



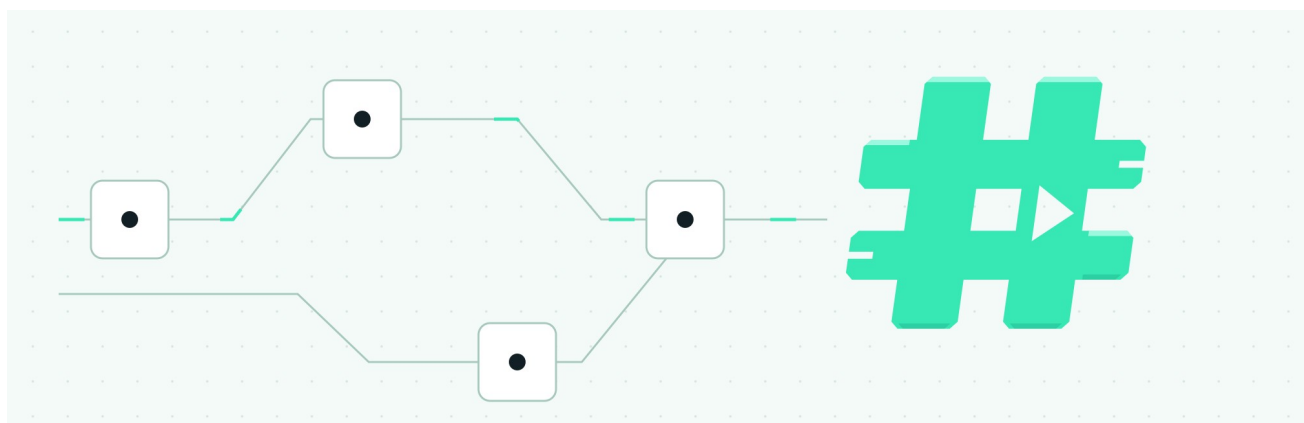
PROJECT WHITEPAPER

HashPlay

项目白皮书

平台机制与资金处理

面向用户与合作伙伴



版本 1.0 / 2026 年 10 月 30 日

阅读导航

01	项目概述	02
02	哈希计算与结果核验	03
03	合约与资金结算	04
04	资金流向与安全机制	05
05	账户管理与服务规则	06

01 项目概述

HashPlay 是围绕区块哈希构建的互动娱乐平台，整合钱包登录、期次查询、订单记录与账户管理。用户可复算公开哈希，结合订单与资金记录核对结果。

平台采用种子承诺与区块哈希结合的计算机制，参与前公布种子凭证、目标以太坊区块高度及封盘时间。目标区块产生后，用户可结合实际区块哈希与公开种子复算结果。

HashPlay 合约负责订单授权校验、赔付预留、结算与超时退款，并记录链上事件。平台维护个人账户账本，按适用规则判定业务结果。

平台功能

功能	用户可查看或办理的事项
钱包与账户	钱包登录、余额查询与账户流水
期次与订单	期次参数、订单提交与处理状态
哈希核验	种子凭证、区块参数与计算结果
资金服务	结算记录、提现及适用的退款流程

参与流程

用户选择房间与币种，确认期号、封盘时间、限额及费用，提交前保存种子凭证与本期参数，提交后保留订单编号及金额。

结果公布后，通过 Hash 记录获取种子与区块参数，复算哈希并核对到账。平台余额和合约钱包分别采用对应房间配置的资金路径。

本文介绍平台功能与协议机制，实际开放功能、币种、合约地址及适用规则，以平台公布资料为准。

02 哈希计算与结果核验

种子凭证

每个房间、每一期使用独立的 32 字节随机种子。参与前公布种子凭证与目标区块高度，结果公布时提供原种子与实际区块哈希。核验时，将复算凭证与原记录比较，确认种子、房间 ID、期号及目标高度是否一致。

公开结果使用 SHA-256，按以下 UTF-8 文本计算：

```
proofText = roomId + ":" + periodNo + ":" + blockNumber + ":" + seed
drawText = proofText + ":" + normalizedBlockHash

drawSeedProof = hex(SHA-256(UTF-8(proofText)))
drawHash = "0x" + hex(SHA-256(UTF-8(drawText)))
```

roomId、periodNo 和 blockNumber 分别为房间 ID、期号及目标区块高度，使用无前导零的十进制文本。seed 为 64 个小写十六进制字符；normalizedBlockHash 为移除 0x 前缀后的 64 个小写区块哈希字符。字段以英文冒号连接，不加入空格或换行；十六进制文本直接参与计算，不先解码为字节。摘要输出为小写十六进制。

核验流程

1. 参与前保存种子凭证、房间 ID、期号、目标区块高度、封盘时间与适用规则。
2. 结果公布后，用公开种子复算 drawSeedProof，与原凭证比较。
3. 通过独立节点或区块浏览器，核对以太坊主网指定高度的区块哈希及确认状态。
4. 复算 drawHash，结合适用规则核对订单结果及资金记录。

封盘时间与业务类型不参与上述摘要，应随本期规则保存。参与前保存的凭证是核验依据，事后取得的凭证不能替代原记录。

合约结果证明

HashPlay 合约使用 Keccak-256 与 Solidity ABI 编码。种子及区块哈希的十六进制文本先解码为 32 字节，再作为 bytes32 参与计算：

```
seedCommitment = keccak256(abi.encode(seed))
resultHash = keccak256(abi.encode(seed, ethereumBlockHash))
```

drawHash 用于公开核验，resultHash 用于合约证明，编码与摘要不能互换。合约校验授权和证明一致性；区块真实性另行核对，平台按规则判定业务结果并授权结算。

03 合约与资金结算

合约分工

HashPlay 合约体系由创建、路由、订单处理、保证金与资金池合约组成。HashPlayFactory 校验创建授权，HashPlayGameDeployer 部署游戏合约，HashPlayRouter 提供统一业务入口。每个游戏合约绑定独立的 HashPlayMargin；HashPlayVault 为平台余额业务保存公共代币资金。

本期首笔成功投注锁定种子承诺、目标以太坊区块号与封盘时间，后续投注沿用同一配置。订单须在封盘前且授权有效期内提交，确认成功的交易及匹配的 BetPlaced 事件共同构成链上接单记录。

订单资金预留

设本金为 A，含本金的约定毛赔付为 G。接单时，钱包或资金池提供 A，保证金合约提供 G 减 A，游戏合约为该订单预留 G。资金到账或授权校验失败时，交易整体回滚。

每笔待处理订单保留其资金预留，直到结算或超时退款。保证金管理地址可提取保证金合约中的可用资金；已经转入游戏合约的订单预留按订单规则释放。

平台费用

HashPlay 合约的平台费比例为 5%，按对应基数逐笔计算，并按代币最小单位向下取整。用户中奖按毛赔付减本金计费，费用从赔付扣除；未中奖按保证金提供方取得的本金收益计费。平局按本金计费，由保证金承担，用户本金全额返还。超时退款不收平台费，Gas 另计。

下表以本金 100、毛赔付 200 为例，订单总预留为 200，其中保证金投入为 100。金额为同一代币的示例单位。

处理结果	用户或资金池收回	保证金合约收回	平台费
中奖	195	0	5
未中奖	0	195	5
平局	100	95	5
超时退款	100	100	0

保证金合约收回金额包括返还的投入，其净变动需扣除原保证金投入。余额订单的回款进入公共资金池，再由平台按订单记录个人账户流水。

本章费用及预留规则适用于对应版本的 HashPlay 合约订单。实际房间采用的资金路径、赔率及代币精度，以该房间规则和部署版本为准。

04 资金流向与安全机制

订单资金流向

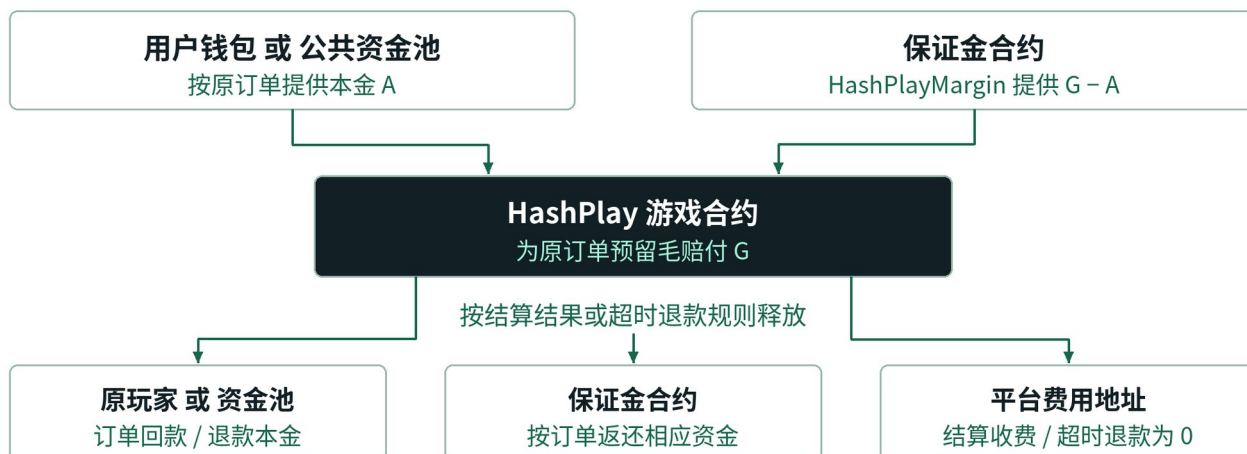


图 1 合约订单的接单预留与资金分配

本金来源及返还路径由原订单确定。钱包订单直接回原玩家，余额订单回公共资金池后关联个人账户。各项分配依据订单结果计算，金额为零的路径不转账；超时退款不收平台费。

核验与资金处理

公开核验



合约执行



超时恢复



图 2 公开核验与合约执行的检查流程

参与前公布目标区块高度，目标区块产生后取得实际哈希，并与公开种子共同核验。公开核验与合约证明采用各自的计算规则；区块来源与业务结果另行核对。资金池管理权限见下一章。

05 账户管理与服务规则

账户与提现

平台账本记录个人可用余额、冻结余额与资金流水。HashPlayVault 保存平台余额业务的公共代币资金，个人余额由平台账本维护。

HashPlayVault 提供授权提现接口：平台核对并冻结可提现余额后，签发包含用户、收款地址、币种、金额、订单编号和有效期的授权，由用户提交链上交易。合约验证授权及资金余额后执行转账，已成功的提现订单不能重复执行。提现需要有效授权、足够的公共池资金以及可执行的代币转账。

钱包直接参与的订单，结算款项转至原玩家地址；平台余额订单的回款进入资金池，并与个人账户记录关联。两种资金路径分别核对，避免同笔回款重复计入余额。

超时退款

HashPlay 合约的处理截止时间为本期首笔成功投注时间加 7 天，各币种共享该截止时间。封盘后且截止前可发布结果，结果发布后可结算；到达截止时，仍未处理的链上订单可按原订单字段申请本金退款。

任何人都可通过路由合约提交符合条件的退款，无需新的平台签名；退款需主动发起交易并支付 Gas。钱包订单本金退回原玩家，余额订单本金退回资金池并由平台按订单入账，保证金差额返回保证金合约。已结算订单保持原终态，退款金额为本金。

该机制适用于已被 HashPlay 合约接受且可匹配原记录的订单。平台支付取消及其他业务退款遵循对应流程；链上退款仍需链与代币处于可转账状态。

管理权限

游戏管理者管理业务签名者；订单签名者授权接单，结果签名者授权结果发布与结算。合约依照有效授权处理订单。资金池管理员管理准入、提现签名者及公共池资金，并具有管理员提币权限；管理员提币与用户授权提现分别记录。

保证金提供方承担相应赔付，用户本金随订单结果变化并可能发生损失。参与前应了解适用规则、费用与权限安排，并符合服务的准入条件。

记录查询

用户可结合期号、订单编号、金额与适用规则查询处理结果。链上订单同时保留链 ID、合约地址及交易记录，通过 BetPlaced、BetSettled 与 BetRefunded 事件核对接单、结算和退款；余额订单还需核对个人账户流水。