VIP-214: PER-EPOCH VRF-BASED RANDOM BEACON

Zhijie Ren
VeChain Foundation
zhijie.ren@vechain.com

Ziheng (Peter) Zhou
VeChain Foundation
peter.zhou@vechain.com

October 20, 2021

1 Overview

In the Proof-of-Authority consensus algorithm [1] (PoA), the block proposer in a future round cannot be predicted if the active/offline status of the nodes are not foreseen. This assumption is practical, however, not quantifiable as there is no theoretical rigorous guarantee on the unpredictability, which is a crucial factor to predict the "adaptive corruption attack". In other words, there remains an unknown probability that adversaries could exploit to bribe a sequence of future leaders and perform a double spending attack.

To improve the unpredictability of PoA, we introduce a Per-Epoch VRF-Based Random Beacon generation mechanism, which is inspired by the random beacon generation mechanisms used in [2, 3, 4]: Firstly, we divide the observed chain into "epochs" of Q blocks, i.e., the block of height h is in epoch e if $h \in [(e-1)Q+1, eQ]$. Then, a random beacon is generated for each epoch e, using the random seeds included in the blocks of epoch $e-2$ with a Verifiable Random Function (VRF) based mechanism. The random beacon will be used for leader selection in this epoch.

We then prove that the random beacon is unpredictable before epoch $e-2$, which is sufficient in practice to prevent adaptive corruption attack since it is unpractical to corrupt all related parties with a short notice. Then, we also show that the beacon cannot be manipulated by the adversaries to gain any significant and accumulative advantage in the leader selection process.

2 Preliminary

2.1 Notations

Symbol	Description
N	Total number of nodes
$u = 1, 2, \ldots, N$	node index
Q	Number of blocks in an epoch
b_e	The random beacon of epoch e
r	Consensus round number
$l_r = 1, 2, ..., N$	Leader in round r
$\mathrm{VRF}(l, \alpha)$	The random number generated by node l using message α
$H(\cdot)$	Cryptographic hash function

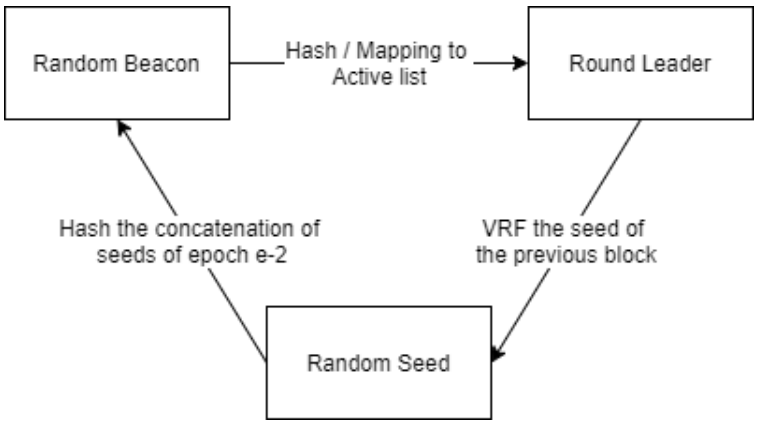

Figure 1: Random Beacon generation

$\beta(B_{e,k})$	The random seed in the k-th block of epoch e
$\beta[u,r]$	The random seeds generated by node u in round r
$\mathcal{A}_{u,r}$	The active list of round r known to node u

2.2 VRF

The verifiable random function can be considered as a public-key version of keyed cryptographic hash. The hash of a given message β can only be computed by the owner of the private key SK and can be verified by anyone given the public key PK and message α. The scheme defines the following functions:

- $\beta, \pi \leftarrow \texttt{PROVE}(\texttt{SK}, \alpha)$ - function that generates VRF proof;
- $\texttt{T/F}, \beta \leftarrow \texttt{VERIFY}(\texttt{PK}, \alpha, \pi)$ - function that verify VRF proof;

Then, we use the notation $\beta_{u,\alpha} = \mathrm{VRF}(u, \alpha)$ if $\beta_{u,\alpha}, \pi \leftarrow \texttt{PROVE}(\texttt{SK}_u, \alpha)$. Here, $\texttt{SK}_u$ is the private key of node u.

2.3 Review AM status in PoA

In [5], the concept of AM (Authority Masternode) status is introduced: All nodes are initially considered as "active", i.e., $\mathcal{A}_{u,r} = \{1, 2, \ldots, N\}$ for all u if $r = 1$. Then, a node u that refrains from proposing blocks will be marked as "inactive" by other nodes. Hence, at round r' if a node u' observes that chain where u fails to propose a block in his round, will set $\mathcal{A}_{u',r'} = \mathcal{A}_{u',r} \backslash u$.

Then, if u determines to become active, he will add himself to his active list $\mathcal{A}_{u,r}$ and propose a block when he is selected as the leader according to the list. When this block is accepted as the canonical chain, other nodes will also add u to the list. Note that when u is proposing a block, another node v could also propose a block according to a list $\mathcal{A}'$ without node u. However, according to our canonical chain selection rule of PoA, the block proposed by u has a higher chance of being accepted since it has a higher "weight" than the block proposed by v.

3 Per-Epoch Random Beacon Generation

In Figure 1, we show a brief diagram for the random beacon generation.

3.1 Random beacon

By definition, an epoch e consists of Q consecutive blocks on chain, denoted by $B_{e,1}, B_{e,2}, \ldots, B_{e,Q}$. In each block, the leader will include a *random seed* (will be introduced later), denoted by $\beta(B_{e,k})$, which is generated by the VRF

introduced in Subsection 2.2. Then, the random beacon of epoch e, denoted by b_e is computed by

$$b_e = H(\beta(B_{e-2,1})|\beta(B_{e-2,2})|\dots|\beta(B_{e-2,Q})). \tag{1}$$

3.2 Random seed

In each round r, the leader l_r will include a random seed $\beta[l_r, r]$ in his proposed block. Here, we assume that the proposed block is at height h, thus denoted by $B_{\lceil h/Q \rceil, h}$. The random seed is generated by using VRF on the seeds from the parent block, i.e.,

$$\beta[l_r, r] = \beta(B_{\lceil h/Q \rceil, h}) = \mathrm{VRF}(l_r, \beta(B_{\lceil (h-1)/Q \rceil, h-1})) \tag{2}$$

3.3 Leader selection

The leader selection mechanism is similar to the original leader selection mechanism in [1]. At each round r, node u derives an active list $\mathcal{A}_{u,r}$ according to his observed chain using the same mechanism as described in [1]. Then, instead of hashing the concatenation of the timestamp and the height, we determine the leader of round r as the following:

$$l_r = \min_{u \in \mathcal{A}_{u,r}} H(b_e|r|\texttt{ADDRESS}_u). \tag{3}$$

4 Security Analysis on the Random Beacon

In this section, we show that the random beacon generation mechanism and the leader selection mechanism is proven secure.

4.1 Unpredictability

Theorem 1. *The probability of knowing the random beacon of epoch e before epoch $e-2$ is negligible.*

Proof. By the random beacon generation mechanism, the random beacon of epoch e is determined by all random seeds of epoch $e-2$, which are generated by the leaders of the blocks in those rounds. Then, as the nodes who generate the random seeds of epoch $e-2$ are all selected independently with the same random beacon b_{e-2}, by the Law of Large Number (LLN), the probability that all seeds are generated by adversaries is negligible when Q is large. Then, since honest nodes only generate their random seeds using VRF in epoch $e-2$ and the adversaries, or any node in general, could not predict the VRF without holding the private keys of the honest nodes, the random beacon of epoch e is not predictable before epoch $e-2$. □

Note that there is no guarantee that the random beacon b_e is unpredictable in or after epoch $e-2$. In particular, the random beacon, as well as all leaders in epoch e are potentially revealed after epoch $e-2$. However, we believe this is a sufficient guarantee to prevent adaptive corruption attack in practice and in line with the unpredictability guarantee of most PoS algorithms [3, 2].

Moreover, the reason of choosing the epoch $e-2$ instead of $e-1$ is for the consistency, i.e., to guarantee that all nodes would recognise the same random beacon with high probability and prevent adversaries from causing inconsistency on the random beacon by creating forks at the end of an epoch.

4.2 Unbiasness

It is also crucial that the random beacon has sufficient "unbiasness", i.e., the adversaries could not arbitrarily manipulate the random beacon to gain significant advantage in the potion of adversarial leaders, or even control the future generation of random beacons. In our random beacon generation mechanism, the adversaries could manipulate the random beacon for at most k times if the last k blocks are all generated by adversaries in an epoch. However, with this biased beacon, the probability that the adversaries could be selected as the last k adversaries decays exponentially as k grows. Hence, the chance that adversaries controlling k last block in an epoch e manipulate the beacon and also controls the leaders of the last k blocks in epoch k is low when k is large. Hence, we conclude that the biasness of the adversaries will not accumulate.

Furthermore, due to LLN, the chances of adversaries being selected as leader in an epoch will not be significantly larger than their ratio when Q is large. Hence, we could conclude that the adversaries could not take any significant advantage in the leader selection process by manipulate the random beacon.

References

[1] Vechain development plan and whitepaper. https://cdn.vechain.com/vechainthor_development_plan_and_whitepaper_en_v1.0.pdf, 2018.

[2] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference*, pages 357–388. Springer, 2017.

[3] Iddo Bentov, Rafael Pass, and Elaine Shi. Snow white: Provably secure proofs of stake. *IACR Cryptology ePrint Archive*, 2016:919, 2016.

[4] Bernardo David, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 66–98. Springer, 2018.

[5] Proof of authority. https://docs.vechain.org/thor/learn/proof-of-authority.html.