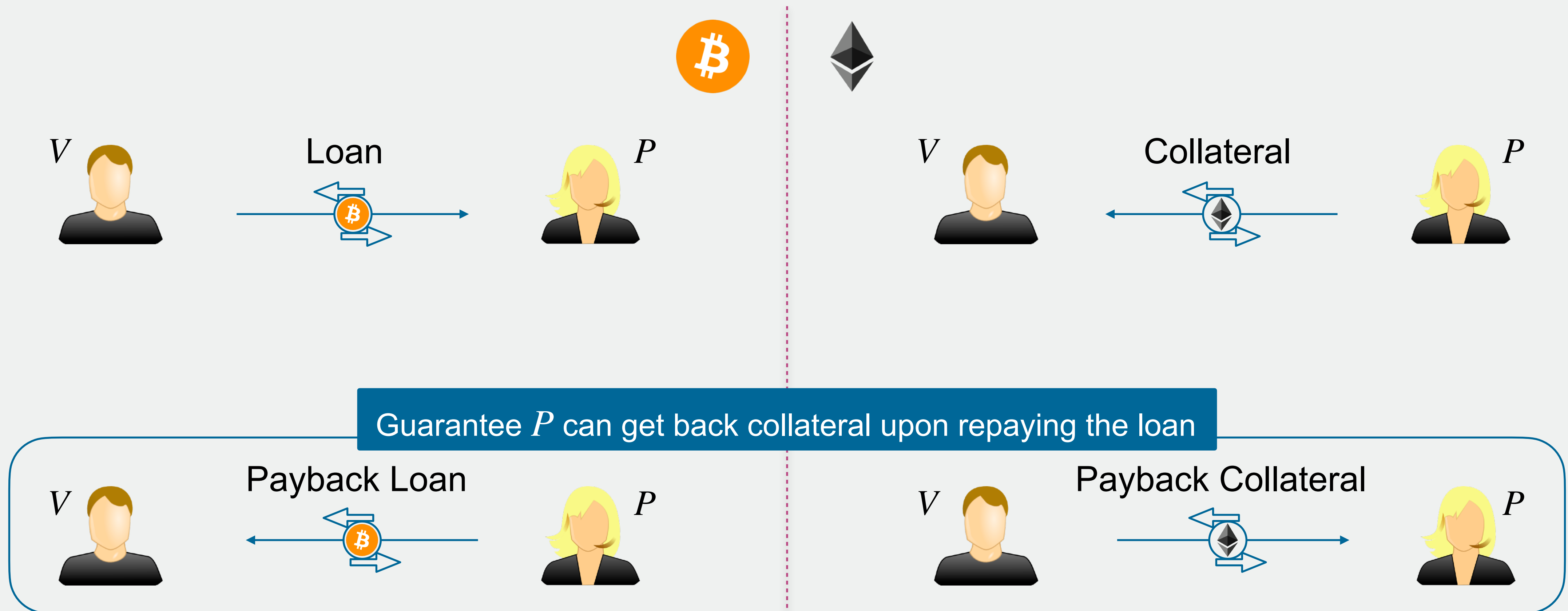


# Glimpse for Cross-Chain Lending

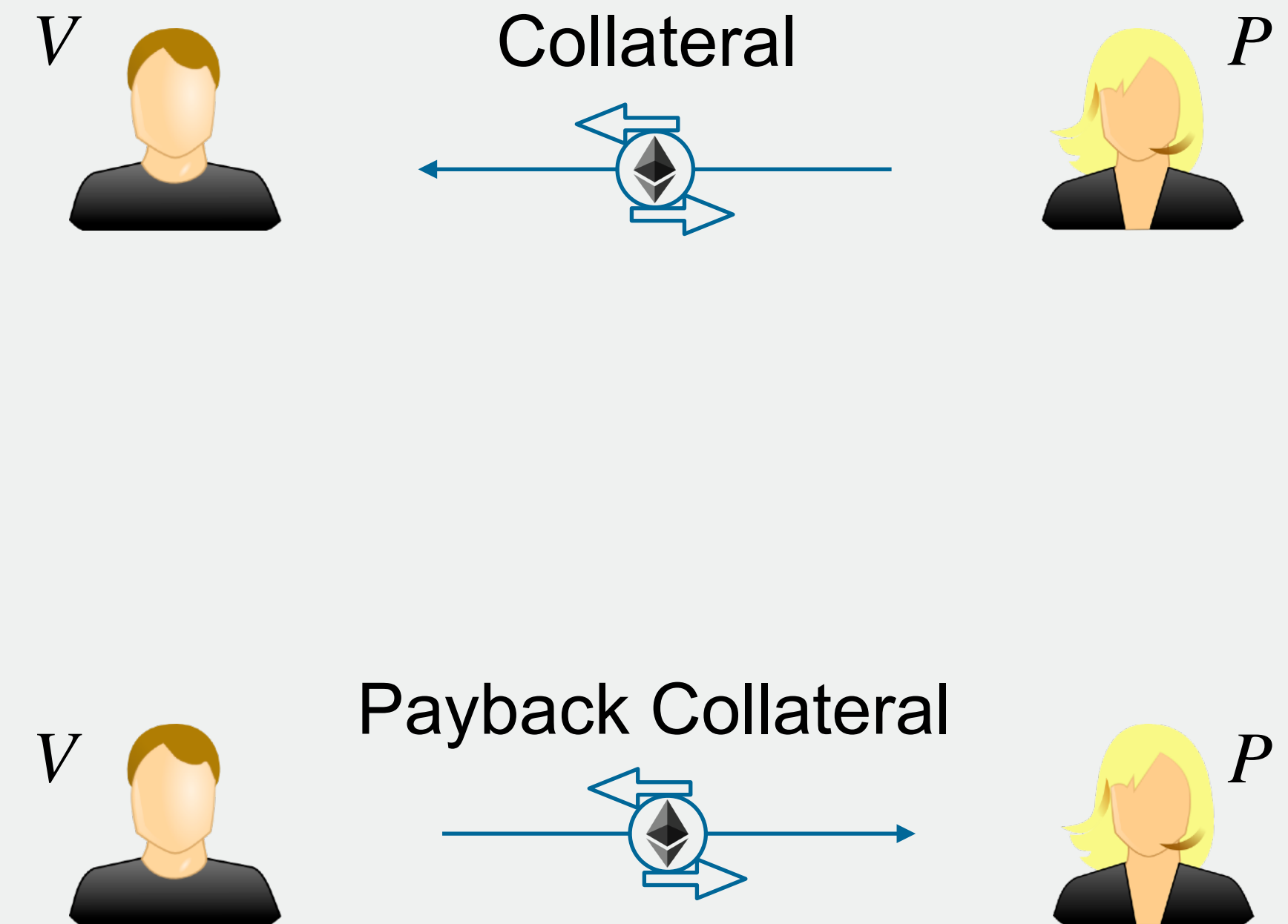
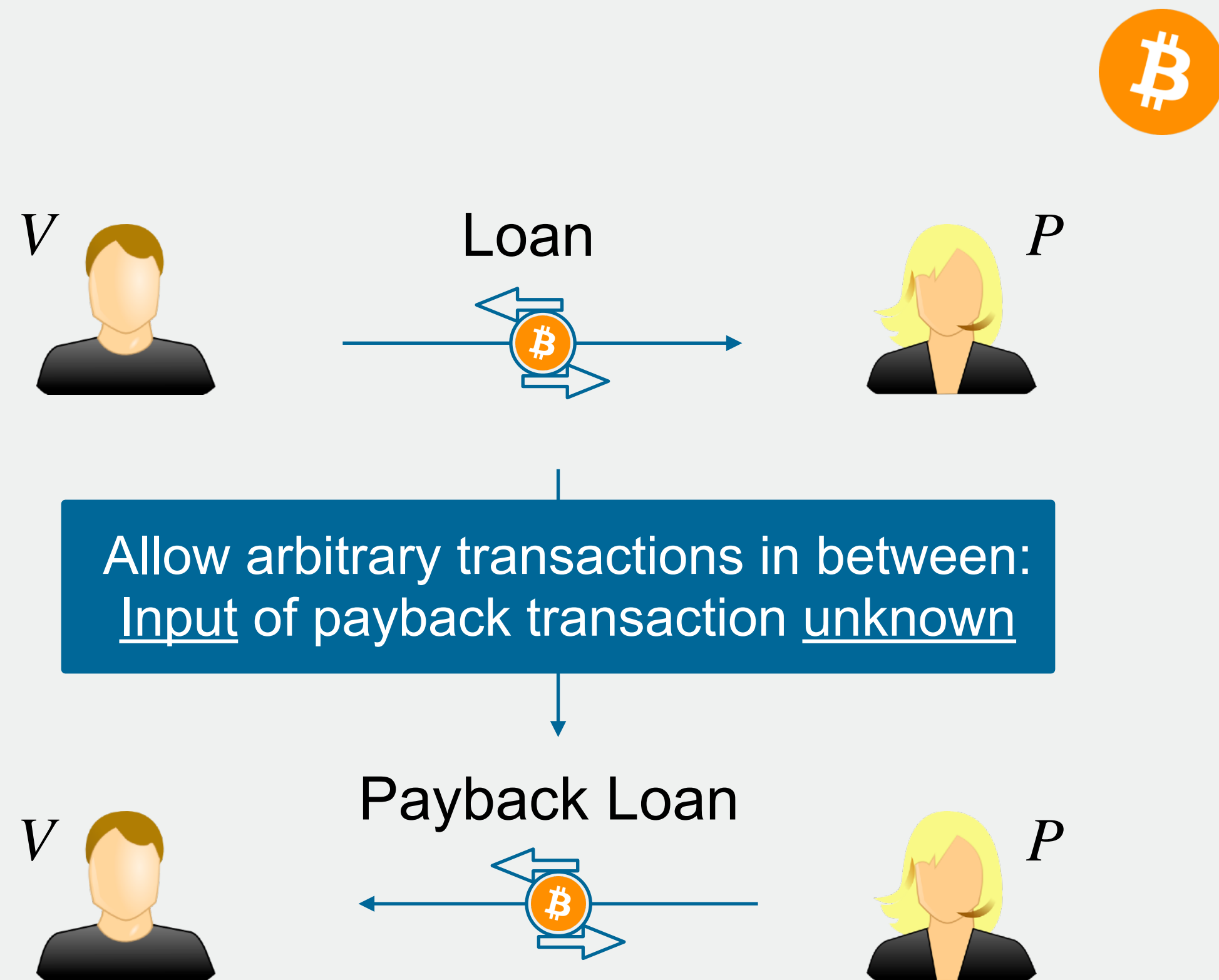




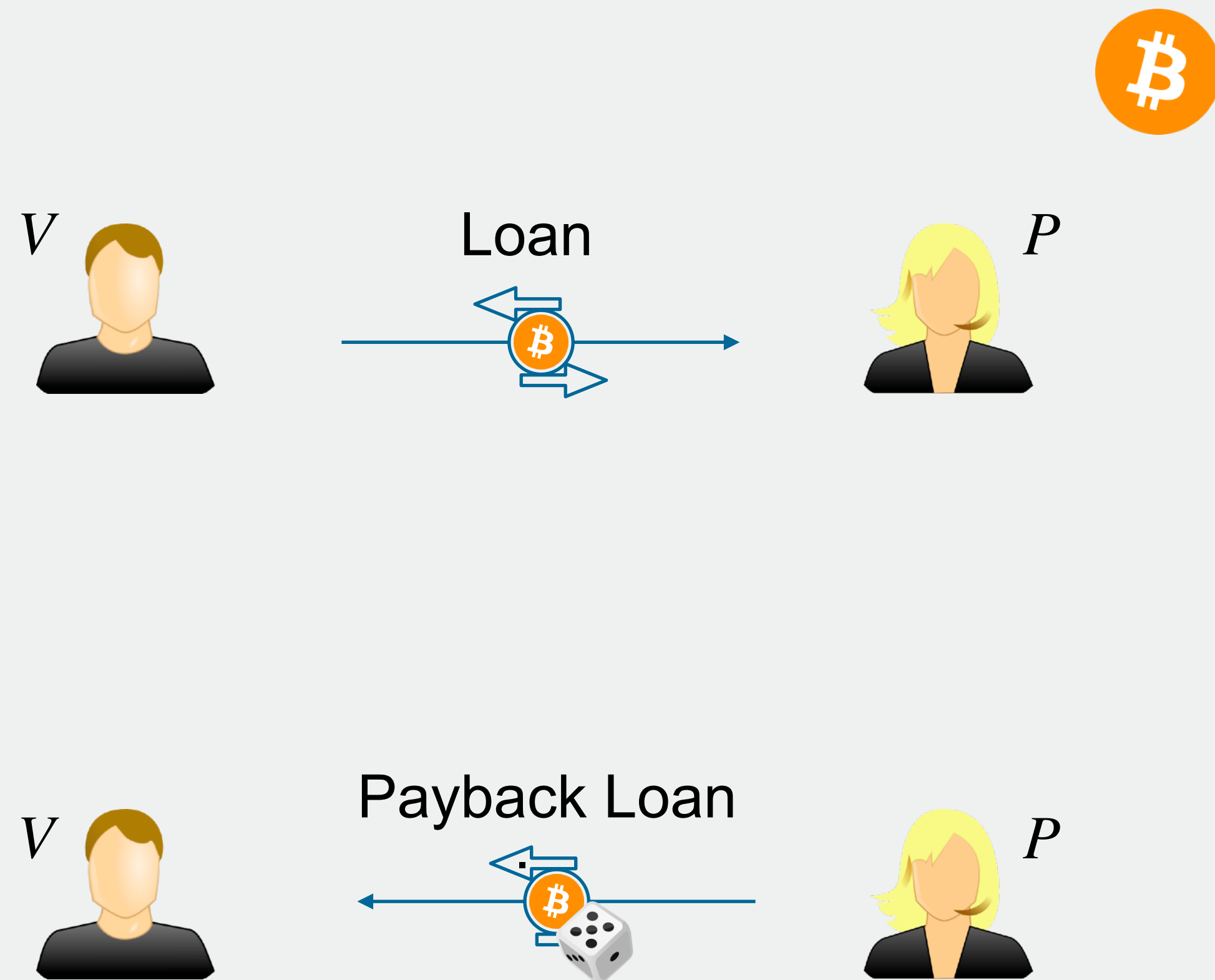
# Glimpse for Cross-Chain Lending




# Glimpse for Cross-Chain Lending



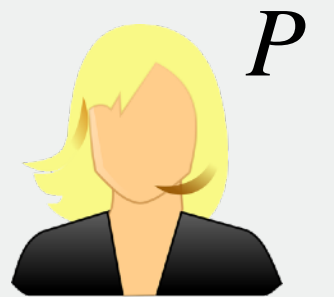
# Glimpse for Cross-Chain Lending



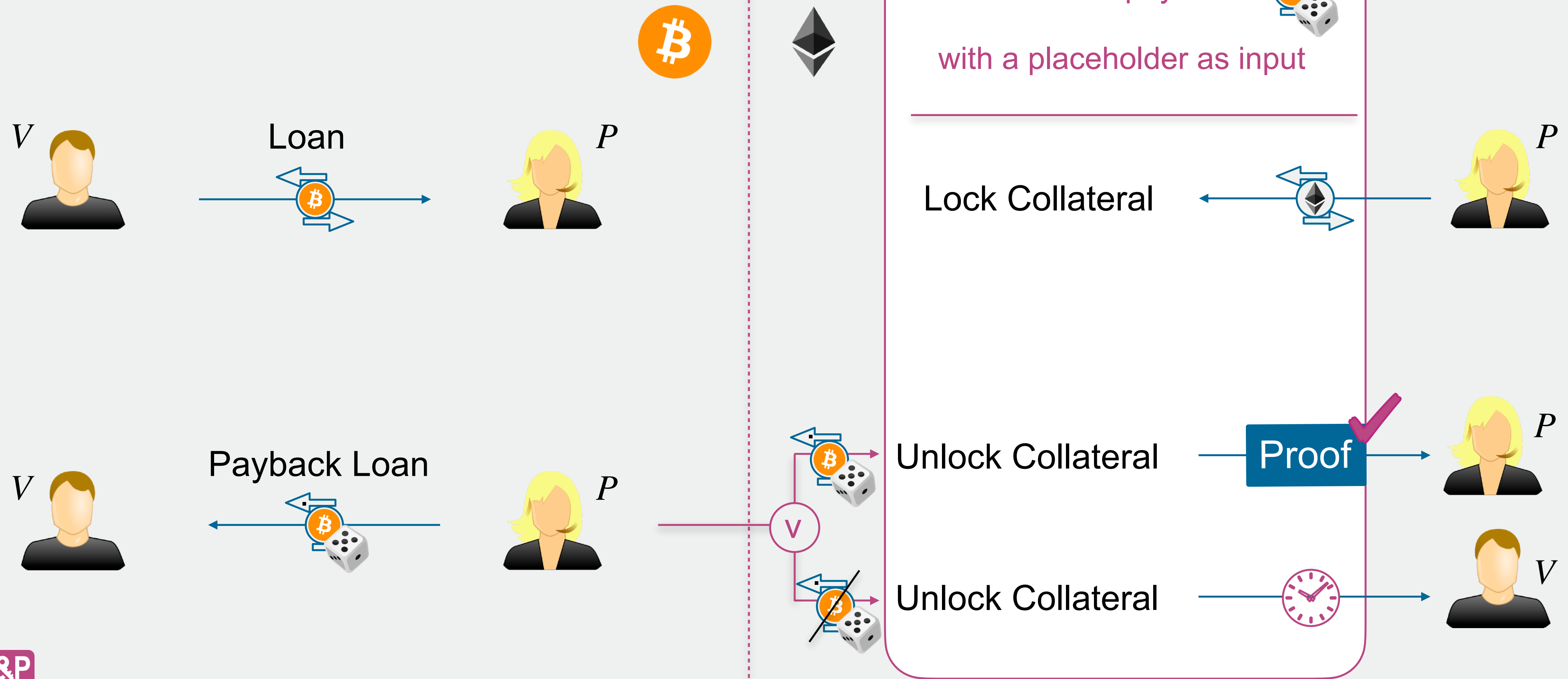
## Glimpse Contract

Conditioned to payback   
with a placeholder as input

Lock Collateral 

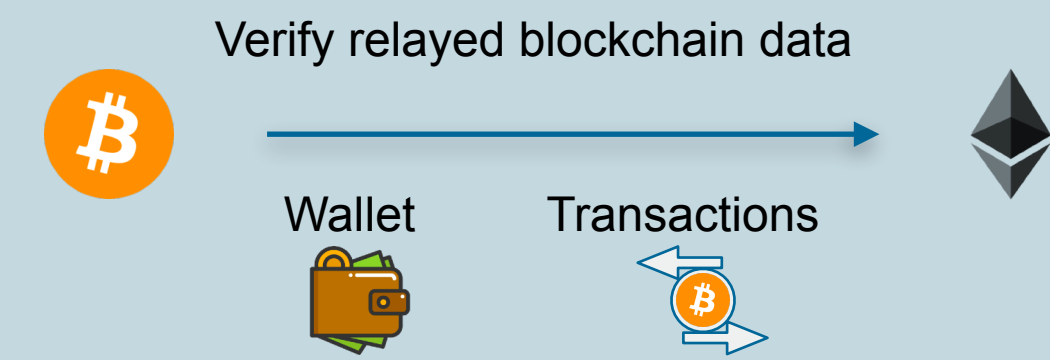


# Glimpse for Cross-Chain Lending



# Transaction Verification

## Transaction Verification



Light Client

Super-Light Client

Glimpse

(On-Demand Light Client)

Relayed Data & Storage:

$$\mathcal{O}(|B|)$$

$$\mathcal{O}(\log(|B|))$$

$$\mathcal{O}(1)$$

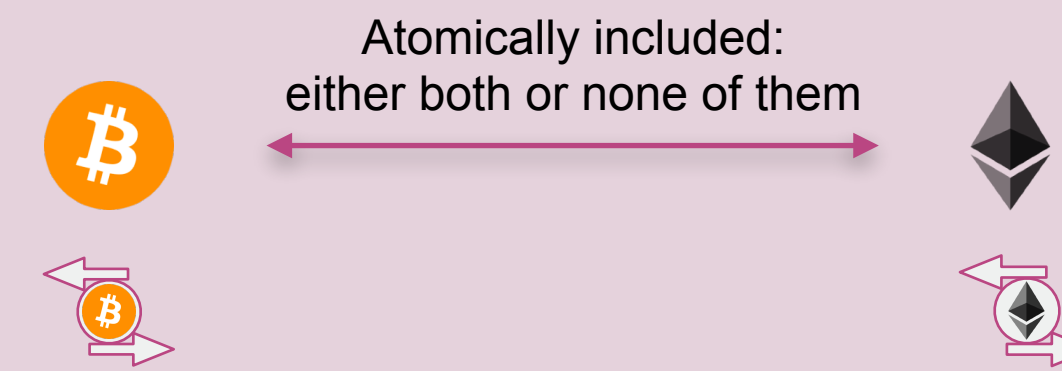
Backward Compatibility:



$|B|$  = Source Blockchain Length

# Transaction Synchronisation

## Transaction Synchronisation



### Atomic Swaps

Expressiveness:

Only Swaps

Compatibility:

Any Chain

### Glimpse

Swaps, DeFi apps, DNF,  
Transactions w/ placeholders



### Chain Relays

Any Application

Quasi-Turing  
Complete Chains

# Glimpse

On-Demand PoW Light Client with Constant-Size Storage for DeFi

Thank You!  
Questions?

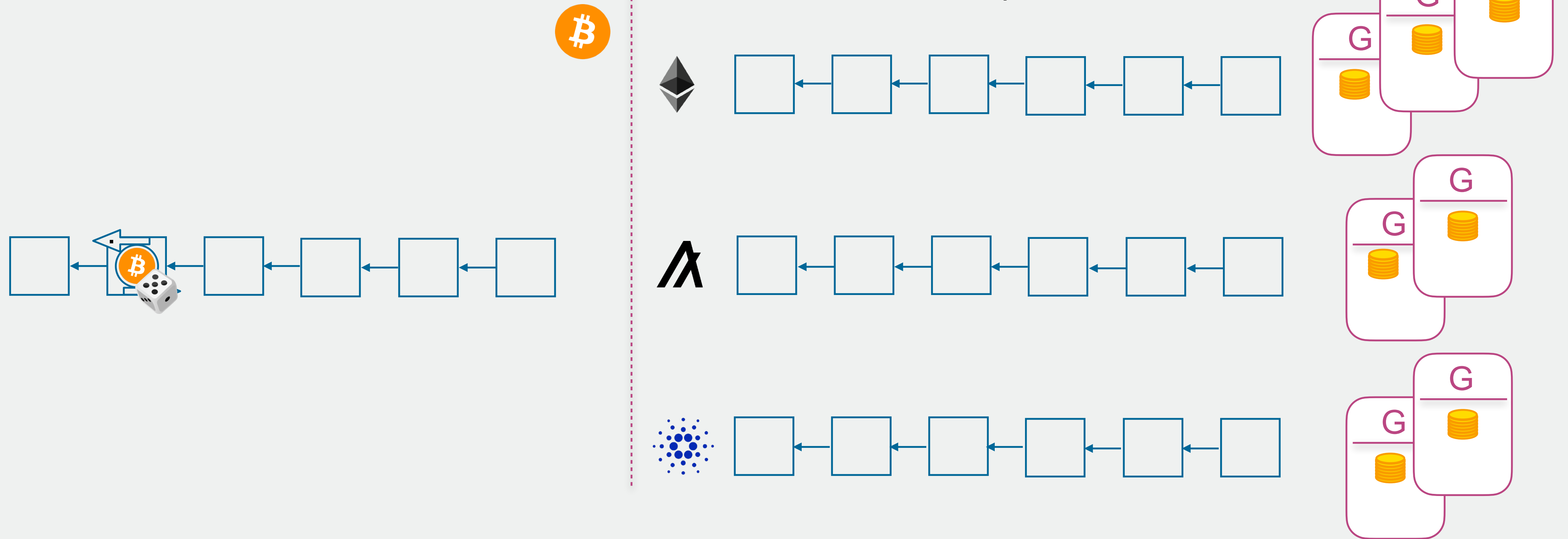
Giulia Scaffino, TU Wien  
✉ [giulia.scaffino@tuwien.ac.at](mailto:giulia.scaffino@tuwien.ac.at)



# Backup



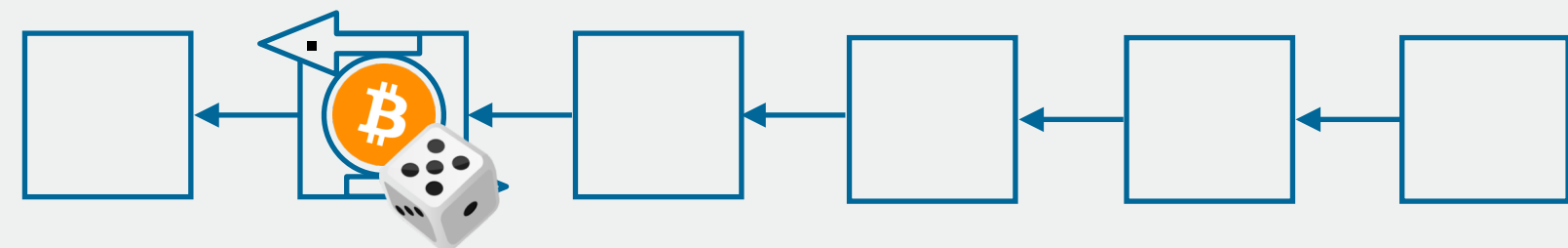
# Proof Forgery Attacks



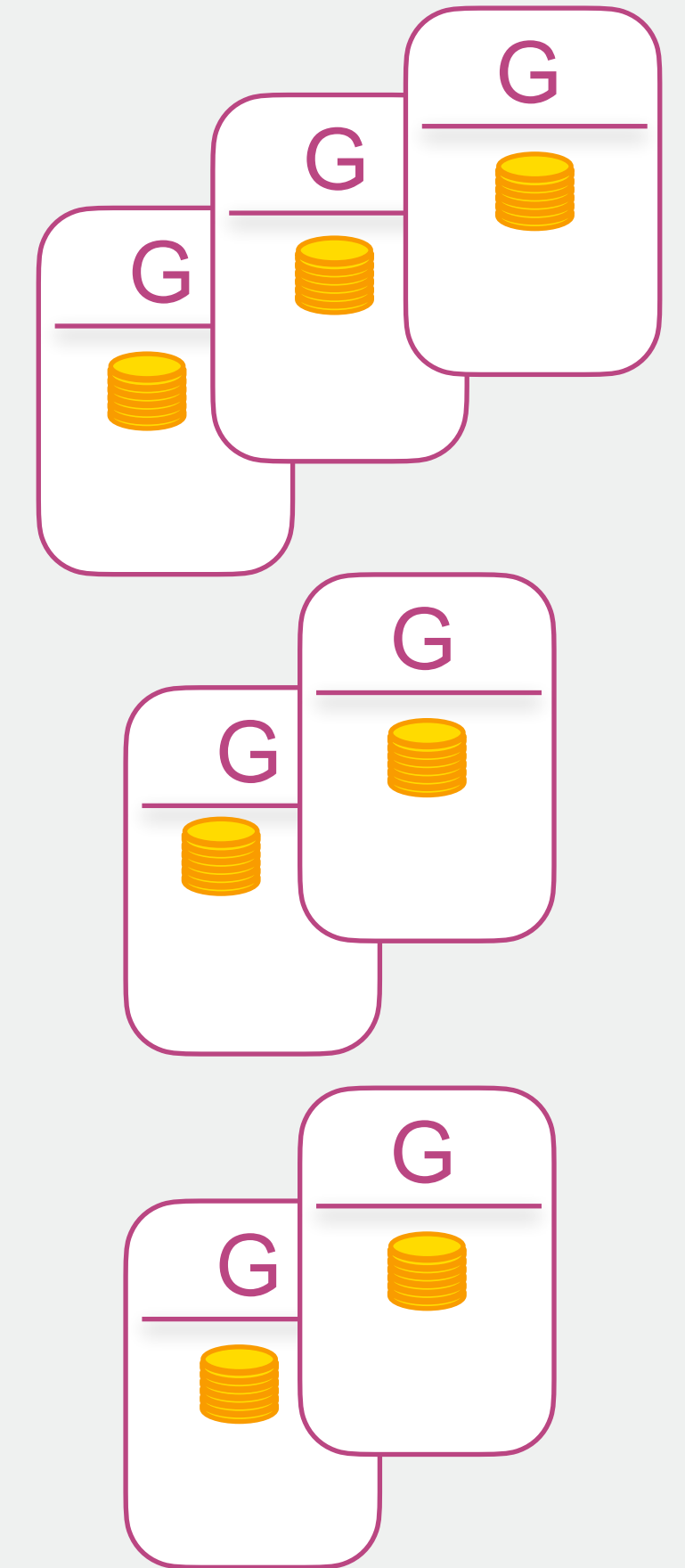
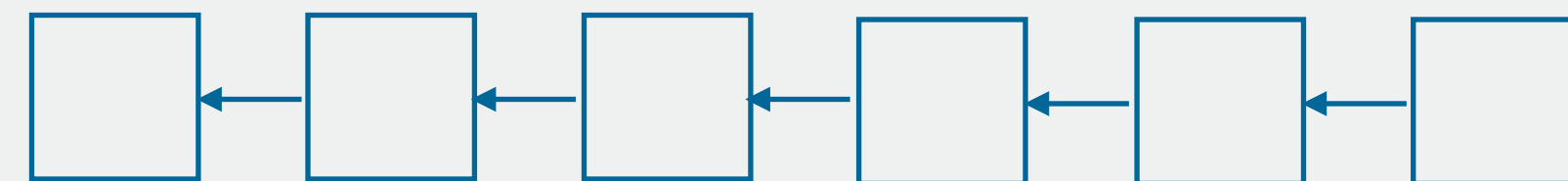
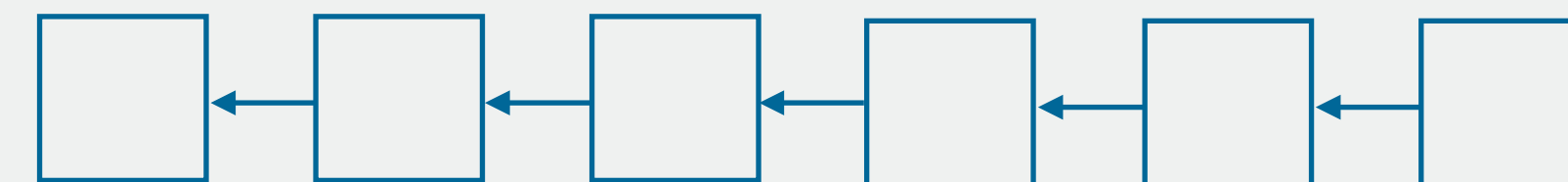
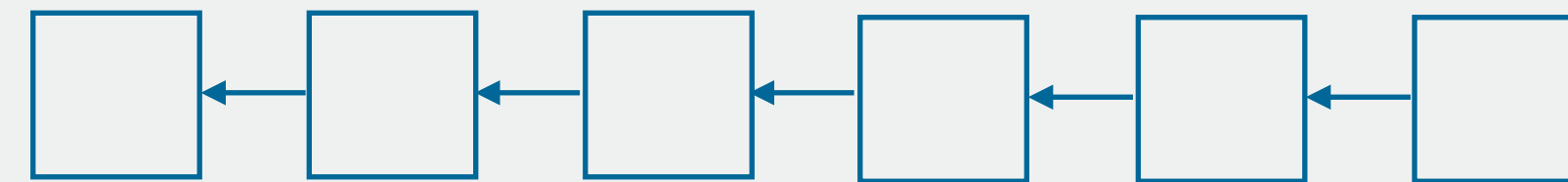
# Proof Forgery Attacks

Bribed miners produce a

**Forged Proof**



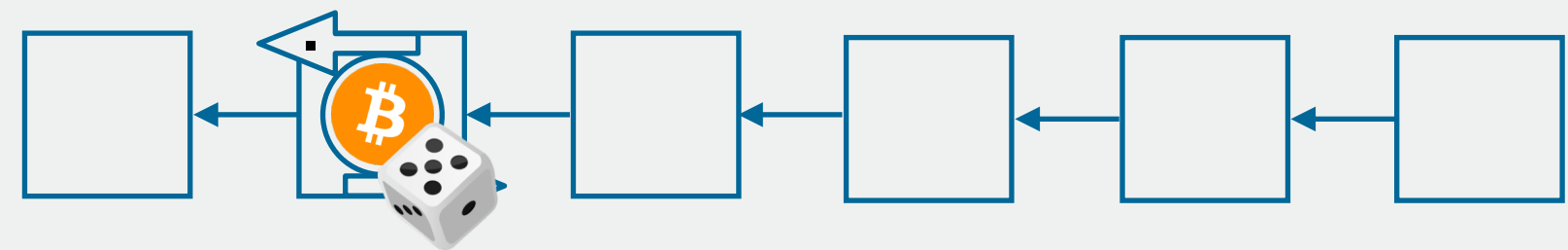
Simultaneously active  
Glimpse contracts



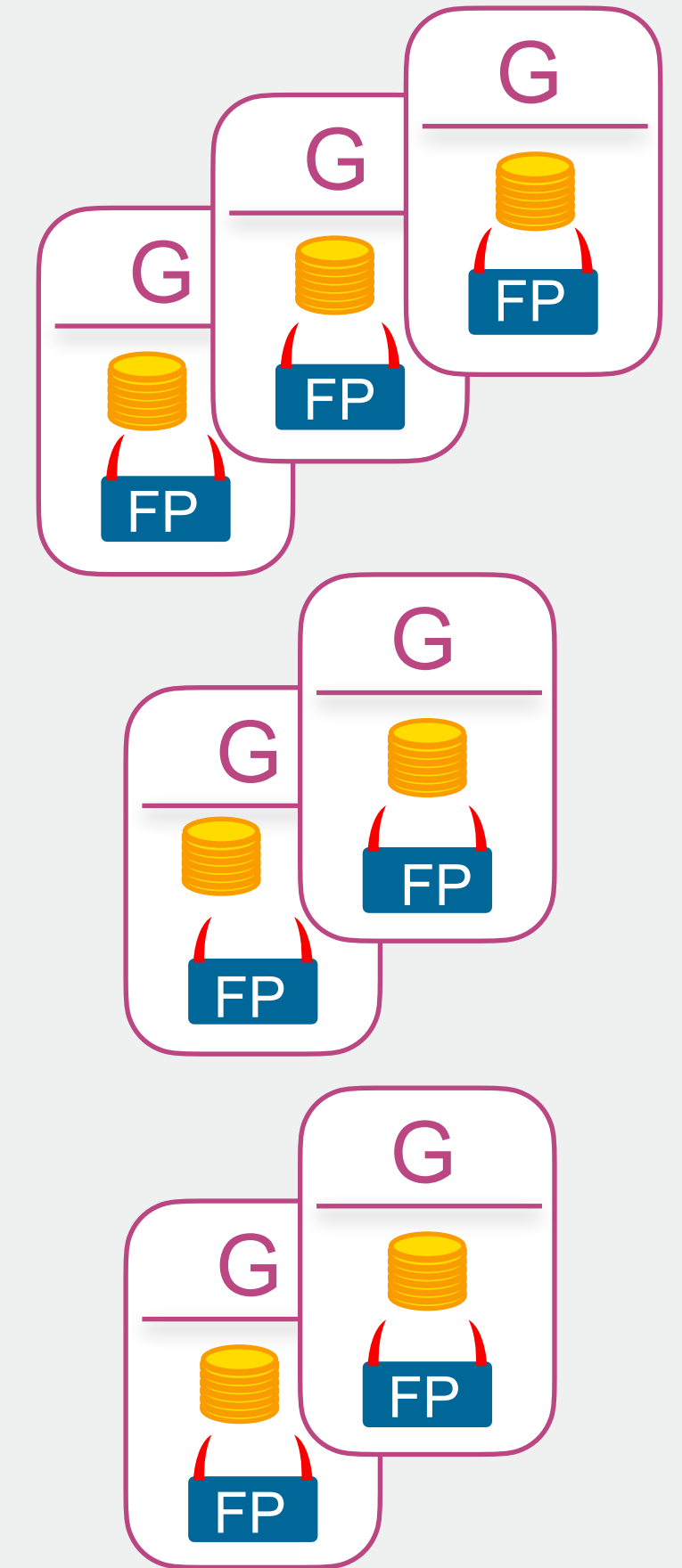
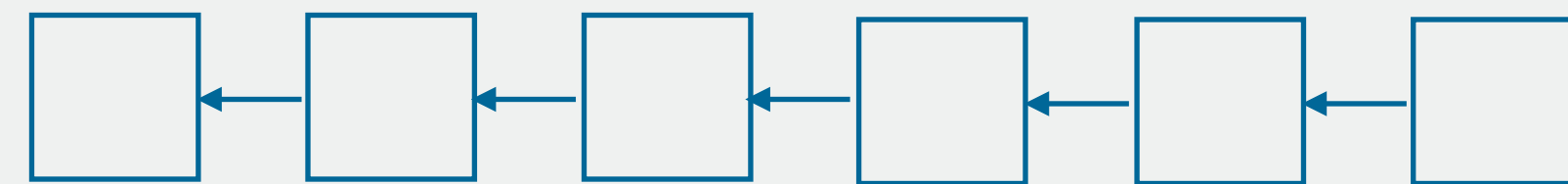
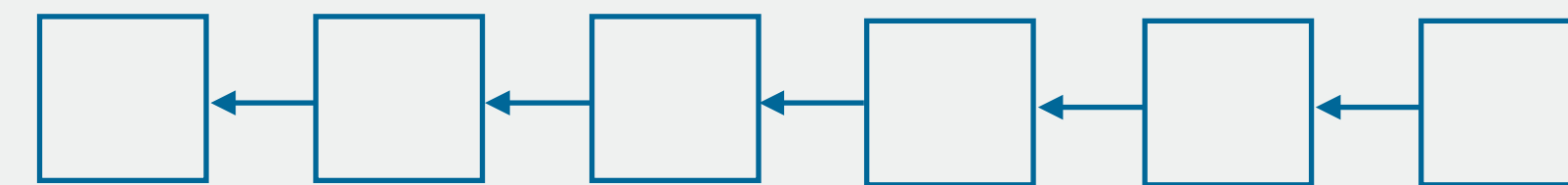
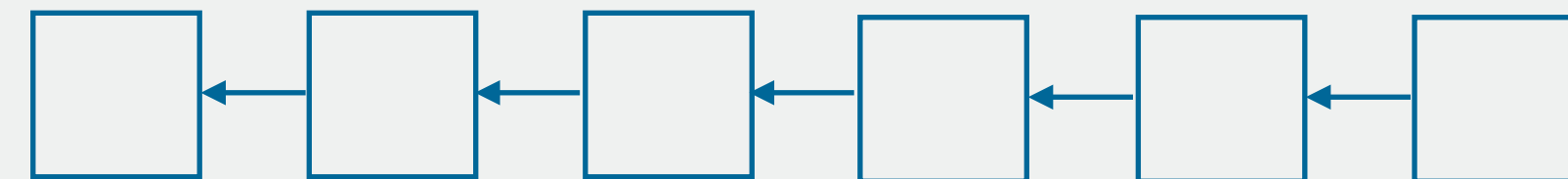
# Proof Forgery Attacks

Bribed miners produce a

**Forged Proof**



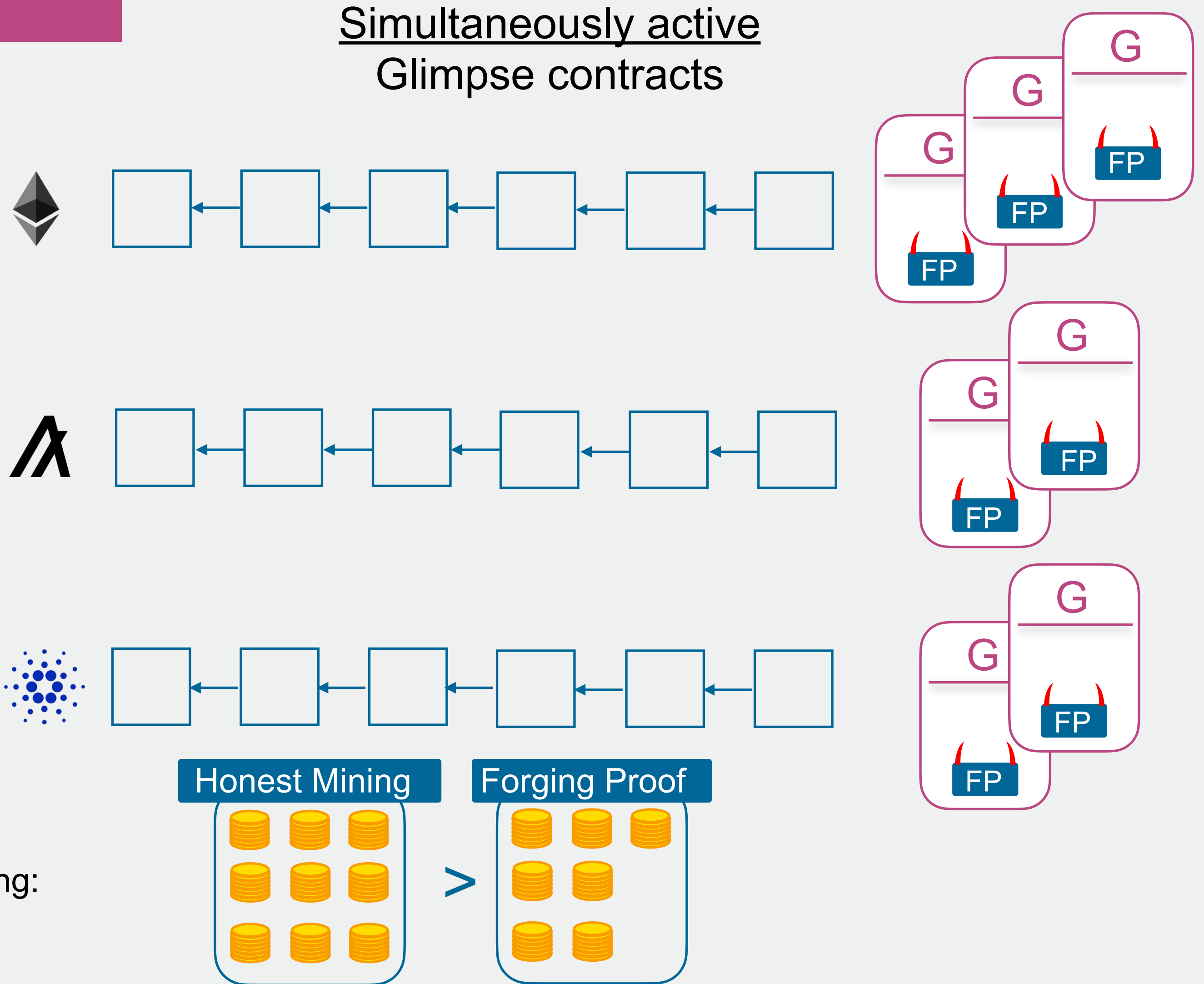
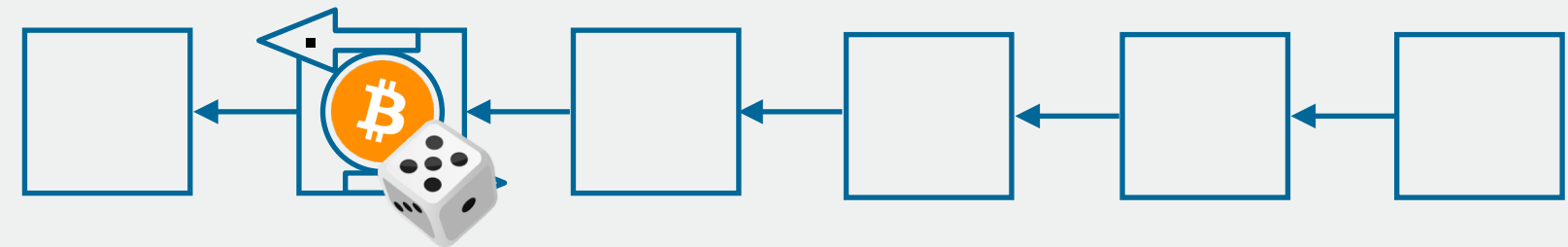
Simultaneously active  
Glimpse contracts



# Proof Forgery Attacks

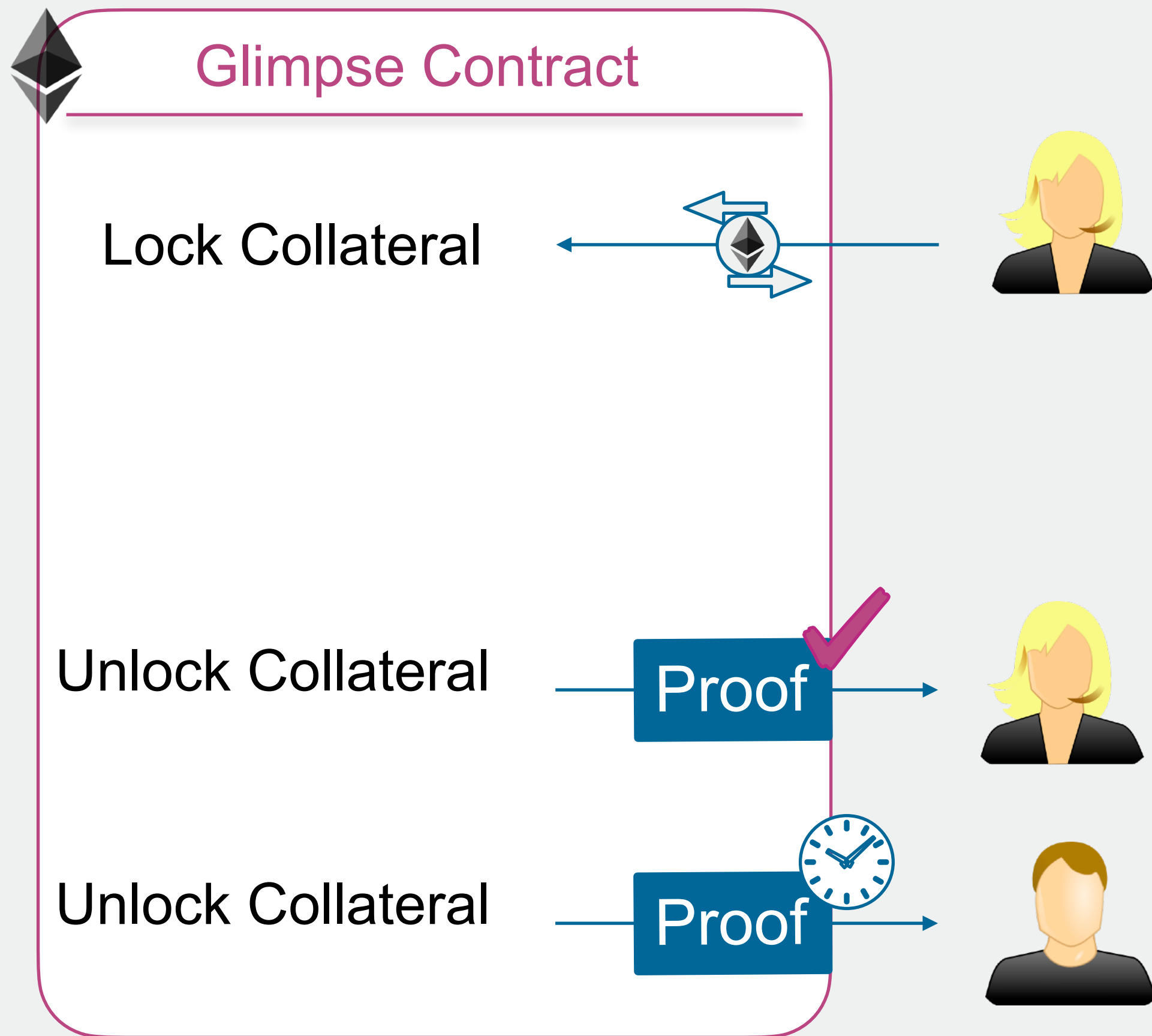
Bribed miners produce a

**Forged Proof**

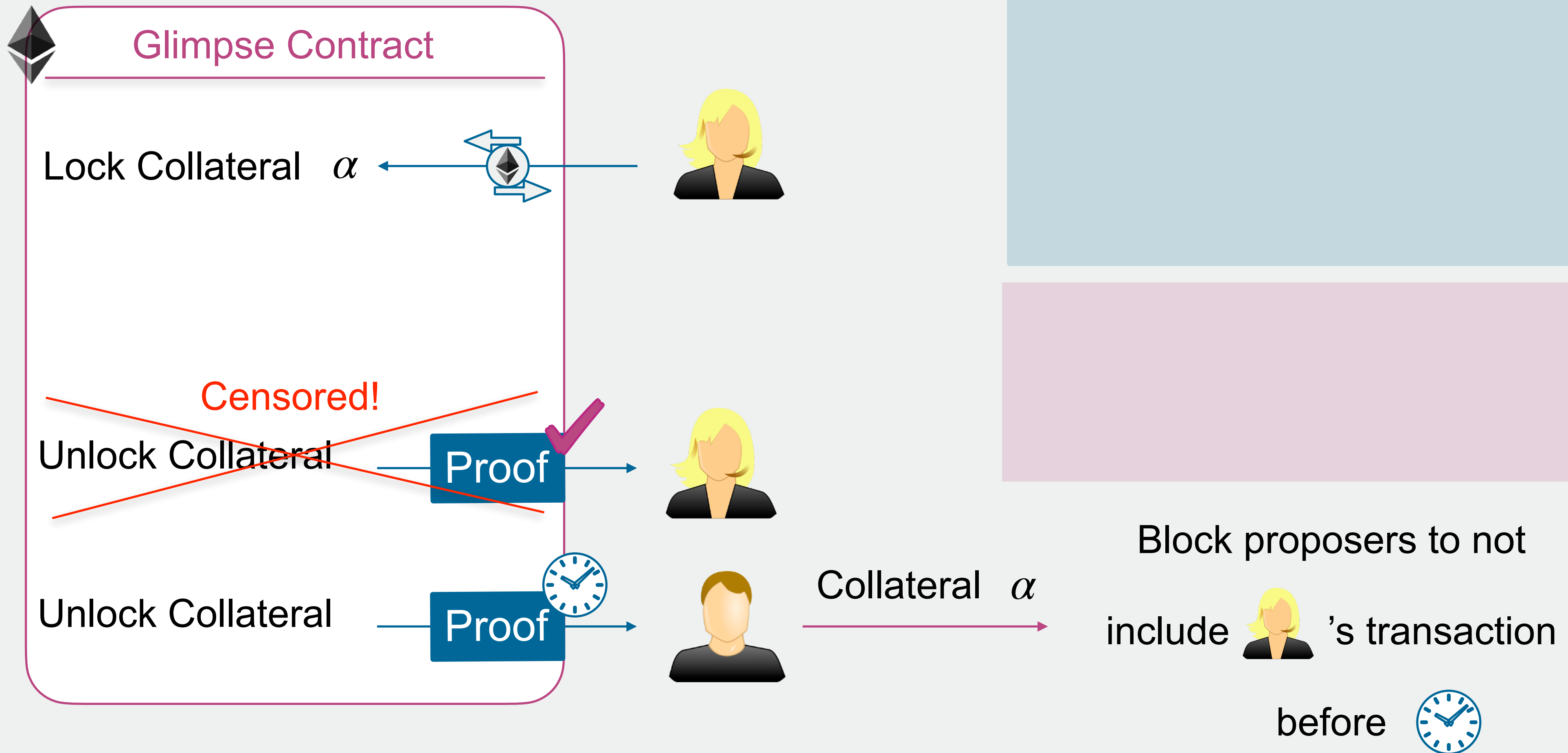


Glimpse is safe if miners' earning:

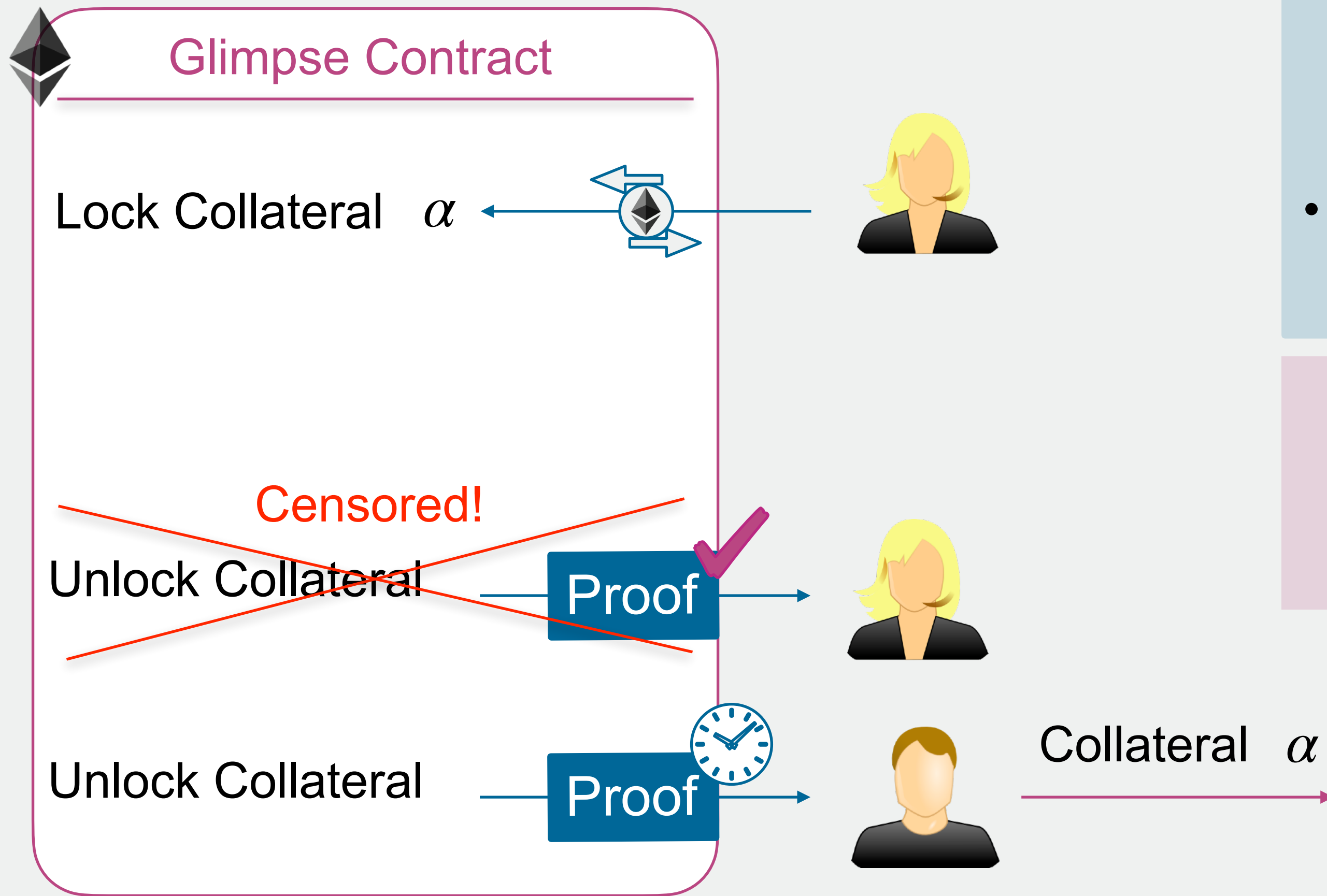
# Censorship Attacks



# Censorship Attacks



# Censorship Attacks



Glimpse is safe if :

- There is at least 1 weak block proposer

such that:  $p < \frac{f}{\alpha}$

- If  $T > \frac{\log \frac{f}{\alpha}}{\log(1 - p_w)}$

“A weak block proposer prefers having  $f$  coins now than  $\alpha > f$  coins later with little probability.”