money heist

ertosns

2023/5/5

1 leader election

1.1 democratized random lottery seed

randomness η_i in the y variable in the leader election comparison, is the output of VRF.

$$\eta_i = VRF(\eta_{i-1}||slot_{id}, coin_{sk})$$

which is publicly verifiable through $verify(\eta_{i-1}||slot_{id}, coin_{pk})$, where $coin_{pk}$ is constrained as public input, and keypair $(coin_{sk}, coin_{pk})$ is protected against grinding attack by published nullifier in the same contract, has advantage over ouroboros, which reduce the grinding effect through multiple queries for the random oracle for favoring high probability of winning by limiting the number of queries to the random oracle. [1]

1.2 grinding η, and delayed stake contract

although randomness from the lead stakeholder provider is decentralized, doesn't reveal identity of the provider, more robust than limited access global random oracle, it's deterministic, predictable, meaning, even with time-locked contracts (see 4), there is a window between un-stake, and stake contracts, or for new adversarial stakeholder, it's possible to target winning at $slot_{id}$, by trying different key pairs, and picking secret key corresponding with lowest y possible. that attack can be prevented by delaying reward proposals from newly staked coins by N slots, N be at least 1, N being a security parameter.

1.3 omerta attack

although selecting key pairs corresponding of η with lowest corresponding y using public on-chain data is fixed, it's still possible to make off-chain agreements, for example at slot i if the contract execution is delayed N slots, it's possible through N agreements with winners of slots i to $i+N$, and since calculation of η is predictable, it's possible to pick elect key pair corresponding to lowest y at slot i+N+1 in the future, early at i slot. note that the off-chain agreement is

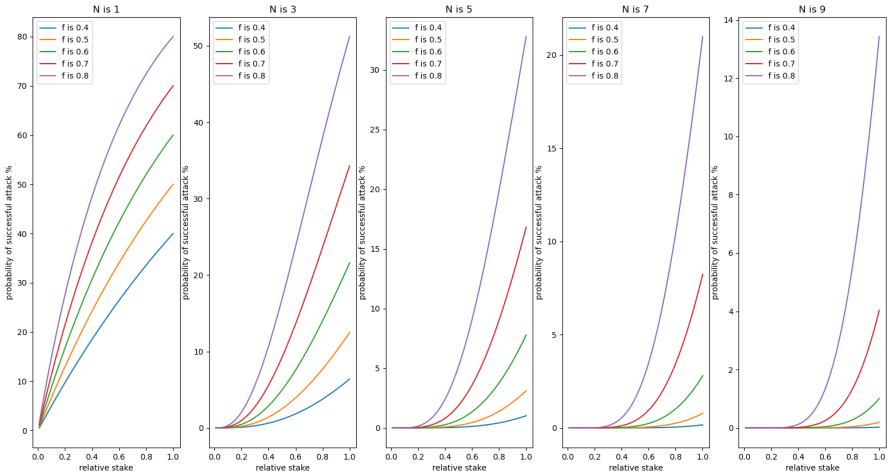

Figure 1: probability of attack for different security parameter

done with probabilistic winners, but once this attack is done once (even if possible with low probability), the adversaries will have high leverage on winning, by mining lowest possible y.

the attack can be fixed, by introducing unpredictable random parameter:

$$\eta_i = VRF(\eta_{i-1}||hash(block_{i-2})||slot_i, sk)$$

note! secret key is constrained 1 slot ahead (assume $N = 1$ for simplicity), and grinding isn't possible since the staked coin is restricted from reward proposals for 1 slot, and η_{i-1} isn't known yet, omerta attack isn't possible since $hash(block_{i-2})$) isn't known ahead of time.

1.4 perpetual lead with predictable block hash

slots are divided into N+2 cycles, (N is security parameter $N \geq 1$), adversary assume winning lottery in the consecutive slots i to i+N, with certain probability, then winning leadership at slot i+N+1 becomes highly probable, only the first block at slot i include a single stake transaction (note staked DRK execution is delayed to slot i+N+1), rest of blocks i+1 to i+N are left with empty transactions, then predicting η_i to η_{i+N+1} is possible, and thus grinding attack can be executed.

if we plot that probability of successful attack, for N (security parameter) delayed slots, function of relative stake (see figure 1), from graph we note that even with 100

1.5 conclusion

the omerta attack with perpetual lead is of diminishing probability of success for security parameter $N \geq 9$.

2 chain fork

fork can occur when multiple stakeholders publish proposal for valid proof of leadership. winning stakeholder can choose to fork with a new block, extend a chain, or extend chanonical longest chain.

2.1 fork finalization

finalization is a compound of longest chain, and single leadership frequency, at the end of any slot, finalization, and re-syncing happen when there is single leader per slot, single leader frequency is controller with secondary discrete PID controller in cascade control. such mechanism is resilient to bribery attack [2], and NAS attack (when the stakeholder write a transaction in one chain, and rewrite the transaction in parallel chain of equivalent stake, and equal fork depth, using relatively small stake) since probability of winning leadership with single leader frequency at small stake at more than one slot during the fork depth is of diminishing probability.

2.2 finalization degree of freedom

it's possible for single lead stakeholder at the end of a fork to honor certain fork chain based off off-chain agreement, or if the stake stakeholder leads another block in the fork.

2.3 deterministic finalization

if there are multiple chain fork, stakeholder execute rank(blocks), and extend the highest order chain. rank perform comparison of block hash modulo

$$concatenate(\eta_{-1}^{canonical}|| \dots ||\eta_{-1-K}^{canonical})$$

, note that $\eta_{-i}^{canonical}$ means eta at canonical chain at index i from last, k is a security parameter. note that blocks of same hash is of diminishing probability, but in such case, the stakeholder can choose either of which if there is such collision between highest ranks.

3 time frequency

blockchain lifetime is series of epochs

3.1 epoch

multiple slots during which the reward value is fixed, and set by primary controller in the cascade control mechanism [3], and stake is dynamic different from the concept of the epoch in ouroboros, in which the epoch has frozen stake for leadership purposes.

3.2 slot

period of time in which new block is issued

3.3 span

leader election span of time, which can be unspecified period using controller, or fixed 1/3 of slot as described in khonsu [4] during which leaders for slots in the future are elected.

4 timelocked contract

4.1 grinding attack in stake, unstake contracts

stakeholders can move funds between different accounts during the slot for higher probability of winning, such attack can be prevented via timelocked contracts.

References

[1] Ouroboros Genesis *Composable Proof-of-Stake Blockchains with Dynamic Availability*, Christian Badertscher, Et al, 22-February-2019

[2] bribery attack *Lecture 18: Bribery and stake grinding attacks*, David Tse, Stanford University, Spring 2020 04-June-2020

[3] cascade, *consensus high incentive monetary policy*, ertosns, 15-4-2023

[4] khonsu, *darkfi khonsu consensus*, ertosns, 31-12-2022