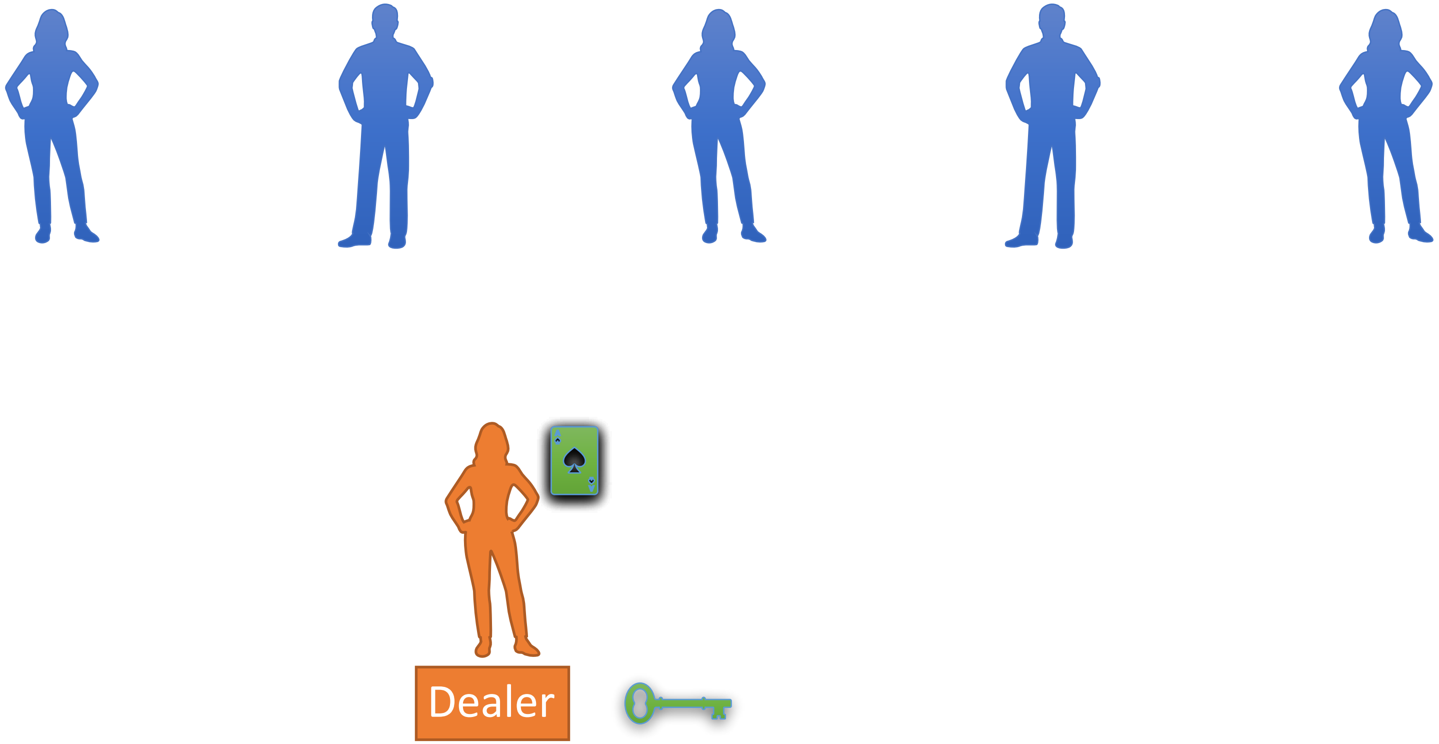
Verifiable Weighted Secret Sharing

Kareem Shehata

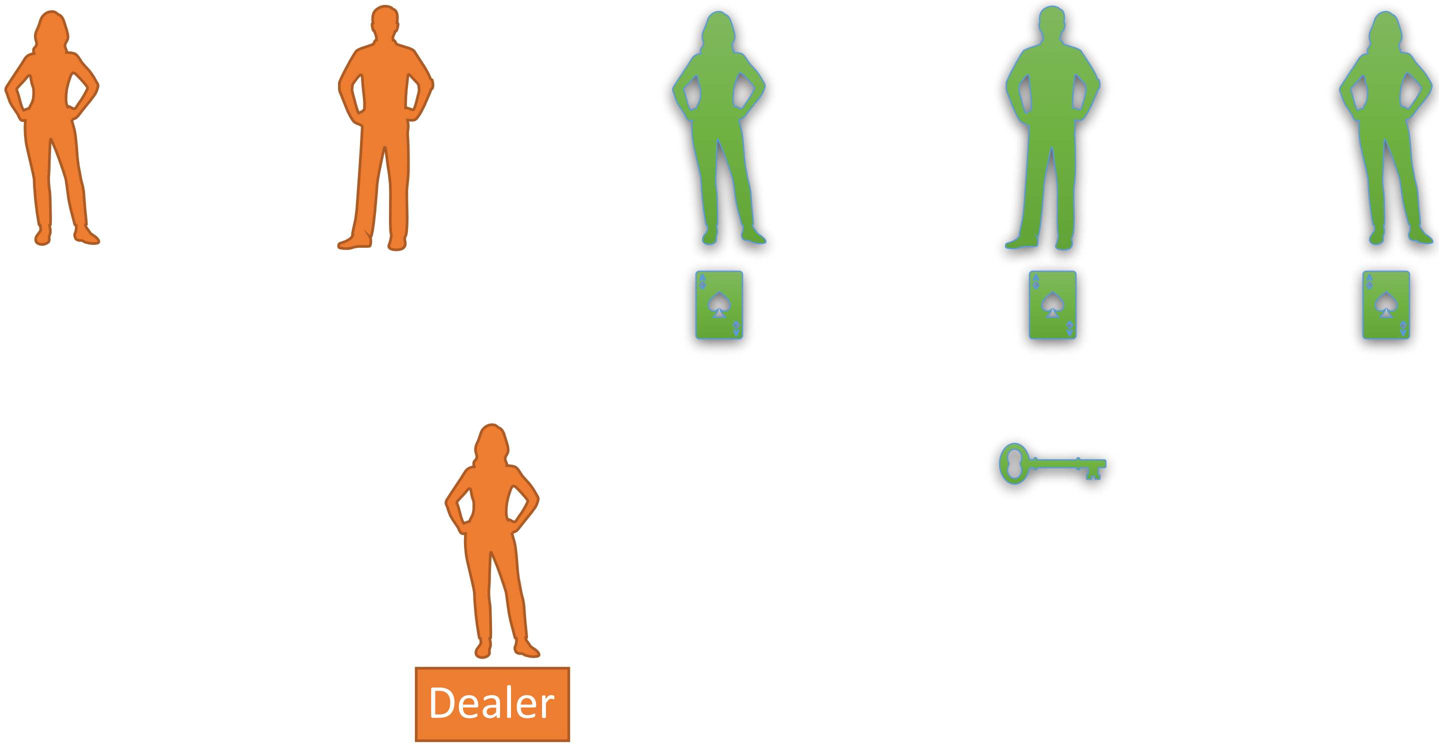
Crypto Valley Conference, 6 June 2025

Joint work with Han Fangqi, National University of Singapore
and Sri AravindaKrishnan Thyagarajan, University of Sydney

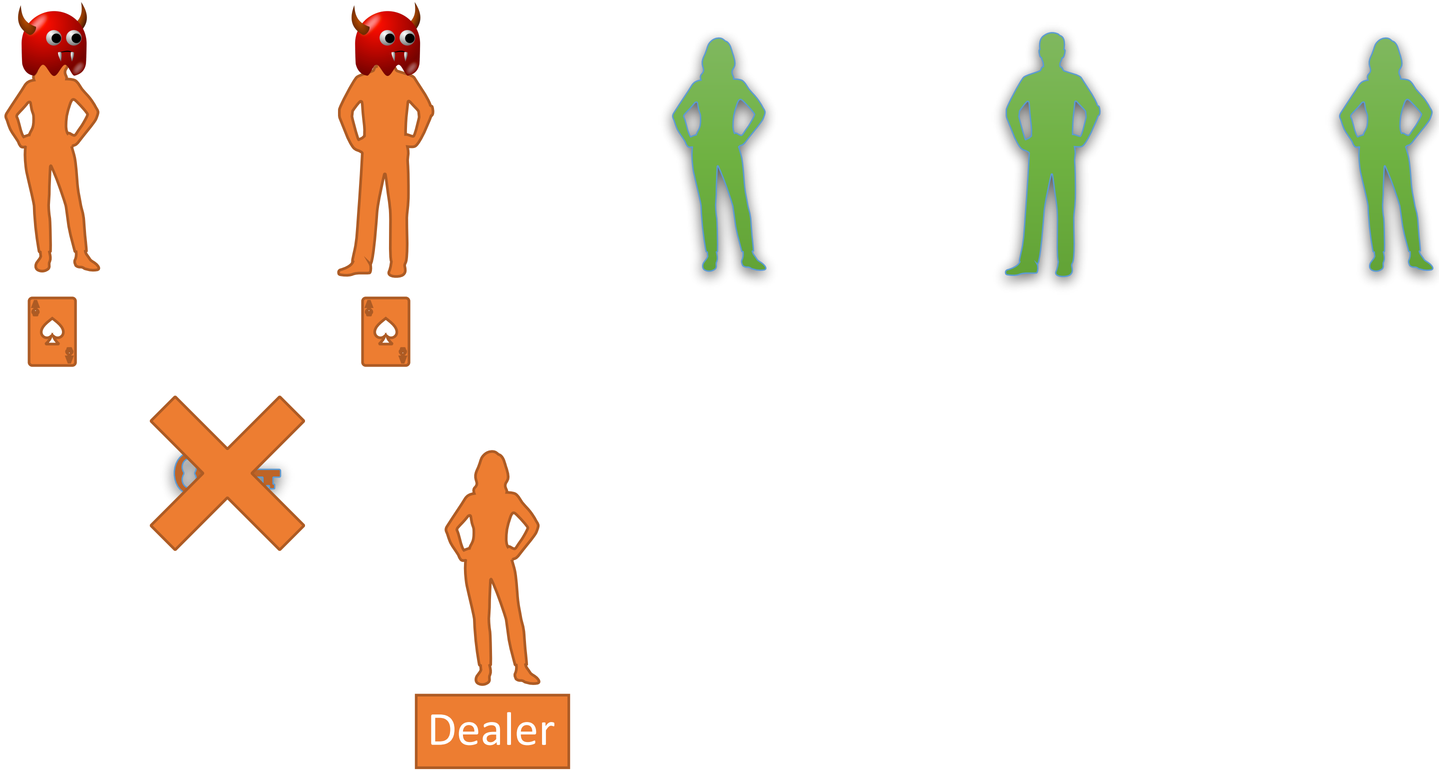
2 Secret Sharing



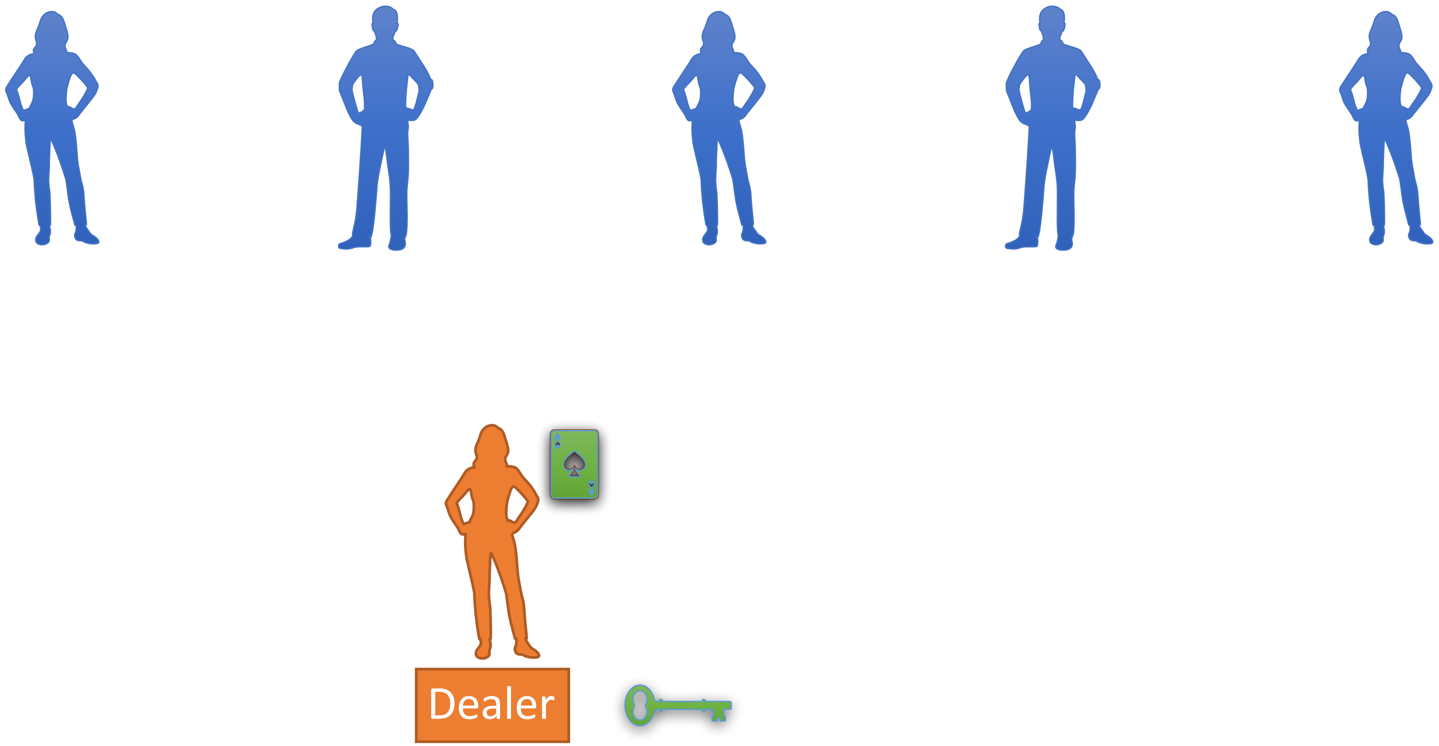
Secret Sharing



Secret Sharing Security

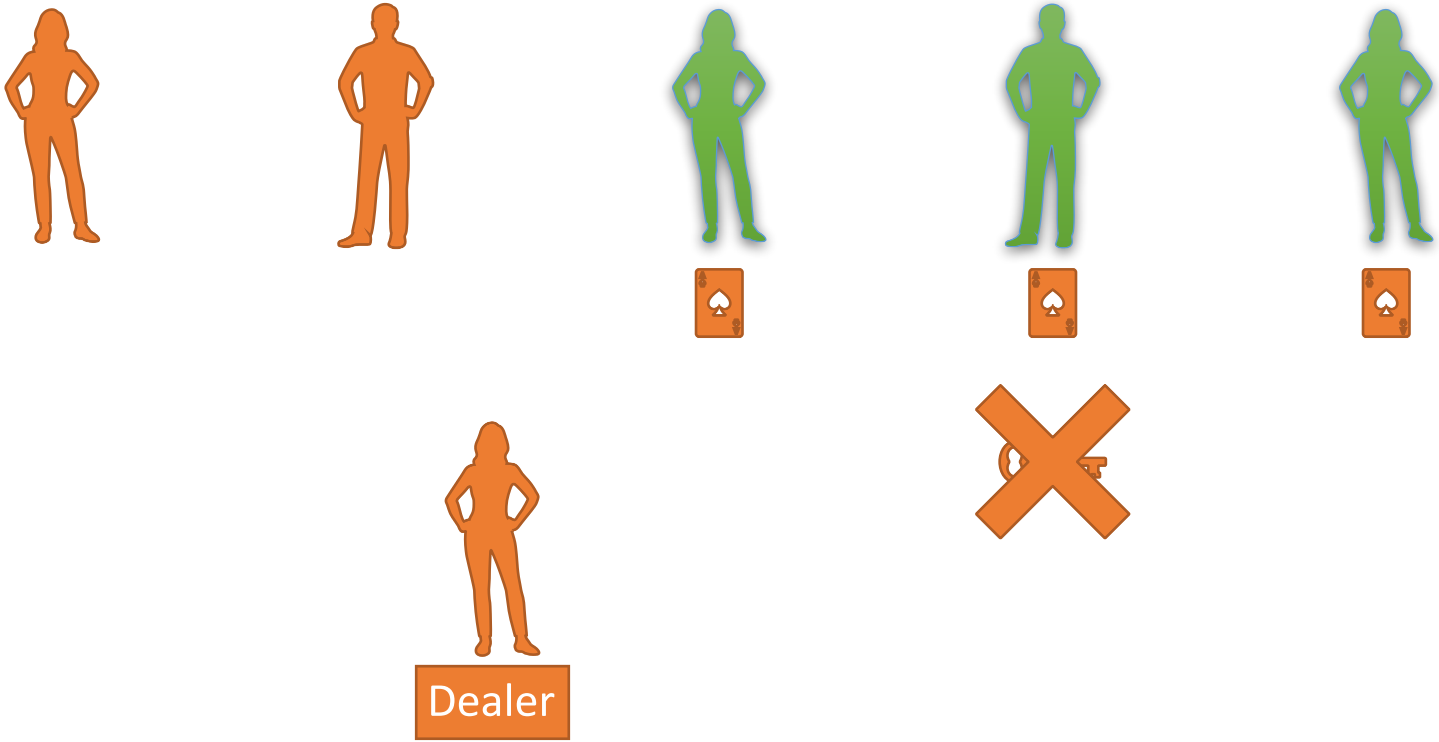


5 What about the Dealer?



6

What about the Dealer?

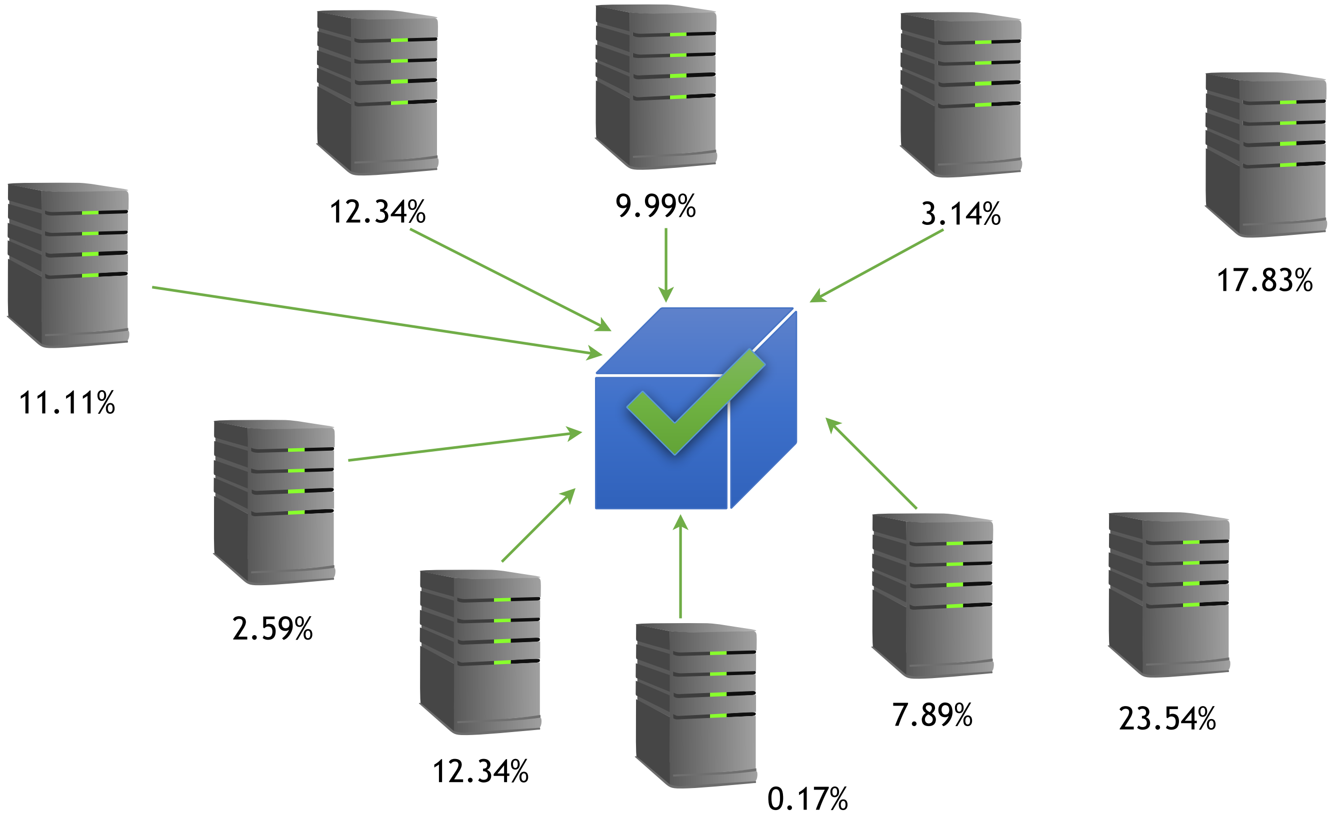


Verifiable Secret Sharing

Why care about Secret Sharing?

- Fundamental concept that underpins many other protocols
- Distributed Key Generation, Threshold Signatures, Consensus, many others…

9 Proof of Stake Blockchain



Implicit Assumption: Equal Weights

- What happens if all parties don’t have the same level of importance or “weight”?

Ethereum Stake

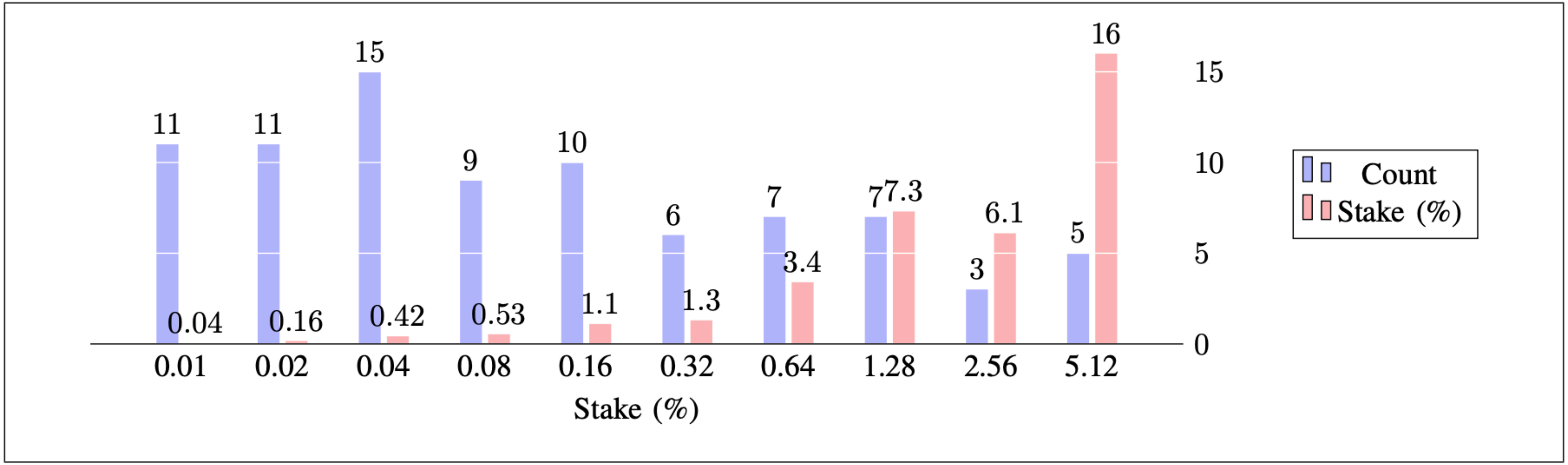
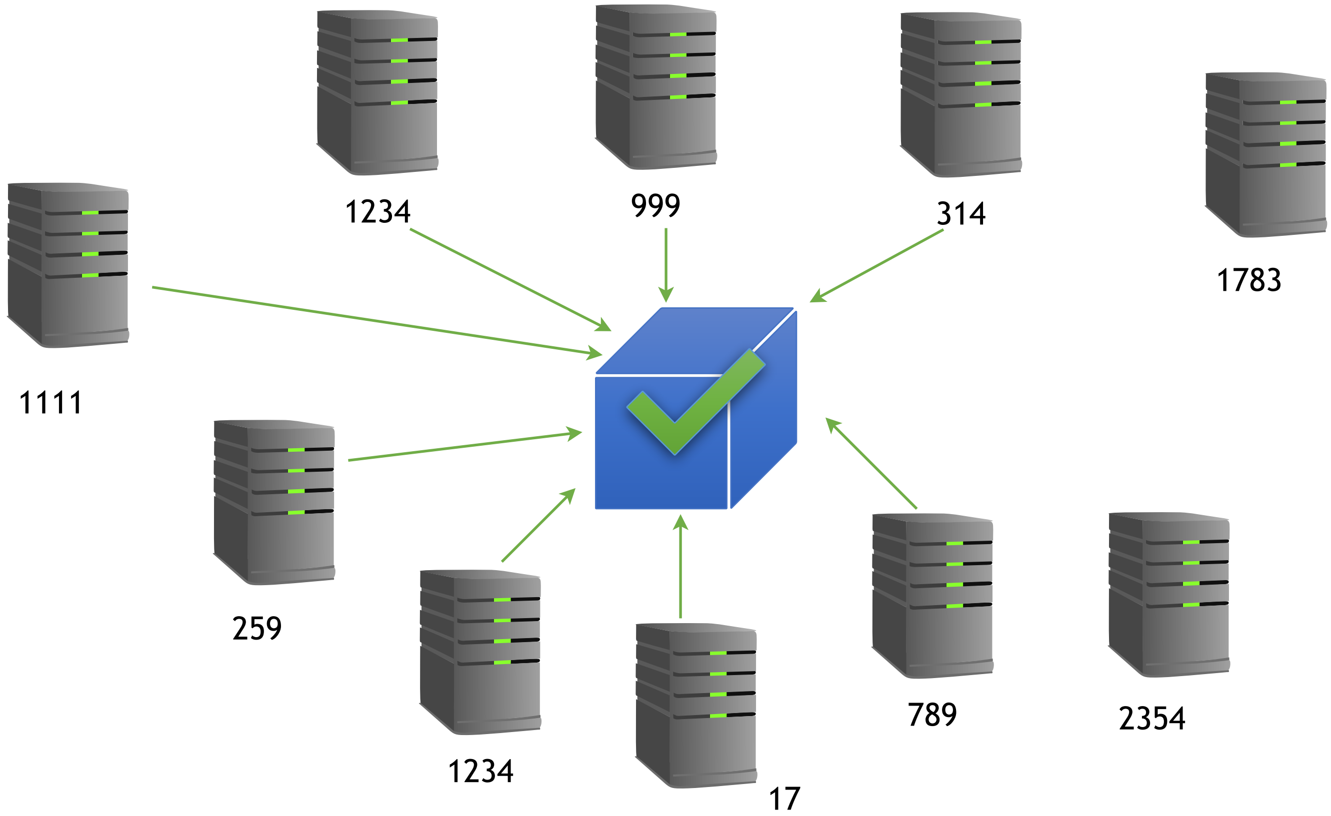


Fig. 2: Distribution of Ethereum Stakes for pools other than Lido and Coinbase. Note that the x-axis is logarithmic.

Virtualisation

- Naïve solution: give parties with more weight more shares.
- Convert all weights to integers, give each party a number of shares equal to their weight.
- Very inefficient: have to do communication and computation that grows with at least $\mathcal{O}(w)$!

13 "Virtualized Shares"



14 Linear vs CRT Secret Sharing

- Linear (SSS):
  - Equal Weights
  - Easy and flexible
  - Verifiable constructions
  - Single group
- CRT (non-linear):
  - Weighted constructions
  - Non-linearity makes it more difficult to work with
  - No verifiable constructions with a single group

Chinese Remainder Theorem

Let $p_1, \ldots, p_n$ be arbitrary integers, all co-prime

Chinese Remainder Theorem:

Given $a_1, \ldots, a_n, a_i \in [p_i]$,

The system of equations $\{a_i = a \mod p_i\}$

Has a unique solution $a \in [0, p_1 \cdots p_n]$

CRT-Based Secret Sharing

- Uses Chinese Remainder Theorem instead of polynomials
- Divisor p_i determines "weight"
- Non-linear, only known verifiable version requires strong RSA assumption and unknown order groups, not good for blockchain.

17 CRT Deal Proof

To prove a correct deal starting from a secret s to a share s_i with “weight” value p_i, we just need to prove that:

$$s_i = s + kp_i$$

For some $k < p_i$,

Why not R1CS / Bulletproofs?

- We can easily prove $s_i = s + kp_i$ using R1CS proofs
- … but only if all the values live in one group.
- For the security of any practical system, we'll want the base secret to be in the group, and the rest of the values much *much* larger than the group.

19 Problems with Cyclic Groups

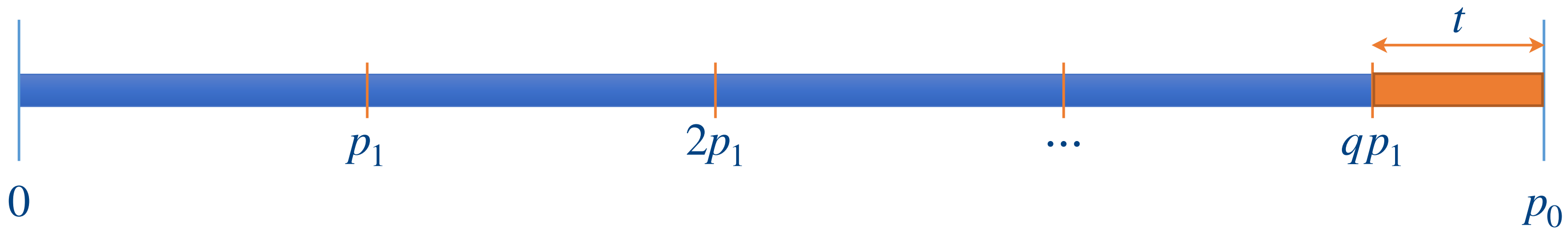
If we use the same cyclic group for commitments as the desired crypto system, then:

1. $s = s_0 + up_0 = s_0 \mod p_0$
2. Can *always* find k' such that $s = s_i + k'p_i \mod p_0$ for any s, s_i!

Either we need to use another, much larger group (previous solutions), change our setup, or be a lot more clever.

Wraparound $\mod p_0$

Let $p_0 = qp_1 + t, 0 \le t < p_1$



If $a = b + kp_1$, and $a < p_0$ then, either:

- $k < q$ and b can be any value in p_1, OR
- $k = q$ and $b < t$

21

“Proof of Mod” $b = a \mod p_1, a, b \in \mathbb{Z}_p$

Prover has a, b, sends verifier $A = \text{Com}(a; r_a), B = \text{Com}(b; r_b)$

Let $p_0 = qp_1 + t$, where $0 \leq t < p_1$

1. Prover sends $V = \text{Com}(k; r_k)$
2. Prover sends proof that $b + kp_1 = a \mod p_0$
3. Use disjunctive proof strategy on following statements:
   A. $(0 \leq k < q) \land (0 \leq b < p_1)$ OR
   B. $(0 \leq k \leq q) \land (0 \leq b < t)$

Both A and B above are just range proofs, can use Bulletproofs or others

With these in place, have a proof-of-mod, since $b + kp_1 < p_0$

22

Proof of mod for values $< p_0^2$

Intuitive idea: use the "proof of mod" several times in a row to progressively bring things in range to show:

$$s_1 = s_0 + ap_0 \mod p_1$$

$$\Downarrow$$

$$s_1 = (s_0 \mod p_1) + (a \mod p_1) \cdot (p_0 \mod p_1) \mod p_1$$

CRT-VSS using a single DL group

If $p_i << p_0$ and $p_0 < P_{max} << p_0^m < P_{min}$

Then the dealer can:

1. Distribute shares as in CRT-SS
2. Provide commitments to all shares
3. Use the expanded proof-of-mod to prove correct dealing for each share

CRT-VSS using a single DL group

Participants:

1. Check that shares match commitments
2. Verify the proof-of-mod for all shares

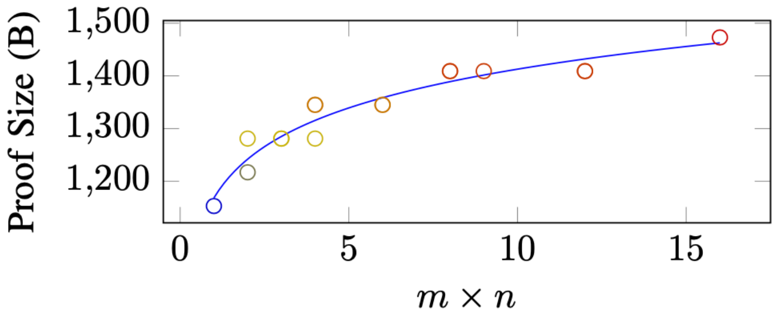
25 Performance Improvement of WR-VSS

- 100x improvement in broadcast bw on current implementation
- 20x improvement in broadcast bw vs virtualized VSS
- 5x improvement in private bw vs virtualised VSS

Design	Broadcast			Private	
	$\mathbb{G}$	$\mathbb{Z}_{p_0}$	Total (B)	$\mathbb{Z}_{p_0}$	Total (B)
Current	$28,000$		$1,344,000$		
Feldman	$6,850$		$219,200$	$4,110$	$131,520$
WR VSS	389	6	$12,640$	~ 892	$28,528$

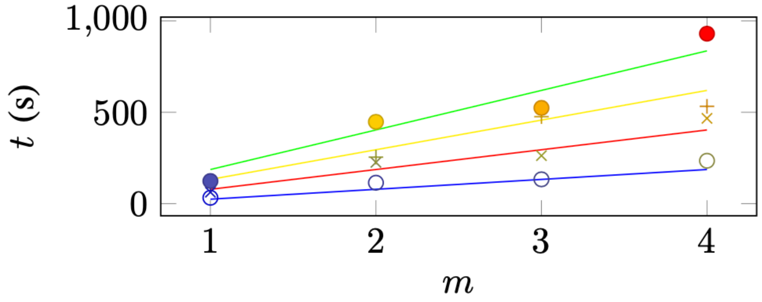
26 Proof Size and Running Time

Proof Size

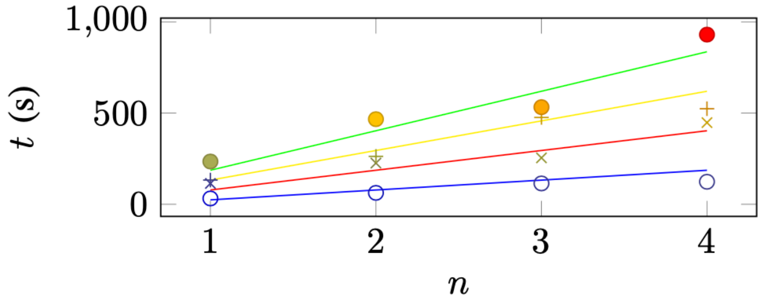


(c)

Running Time

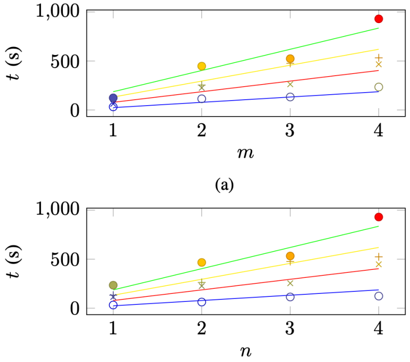


(a)

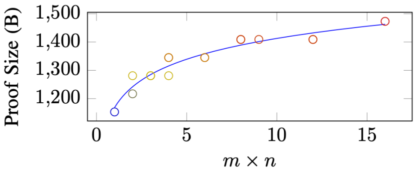


Summary

- Shown how to construct the first verifiable and weighted secret sharing scheme that uses only a single discrete-log group.
- WR-VSS produces much smaller proofs than using even the simplest non-weighted VSS.
- But current R1CS proof systems have high overhead in proving time, not yet practical for use.

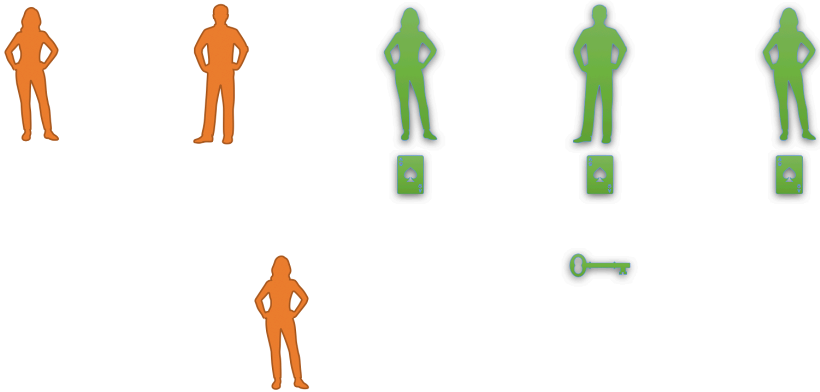


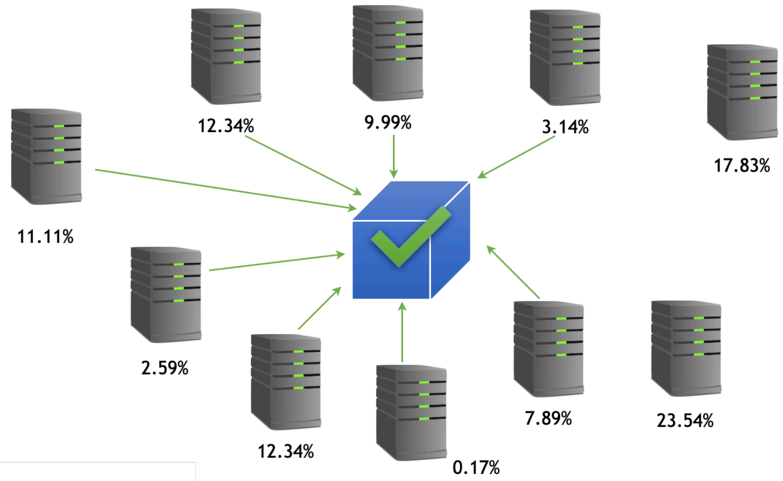
Running Time



(c)

Proof Size





Questions?

Let $p_0 = qp_1 + t, 0 \leq t < p_1$