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

PoW Source Blockchain

Glimpse

Glimpse contract

Destination Blockchain
Trustless Cross-Chain Communication
Trustless Cross-Chain Communication

Transaction Verification

Verify relayed blockchain data

Wallet  Transactions  Ethereum
Trustless Cross-Chain Communication

Transaction Verification

Verify relayed blockchain data

Atomically included: either both or none of them

Transaction Synchronisation
Glimpse: Overview

P Glimpse Contract V

Giulia Scaffino - Glimpse: On-Demand PoW Light Client with Constant-Size Storage for DeFi
“If included in , publish , upon verifying
Else, after publish .”
Glimpse: Overview

“If included in Bitcoin, publish $X$, upon verifying $\text{Proof}$. Else, after $T$ publish $Y$.”
Glimpse: Proof Construction

Merkle Root

$H$ $H$

Merkle Proof of Inclusion

$MP(\text{Proof})$

If included in $B$, publish $X$, upon verifying $MP(\text{Proof})$

Else, after $T$ publish $Y$.
Glimpse: Proof Construction

Merkle Root

H

Merkle Proof of Inclusion

MP( )

Glimpse Contract

"If included in , publish , upon verifying

Else, after publish ."

Proof
Glimpse: Proof Construction

By fully knowing $B$ upfront, can forge a proof beforehand!

"If $B$ included in $\mathcal{B}$, publish $X$, upon verifying $MP(B)$.

Else, after $T$ publish $Y$.”
Glimpse: Proof Construction

Merkle Root

\[ H \quad H \]

Merkle Proof of Inclusion

\[ MP(\cdot) \]

Glimpse Contract

"If \( \cdot \) included in, publish \( X \), upon verifying Proof \( MP(\cdot) \)

Else, after \( T \) publish \( Y \)."
Glimpse: The Contract

- Check that includes the random string
- Check that 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

\[ P \quad \text{Glimpse Contract (} d_S \text{)} \quad V \]

Giulia Scaffino - Glimpse: On-Demand PoW Light Client with Constant-Size Storage for DeFi
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

V → Loan → P

V → Collateral → P
Glimpse for Cross-Chain Lending

V → Loan → P

V → Payback Loan → P

V → Collateral → P

V → Payback Collateral → P
Glimpse for Cross-Chain Lending

Guarantee $P$ can get back collateral upon repaying the loan

Giulia Scaffino - Glimpse: On-Demand PoW Light Client with Constant-Size Storage for DeFi
Glimpse for Cross-Chain Lending

Allow arbitrary transactions in between:
Input of payback transaction unknown

Giulia Scaffino - Glimpse: On-Demand PoW Light Client with Constant-Size Storage for DeFi
Glimpse for Cross-Chain Lending

Glimpse Contract

Conditioned to payback with a placeholder as input

Lock Collateral

V

Loan

P

V

Payback Loan

P

Giulia Scaffino - Glimpse: On-Demand PoW Light Client with Constant-Size Storage for DeFi
Giulia Scaffino - Glimpse: On-Demand PoW Light Client with Constant-Size Storage for DeFi

Glimpse for Cross-Chain Lending

Glimpse Contract

Conditioned to payback with a placeholder as input

Lock Collateral

Unlock Collateral

Unlock Collateral

Payback Loan

Loan

V

P

V

P

V

P

V

P
Transaction Verification

- **Light Client**: $\mathcal{O}(|B|)$
- **Super-Light Client**: $\mathcal{O}(\log(|B|))$
- **Glimpse (On-Demand Light Client)**: $\mathcal{O}(1)$

**Relayed Data & Storage:**
- Light Client: $\mathcal{O}(|B|)$
- Super-Light Client: $\mathcal{O}(\log(|B|))$
- Glimpse: $\mathcal{O}(1)$

**Backward Compatibility:**
- Light Client: ✓
- Super-Light Client: ✗
- Glimpse: ✓

|$B|$ = Source Blockchain Length
Transaction Synchronisation

Atomic Swaps
- Only Swaps
- Any Chain

Glimpse
- Swaps, DeFi apps, DNF, Transactions w/ placeholders
- + Liquid
- + Bitcoin 
  - (OP_CAT, OP_SUBSTR)

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
Backup
Proof Forgery Attacks

Simultaneously active Glimpse contracts

Giulia Scaffino - Glimpse: On-Demand PoW Light Client with Constant-Size Storage for DeFi
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

Forged Proof

Bribed miners produce a forged proof.
Proof Forgery Attacks

Bribed miners produce a **Forged Proof**

Simultaneously active Glimpse contracts

Glimpse is safe if miners’ earning:

Honest Mining > Forging Proof
Censorship Attacks

Glimpse Contract

Lock Collateral

Unlock Collateral

Unlock Collateral

Proof

Proof
Censorship Attacks

Glimpse Contract

Lock Collateral $\alpha$

Unlock Collateral

Censored!

Unlock Collateral

Proof

Block proposers to not include person’s transaction before

Collateral $\alpha$
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.”

Block proposers to not include \( \alpha \)’s transaction before.