A Tale of Two Trees: One Writes, and Other Reads

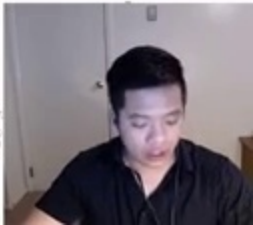
Optimized Oblivious Accesses to Bitcoin and other UTXO-based blockchains

Duc V. Le, Adil Ahmad, Mohsen Minaei, Aniket Kate (Purdue University)

Lizzy Hurtado (National University of Colombia)

Byoungyoung Lee (Seoul National University)

le52@purdue.edu, aniket@purdue.edu



https://vizle.offnote.co

Contact us: **vizle@offnote.co**

This document was generated automatically by **Vizle**

Your **Personal Video Reader Assistant**

Learn from Videos **Faster** and **Smarter**

VIZLE **PRO / BIZ**

PDF, PPT ~~Watermarks~~

- Convert *entire* videos
- *Customize* to retain all essential content
- Include Spoken *Transcripts*
- Customer support

Visit **https://vizle.offnote.co/pricing** to learn more

VIZLE **FREE PLAN**

PDF only Watermarks

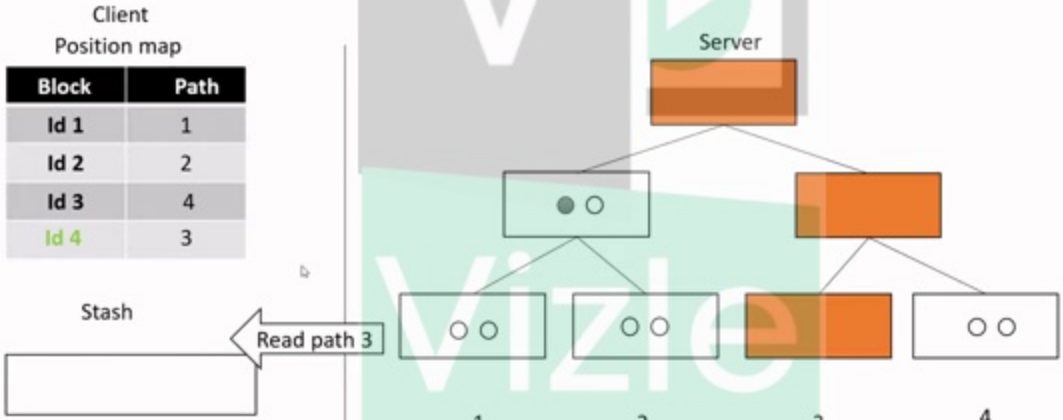
- Convert videos *partially*
- Slides may be *skipped**
- Usage restrictions
- No Customer support

Visit **https://vizle.offnote.co** to try free

Login to Vizle to unlock more slides*

Tree-based ORAM schemes

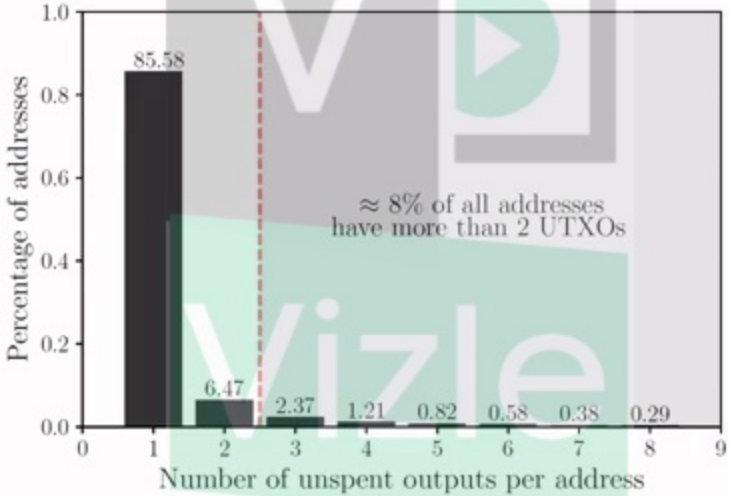
- Path-ORAM example.



Challenge 2:

- The Bitcoin network generate new Bitcoin block every 10 minute
- New Bitcoin block can generate thousands ORAM update requests.

Output/Address distribution



https://vizle.offnote.co

Contact us: **vizle@offnote.co**

This document was generated automatically by **Vizle**

Your **Personal Video Reader Assistant**

Learn from Videos **Faster** and **Smarter**

VIZLE **PRO / BIZ**

PDF, PPT ~~Watermarks~~

- Convert *entire* videos
- *Customize* to retain all essential content
- Include Spoken *Transcripts*
- Customer support

Visit **https://vizle.offnote.co/pricing** to learn more

VIZLE **FREE PLAN**

PDF only Watermarks

- Convert videos *partially*
- Slides may be *skipped**
- Usage restrictions
- No Customer support

Visit **https://vizle.offnote.co** to try free

Login to Vizle to unlock more slides*