Lecture 16

Scaling

Today)

↳ Finish PoS.

↳ Scaling

PoS

$$H(\text{randSource}, pk, t) < T \times \text{stake}(pk)$$

randSource updated periodically.

↳ Require consensus randSource

$\text{VRFEval}(\text{randSource}, t, sk)$

(y, π) ↳ proof.

$\text{VRFVerify}(y, \pi, \text{randSource}, t, pk)$

↳ {True, False}.

s-truncated LC.

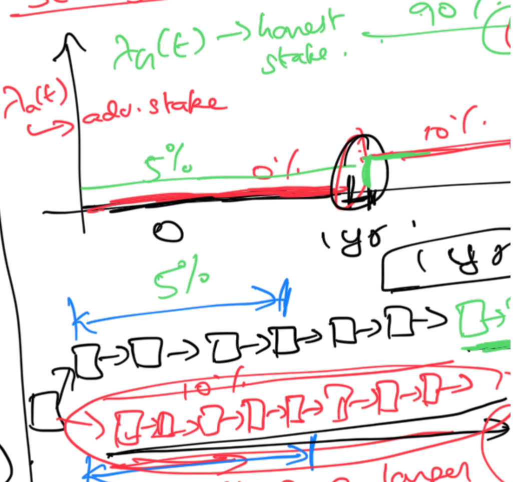
Props

CONS:

(i) Leadership slot is self-predictable

(ii) Not fully dynamic all availab

Setting



creating a longer chain is cost-free.

Long range attack

PoSAT (Proof-of-Stake with Arrow-of-Time).

Verifiable Delay Functions. (VDF).

↳ Mechanism to certify the passage of tim

x → input.

Want
Calculate $H^l(x) = H(H(H(\cdots H(x)))$

↳ Sequentially calculate hashes.

<u>Key idea:</u> Not parallelizable.

'T' time to compute hash ⟹ Tl time to compute H^l.

Not easy to verify $H^l(x) = y$.

[Verification and computation take same time]

Cryptographic mechanisms to create a short proof that $H^l(x) = y$.

VDF Prove & VDF Verify.

$\Downarrow$ prover
↳ $H^l(x)$ and a proof

$\Downarrow$ Verifier.
↳ (Verify quickly $H^l(x) = y$ using proof)

$H(\text{randSource}, pk, \underline{t}) < fn.\ Stake(pk)$

random ↦ $\boxed{H^L(\text{rand Source}, pk) < fn.\ Stake(pk) \Rightarrow LC}$

[Ignore verifier complexity.]

↳ can be dealt using VDF.

is available is

the time at which

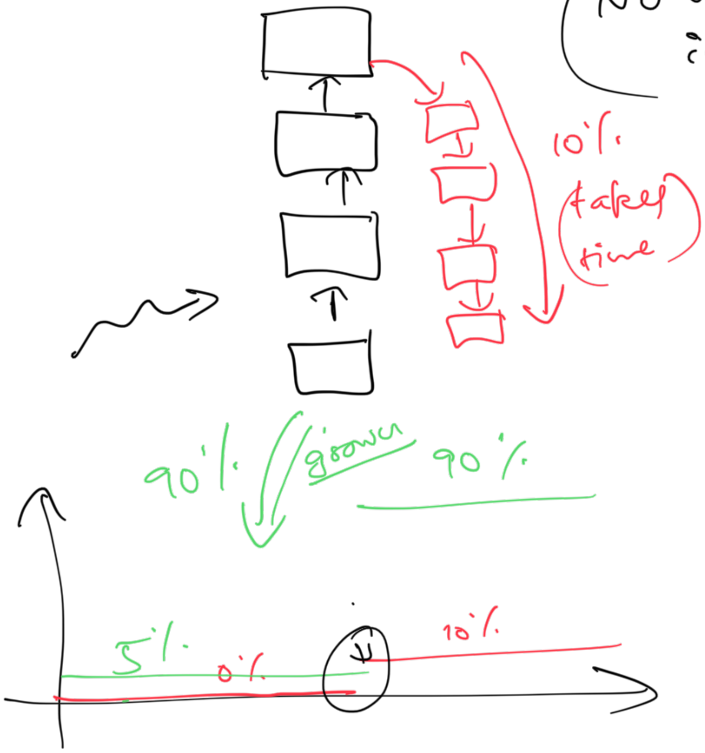
unpredictable even by yourself

Earlier : Rand Source → fixed at genesis.

Now : Rand Source ⟹ H^L(randsource, pk) in the previous block. LC.

↓ comes from prev block.

(No notion of time in the protocol

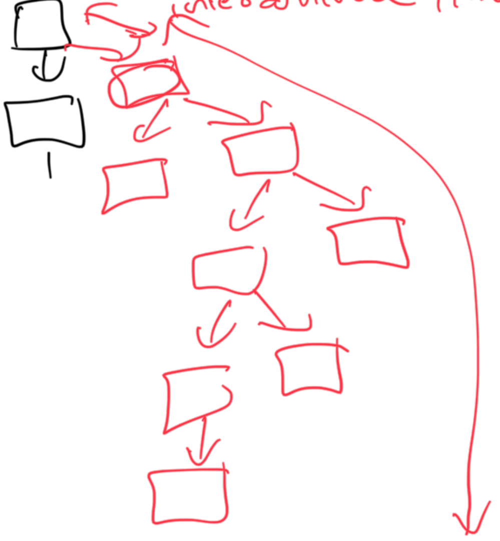


Assumption $H^L(.)$ takes same amount of time for all nodes.

↳ Rate of seq work is same across all nodes

[No benefit of parallelism].

Nothing at attack
stake



interarrival time = 1.

T tim

⇒ LC ?

Branching random walks ⇒

without attack, LC → ~T

with attack, LC → ~$\underline{e}$T

≈ 2.7

Secure as long as $\boxed{\lambda_h^{(t)} > \underline{e}\, \lambda_a^{(t)} \quad \forall}$

$\underline{e} \xrightarrow{?} 1$

c-correlation ⇒ $\begin{cases} \lambda_h^{(t)} > \phi_c \, \lambda_a(t) \\ \phi_c \to 1 \text{ as } c \to \infty \end{cases}$