HOFSTRA UNIVERSITY

ZeroAUDIT

Aman Luthra, James Cavanaugh, Hugo Renzzo Oclese, Rina M. Hirsch, Xiang Fu
Hofstra University


PONZI
SCHEME
How did you make the money?
Commercial Secret!

Research Question

Transactions	Portfolio			Public Info.		
	Cash	Stock1	Stock2	Units	Total	NAV
[redacted]				0	$0	$50
				10	$500	$50
				30	$1500	$50
				45	$2250	$50
				45	$2250	$50
				45	$2700	$60
				35	$2100	$60

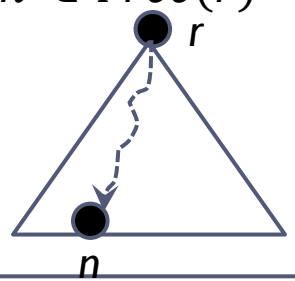
Audit Transactions But Knowing

Nothing?

Our Contributions

Zk-Membership Proof for Merkle Tree

Given C(r) and C(n):
Prove $n \in Tree(r)$



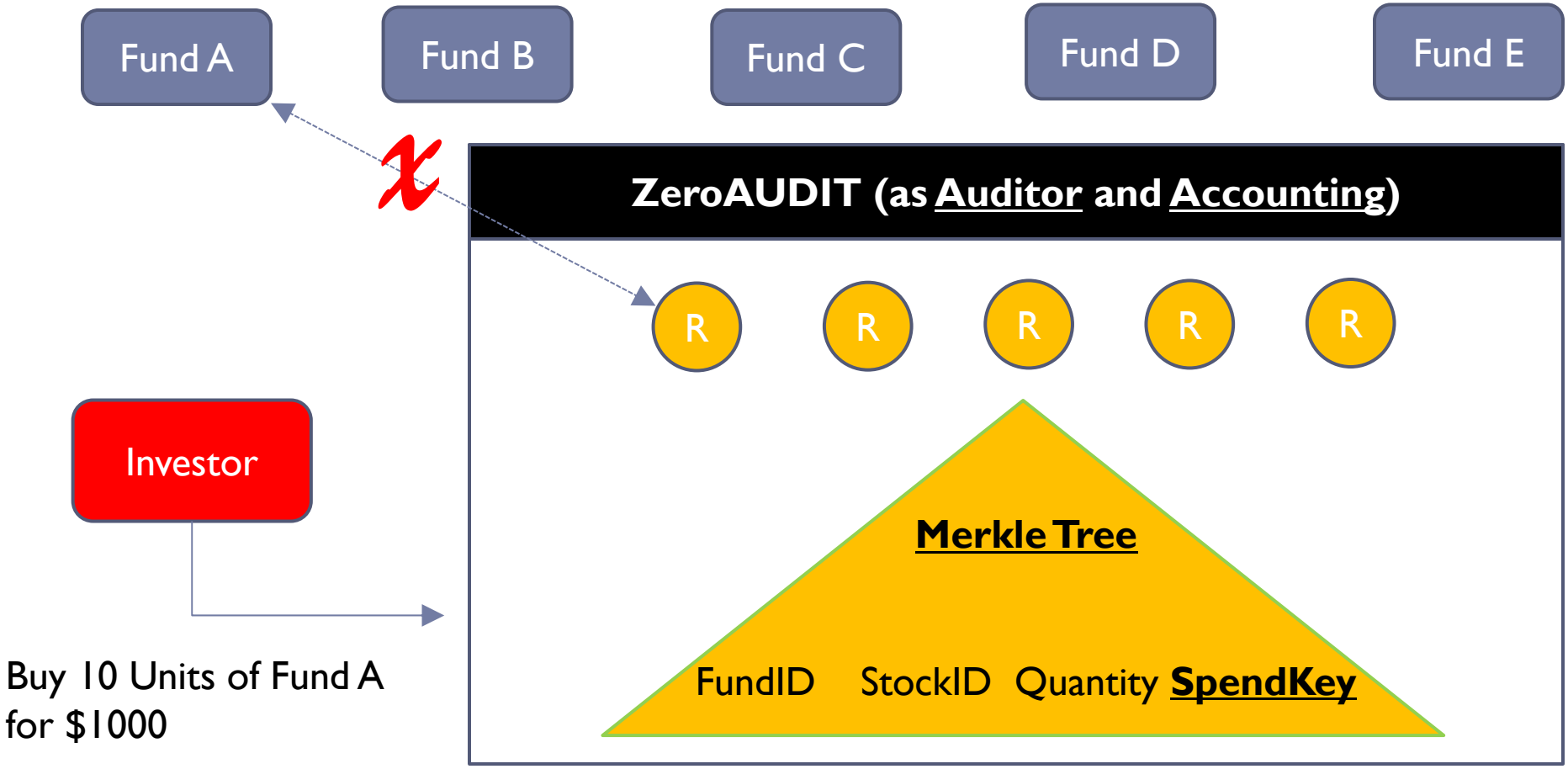
Implementation & Optimization

- 25K GO on **Fabric**
- Small Test Exponent Test
- Chained Schnorr Groups
- Pippenger's Multi-Exponent.
- Bullet Range Proof
- …

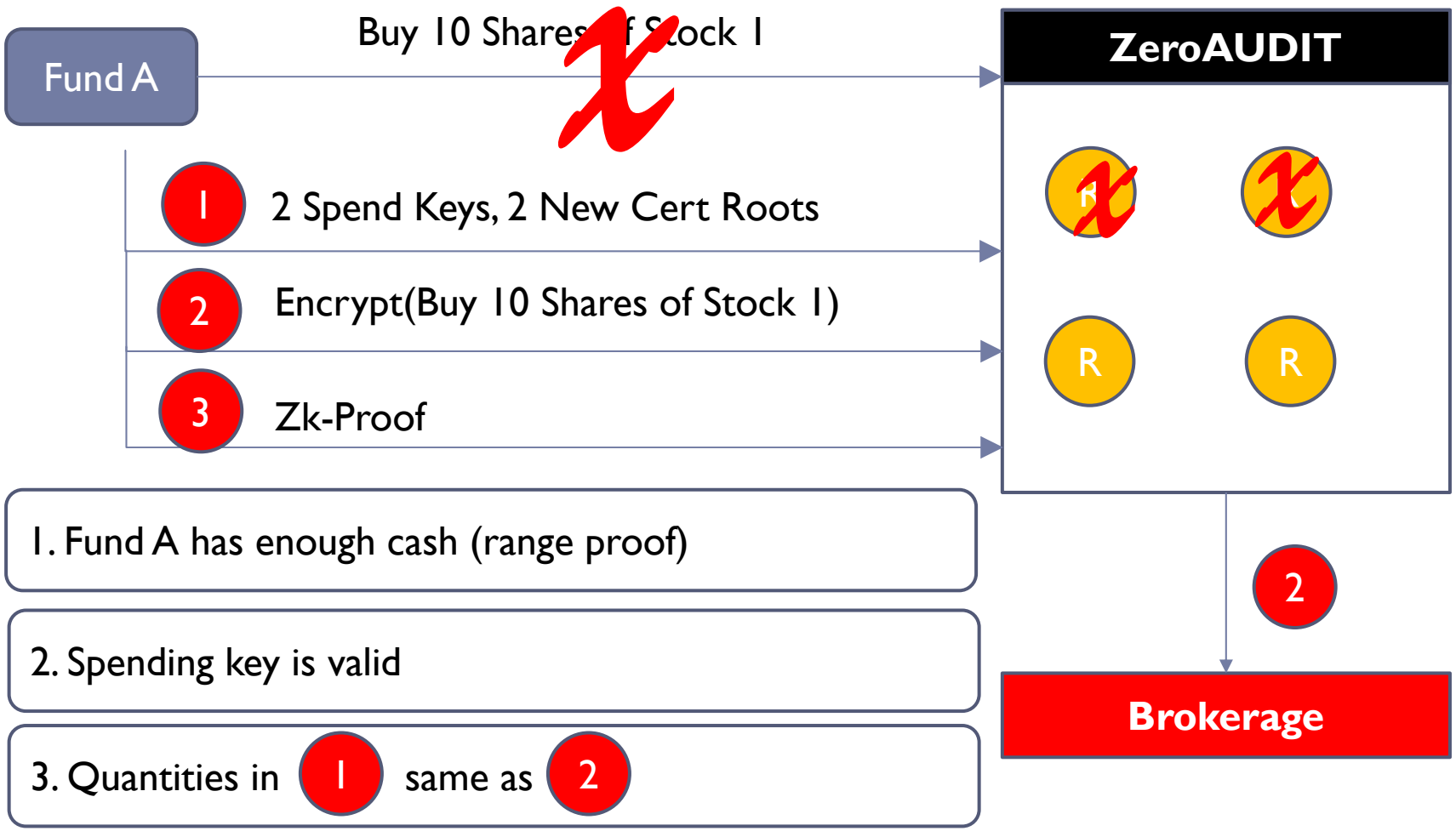
ZeroAudit Protocol

- Auditor Maintain Fund Portfolio – Work on **Commitments**
- Inspect Each Transaction at **Fair Market Price**
- Certify Net Asset Value Any Time
- **No Trusted Setup**!
  - Eq. Proof of Commits. over 2 Groups of **Different Prime Orders**
  - Using **Range Proof**

ZeroAUDIT Architecture

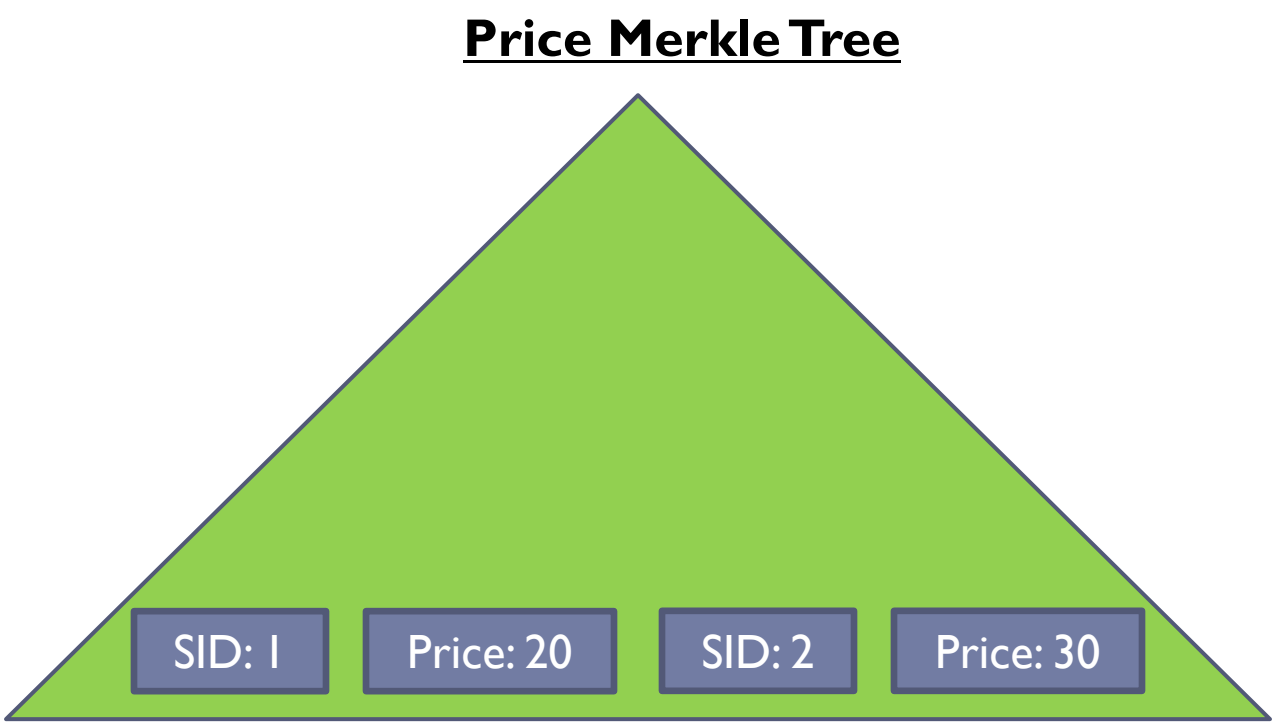


Trading Operation



Verify Fair Market Price

- Given $Commit(SID)$ and $Commit(price)$
- Prove: $(SID, price) \in Tree$

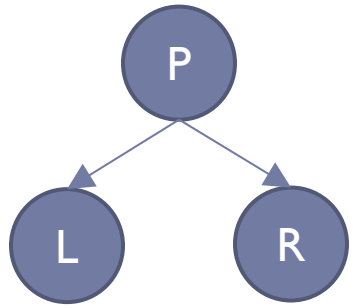


Chained Schnorr Groups

$Commit_p(P) \quad \in G_p$

$Commit_q(L) \quad \in G_q$

$Commit_q(R) \quad \in G_q$



$g_{q1}^{L} g_{q3}^{r} \; mod \; p$ $\qquad$ $g_{q2}^{L} g_{q3}^{r'} \; mod \; p$

$P = hash(L, R)$

$P = \; Commit_q(L, R)$

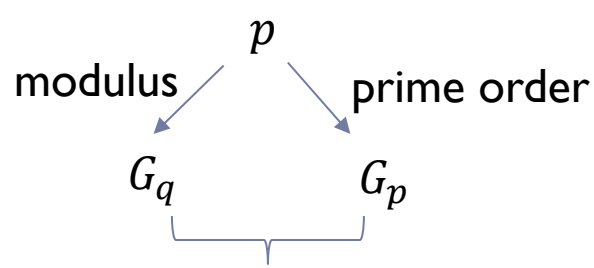
$P = g_{q1}^{L} \, g_{q2}^{R} \, g_{q3}^{r} \; mod \; p$

<u>Pedersen Commitment</u>:

2 Primes $q < p$: $G_q \; subgroup \; of \; Z_p$

2nd Larger Group

$p < r$: $G_p \; subgroup \; of \; Z_r$



<u>Chained Schnorr Groups</u>

DDLP in Child Proof

$Commit_p(P)$ $\quad P = g_{q1}^{L}\, g_{q2}^{R}\, g_{q3}^{r} \bmod p$

$Commit_q(L)$

$Commit_q(R)$ $\quad P = Commit_q(L) Commit_q(R)\, g_{q3}^{D} \bmod p$ for some D

Prover should not release D or g_{q3}^{D}

Prover can disclose $Commit_p\,(g_{q3}^{D})$

Key Observation:

$$Commit_p\,(g_{q3}^{D})^{Commit_q(L)Commit_q(R)} \triangleq Commit_p(P)$$

$$g_{p1}^{Commit_q(L)Commit_q(L)g_{q3}^{D}}\; g_{p2}^{r'}$$

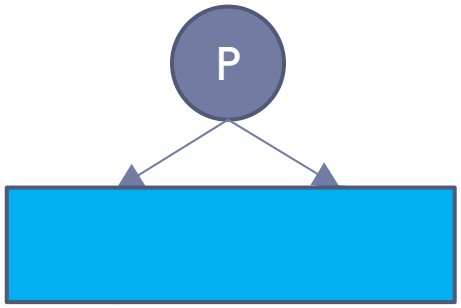
Prover knows the D
Double Discrete Logarithm Proof
(DDLP) [Stadler'97]

Complete Merkle Tree Proof

$Commit_p(P)$

$Commit_q(L)$

$Commit_q(R)$



- Disjunctive Zk-Proof
- Zk-Equality Proof Over Groups of **Different** Order
  - [Camenisch CRYPT'99] Chain Commit. on **Unknown** Order
  - Our Approach [**No Trusted Setup**]
    - **Range Proof** to Confine Values [Special Chained Schnorr Setting]
    - Challenge: Huge Range $[0, 2^{1800}]$
    - Incorporate ***Inaccurate*** Range Proof

System Implementation

- 25K Golang
- Over Hyperledger Fabric

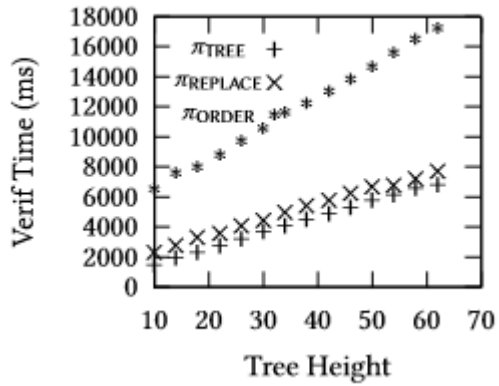
Proof	Reps	Build	Verif	Size	SmallExp	LargeExp
π_{DLP}	200	1.08	0.78	0.29	2	0
π_{DDLP}	200	561.98	48.23	76.22	189	1
π_{SAME}	200	57.43	5.75	2.08	4	1
π_{OR}	100	3614.53	59.13	494.67	91	2
π_{EDGE}	100	4241.48	111.20	557.44	259	4
π_{TREE}	1	42778.61	1597.28	5732.72	3437	87
π_{RANGE}	100	7995.79	69.65	6.24	21	18
$\pi_{REPLACE}$	1	75163.24	2640.24	10324.36	6370	111
π_{ORDER}	1	216961.74	8382.76	28726.65	18722	238
$\pi_{HOLDING}$	1	116534.11	3811.67	16091.07	8342	151

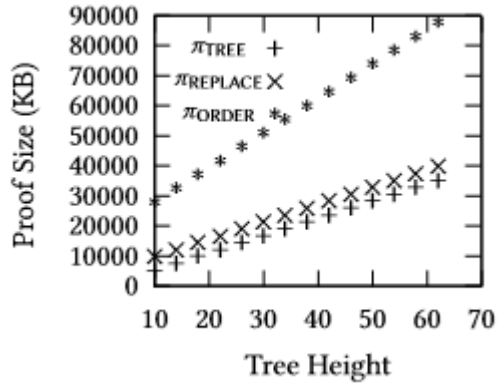
Build & Verif: Proof construction and verification time in milliseconds. SmallExp: number of small exponentiation (exp < 2ℓ). LargeExp: large exponentiation. Size: proof size in KB. Tree height settings for $\pi_{REPLACE}$, π_{ORDER}, and $\pi_{HOLDING}$: T_{RR} (11) and T^{PRICE} (16).

Table 3: Zero Knowledge Proof Cost

Operation	Verif Time (ms)	Chaincode Request (KB)
NewFund (per cert)	571	3648
Order	15443	36742
Invest	7062	16051
SetNAV (per cert)	8076	20425

Table 4: Hyperledger Fabric Client Operation Cost





Performance Data

	Trusted Setup	Assumptions	Approach	Security Strength	Anonymity Set Size	Proof Size	Proof Time (ms)	Verify Time (ms)	Verify Complexity
ZeroCoin [33]	Yes	SRSA	SRSA Accumulator[13]	128/80-bit	2^{160} [a]	45KB	–	420 [b]	$O(1)$
ZeroCash [21]	Yes	DH, KEP	zkSnark	128-bit	2^{64}	0.28KB	175000	8.5 [c]	$O(1)$
zkLedger [35]	No	DH	Columnar Update	128-bit	20	96KB	160	140 [d]	$O(n^2)$
Monero [53]	No	DLP, DH	Ring Signature LogSize Set Member. Prf	128-bit	2^{10}	1.3KB	5000	3000 [e]	$O(n)$
ZeroAUDIT	No	DLP, RO	Anony. Merkle Tree Member. Prf	112-bit	2^{15}	28MB	216961	8382 [f]	$O(\log_2 n)$

Assumptions. DLP: Discrete Logarithm; DH: Diffie-Hellman Variants; KEH: Knowledge of Exponent; RO: Random Oracle; SRSA: Strong RSA. **Verify Complexity.** the verification run-time on the anonymity set size n. –: not reported. [a] Estimate is based on 160-bit serial numbers. [b] Data is from Figure 3 (a),(b). [c] Data is from Figure 3. [d] Data is estimated from Table 1. Using k=20. [e] Data is estimated from Figure 2(a)(b) with input size 2. [f] Data is from the cost of π_{ORDER} in Table 3.

Table 5: Performance Comparison

- Extra Cost Paid for No Trusted Setup
- Proof Size Huge (Needs Improvement)

Conclusion

- ZeroAUDIT
  - Inspect Trading Transactions Without Knowing Details
- Anonymous Merkle Tree Membership Zk-Proof
  - No Trusted Setup
  - Simple Assumptions: DLP + Random Oracle
  - Log(n) Proof Size and Verification Time (n: anonymity set size)
  - Equality Proof (on Different Order Groups) Using Range Proof
- Varieties of Optimization Techniques

Questions