2019~2020 学年冬学期《区块链与数字货币》课程作业 3

应承峻 3170103456

1. 说明什么是 create 指令，什么是 create2 指令，两者的区别是什么？

在 CREATE2 以前，CREATE 指令创建的合约地址是通过交易发起者（sender）的地址以及交易序号（nonce）来计算确定的。sender 和 nonce 进行 RLP 编码，然后用 Keccak-256 进行 hash 计算。当使用 CREATE 时，无法提前预测哪段代码将处于某个给定的地址上，也无法在合约部署之后容易地“验证”这段代码，除非有区块链的直接访问权限，或者使用某些非常复杂的技巧。这些技巧可能包括与无密钥地址（即合约地址）进行非常混乱的多重转账操作，并且需要提前预付未来的手续费用等等。

而 CREATE2 函数则让地址变成了对合约代码的一种承诺，并且相比之下可能的状态更少。它由 初始化代码（init code），哈希值（hash）和盐（salt）共同决定了这个合约的地址。这实际上是一个巨大的优势，只要人们确实验证了初始代码。因为它意味着人们可以检查代码工厂与它们所创合约之间的关系，甚至完全无需知晓网络的状态，也可以判断正在部署的合约。所以硬件钱包，冷钱包之类的服务都能很好地运行。

2. 尽可能多地列举 create2 的使用场景，能够在哪些案例下为用户带来较大地便利。

Case 1：状态通道

状态通道由支付通道演进而来，我们先通过一个简单的例子介绍下支付通道，假设晓娜经常要去楼下的咖啡店喝咖啡，晓娜每次除了支付 0.1 eth 咖啡费用之外，还需要支付一笔小费给矿工。为了节约小费，晓娜可以在她与咖啡店之间创建一个支付通道，通过加密签名可以重复安全的转移以太币，而不用支付手续费。晓娜可以这样做：

1. 创建一个支付通道智能合约，并存入 20 个以太币（链上）。
2. 每次买咖啡时签名一条交易信息给老板，交易信息包含内容有：第几次购买咖啡、总共要支付多少钱给老板及签名数据本身。（链下）
3. 晓娜重复步骤 2，而老板任何时候都可以把晓娜的签名信息发送给链上支付通道智能合约，取回资金。
4. 晓娜不想喝咖啡了，取回支付通道的余额。

通过这样的方式，晓娜可以节约大量的手续费。状态通道则可以基于特定应用程序的状态进行链下交互（而不仅仅是支付信息）。

Case2：广义状态通道与 Force-Move 游戏框架

如果可以部署一个游戏合约定义游戏规则并抵押资金，玩家可以在链下玩游戏（每进行一步游戏签名发给对方），游戏结束时，只需要把最后的状态提交给合约，合约进行输赢判断，并奖励。Force-Move 游戏框架 就是让开发者可以模块化的、可扩展的方式，开发基于状态通道的的回合制游戏。

Tiny 熊和晓娜拥有一个抵押的资金的多签钱包，然后定义一个剪刀石头布的游戏合约，每次输方向赢方支付 1 个以太币，玩游戏可以在链下进行，结束后，最终的状态提交给游戏合约，并触发多签钱包根据状态分配资金。

通过使用 CREATE2，可以在游戏合约不上链的情况下进行游戏，因为只要游戏的规则代码确定了，就可以确定游戏合约的地址，在链下就可以基于这个确定的合约地址进行签名玩游戏，甚至我们根本不需要部署游戏合约，仅仅在有游戏玩家作弊的时候，部署游戏合约进行链上仲裁。

假如 Tiny 熊和晓娜赢的次数一样多，这样谁也不用给对方支付费用，对于链上的多签钱包，相当于什么也没有发生，这样也同样不需要部署游戏合约。

Case 3：

当货物寄出，并且是用户所相信的人成为 shipper 之后，用户就完全相信接下来的状态的改变，假设用户通过监听日志，发现已经被设置为寄出状态时，就发送报酬给商家。用户是聪明的，看到这个合约，发现，一但 shipper 被设置后，不能被再次设置，所以当用户看到已经是自己相信的寄出者之后，就完全相信。在 create2 指令之前，这是没有问题的，但是有了 create2，开发者可以 selfdestruct 之后 redeploy，然后直接设置自己为 shipper，修改寄出的状态。

参考资料：

[1]https://learnblockchain.cn/2019/10/23/create2-statechannel/

[2]https://www.chainnews.com/articles/751190833870.htm