BABE

Introduction

B lindA ssignment forB lockchainE xtension (BABE) serves as a block production engine, drawing inspiration from Ouroboros Praos(opens in a new tab) , another proof-of-stake protocol. It functions autonomously, offering probabilistic finality, or it can be integrated with a finality mechanism like GRANDPA.

BABE operates on a slot-based algorithm, dividing time into eras, epochs, further segmented into slots. Within the Avail context, each slot lasts for twenty seconds, aligning with the target block time. In every slot, BABE determines an author (or potentially multiple authors) responsible for producing a block.

If you're not familiar with Avail's terminology, you may check out our Glossary . On Avail's explorer, you can observe the eras and epochs by navigating to the staking page and locating the information at the top-right corner.

BABE Block Production Process

Each slot may have both a primary and a secondary author, chosen from amongst a set of active validators. The assignment of primary authors, aka slot leaders, is a random process governed by the VRF function. However, due to the way the function works, there may be instances where no validators qualify as the primary author. To maintain a consistent block time, BABE employs a round-robin system to designate secondary slot leaders, who produce new blocks without a designated leader.

As we know, the selection of primary authors is powered by a verifiable random function (VRF). It thus becomes crucial to establish a universally accepted form of randomness that remains untampered and verifiable for all parties involved. VRFs address this challenge by generating a pseudo-random number accompanied by a proof of its proper generation. These functions take various parameters, including a private key. The VRF considers an epoch random seed (pre-determined by all nodes), a slot number, and the author's private key. As each node possesses a unique private key, this ensures the generation of a distinct pseudo-random value for each slot.

During an epoch, each author employs its VRF for every slot. For slots where the output falls below an agreed-upon threshold, the validator gains the right to author a block during that slot. The random nature of slot assignment introduces the possibility of slots without a primary leader and those with multiple primaries.

To address vacant slots and maintain uninterrupted block production, BABE incorporates a round-robin fallback mechanism. Each slot is assigned a secondary leader. In cases where no entity declares itself as the primary leader at the slot's commencement, the secondary leader steps in to produce a block. This fallback mechanism ensures that every slot has an assigned block author, contributing to the assurance of a consistent block time.

Below is an example of BABE block production in action.

Prepared block for proposing at 127907 (121 ms) [hash: 0x7f68240041f3e921c33968dd834468335da4150ea323d99f60b6cdf28ac82bbf; parent_hash: 0xb34c…9bf8; extrinsics (15): [0x04c0…652f, 0x8751…b60b, 0xfbe4…23f7, 0x9817…c7ee, 0x33ab…b82f, 0x5296…ab61, 0xfb50…16a7, 0xba5e…bf07, 0xafba…c299, 0xc383…ec57, 0x2876…e25b, 0x4971…0cc8, 0x5204…5aa5, 0xbf53…3ab0, 0xdd87…ef68]
Pre-sealed block for proposal at 127907. Hash now 0x329230818f4aba570925f85d4ed78eca38cdd3f08996777588fd29050f565e4a, previously 0x7f68240041f3e921c33968dd834468335da4150ea323d99f60b6cdf28ac82bbf. Prepared block for proposing at 127939 (126 ms) [hash: 0xcc5158a686169433cf8c8b7a417103381d9cf96e8c57a695c8bae2a9cf466378; parent_hash: 0x35f0…9f48; extrinsics (11): [0x3386…2d55, 0xe4df…ba5a, 0xe924…a0e9, 0x7265…be43, 0x0d0e…4365, 0x474c…e485, 0x2613…e297, 0x3d2b…e930, 0x5d93…e34f, 0x3457…4676, 0xbfdf…76c9] Pre-sealed block for proposal at 127939. Hash now 0x20ba2195108a6b76faf3c83656d9ba265e426041e97681a66264c15362c0241e, previously 0xcc5158a686169433cf8c8b7a417103381d9cf96e8c57a695c8bae2a9cf466378.

BABE Functions

Here's an overview of how BABE functions.

Slot-Based Consensus : BABE operates on a slot-based mechanism, where time is divided into fixed intervals known as slots. Each slot represents a designated timeframe during which a new block can be produced.

Leader Election : In each slot, a leader is elected to propose and produce a new block for the parachain. The leader election process in BABE is deterministic and depends on a combination of the block's hash and a random number derived from the VRF (Verifiable Random Function) scheme. The VRF helps ensure unpredictability while still allowing nodes to verify the legitimacy of the leader.

Blind Assignment : The term "Blind Assignment" in BABE refers to the process of selecting the leader for a slot without revealing the identity of the leader until the block is produced. This adds an element of security and prevents potential attacks based on knowing in advance who the leader will be.

Adaptive Time Slot Duration : BABE features an adaptive time slot duration, meaning that the length of each slot can be adjusted dynamically based on network conditions. This adaptability helps Avail handle variations in block production times more efficiently.

Finalization : While BABE is responsible for proposing and producing blocks, finalization of blocks is achieved through the GRANDPA consensus algorithm. GRANDPA is responsible for ensuring the overall security and consistency of the Avail chain.

While BABE is a powerful algorithm to select new block authors in a verifiably random way, Avail uses GRANDPA in addition to BABE to achieve deterministic chain finalization. In the next article, we will learn about GRANDPA, Avail's block finalization mechanism.

Consensus GRANDPA