区块链技术与应用

第十七讲 智能合约与去中心化应用

主讲人：赵其刚

智能合约

智能合约

使区块链真正成为了一个底层技术

使区块链可以应用于很多去中心、去信任的场景中，区块链的基础性价值才获得了较广泛的认可

智能合约

对智能合约的支持

- 公链技术架构的以太坊
- 联盟链技术架构的超级账本

智能合约

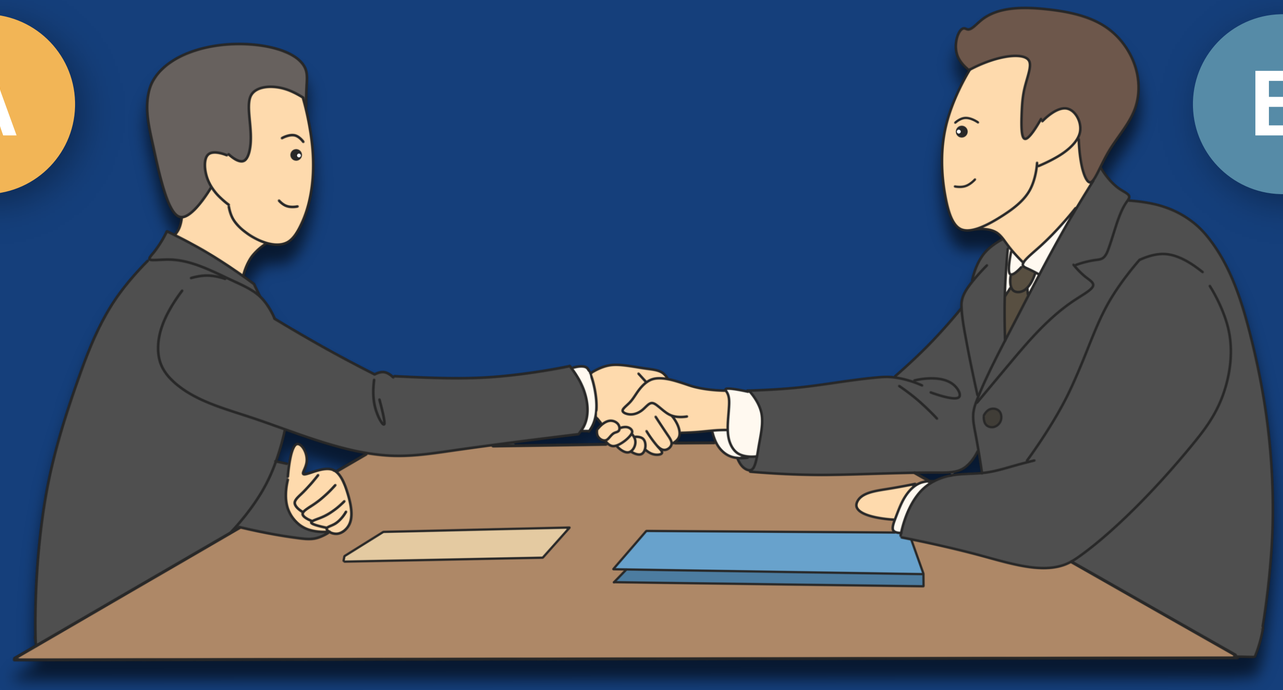
为什么说智能合约的出现，它使区块链对我们具有了基础性的意义呢？

智能合约

执行合约需要耗费大量社会资源

A

违反合同条约

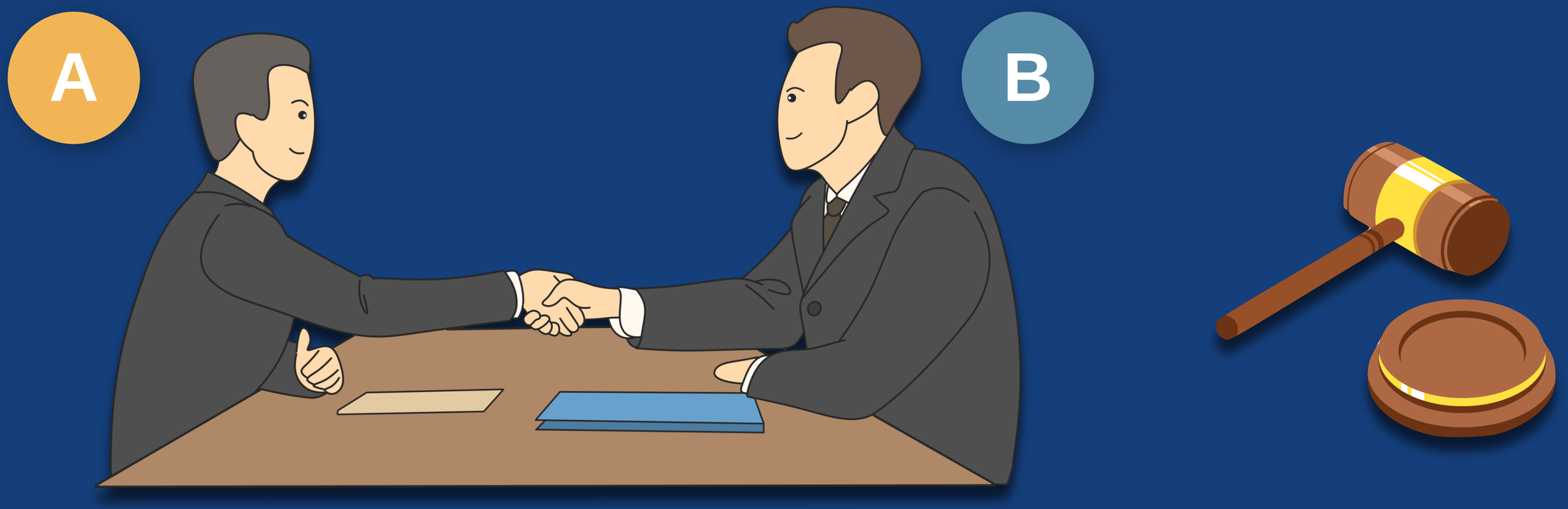


B

损失重大

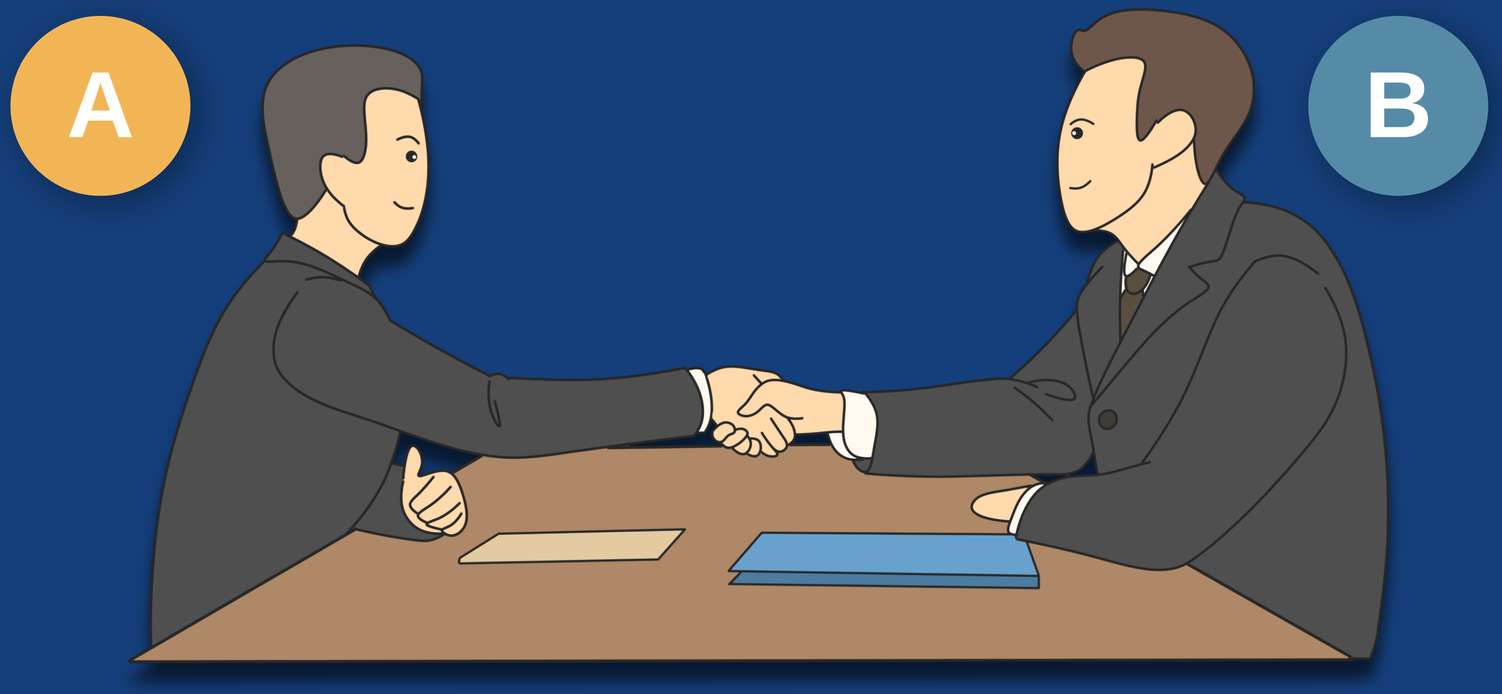
智能合约

执行合约需要耗费大量社会资源



智能合约

执行合约需要耗费大量社会资源



申请强制执行

- 立案
- 提供财产线索

智能合约

区别

- 就在于“智能”，不涉及人类主观想法，一切皆代码。

智能合约

智能合约

是一段写在区块链上的代码，一旦某个事件触发合约中的条款，代码即自动执行。

智能合约

智能合约是一段写在区块链上的代码

- 基本过程

智能合约

1

智能合约由区块链内的多个用户共同参与制定，可用于用户之间的任何交易行为。

协议中明确了双方的权利和义务，开发人员将这些权利和义务以电子化的方式进行编程，代码中包含会触发合约自动执行的条件。

智能合约

在每月5号之前给你打房租

收到房租时马上给对方钥匙

A

智能合约

2 一旦编码完成，这份智能合约就被上传到区块链网络上。

3 智能合约会定期检查是否存在相关事件和触发条件；满足条件的事件将会推送到待验证的队列中。

智能合约

4 区块链上的验证节点先对该事件进行签名验证，以确保其有效性；

等大多数验证节点对该事件达成共识后，智能合约将成功执行，并通知用户。

5 成功执行的合约将移出区块。而未执行的合约则继续等待下一轮处理，直至成功执行。

智能合约

部署到以太坊上的智能合约要消耗以太币

仲裁人 | 法官 | 执行人

“Less is more”

- 逻辑应尽可能地简单

智能合约的作用

区块链账本

- 所有交易数据无法篡改、不可伪造
- 能减少人工对账的出错概率和人力成本

智能合约的作用

区块链账本

- 所有交易数据无法篡改、不可伪造
- 能减少人工对账的出错概率和人力成本

智能合约的作用

- 投保乘客信息
- 航班延误险
- 航班实时动态

- 一旦航班延时符合赔付标准，赔偿款将自动划账到投保乘客账户

智能合约的作用

借钱给亲戚

借条

智能合约的作用

借钱给亲戚

智能
合约

去中心化应用——DAPP

中心化的服务模式

- 容易导致服务内容缺乏透明度，用户隐私泄露、数据被滥用等问题。

服务方和消费者之间的交易需要由极高的公司信誉和完善的评价系统甚至社会征信体系背书。

去中心化应用——DAPP

Dapp是去中心化应用（Decentralized Application）的简称

中心化应用（Centralized Application）

- BS模式下的 web 应用

分布式应用

去中心化应用——DAPP

中心化应用

- 分布式
- 非分布式

去中心化应用

- 一定是分布式

去中心化应用和现在的分布式应用的区别到底在哪里呢？

去中心化应用——DAPP

去中心化应用

- 开源
- 内部货币
- 去中心化的共识机制
- 无单点故障缺陷

去中心化应用——DAPP

DApp天然是分布式应用，避免了单点故障

- 区块链上的用户数据通常是用加密方式存储，数据的所有权归属用户，而非DApp的开发者。

去中心化应用——DAPP

- DApp的后端程序是部署在区块链上的智能合约，智能合约是一组预定义的业务规则，具备确定性（Deterministic）执行的特征，能有效降低信任成本。

DApp中消耗的资源由数字货币经济模型予以补偿或激励

去中心化应用——DAPP

DApp → D（Decentralized）

- 它具备分布式（Distributed）的特征
- 它具备分权（Decentralized）的特征

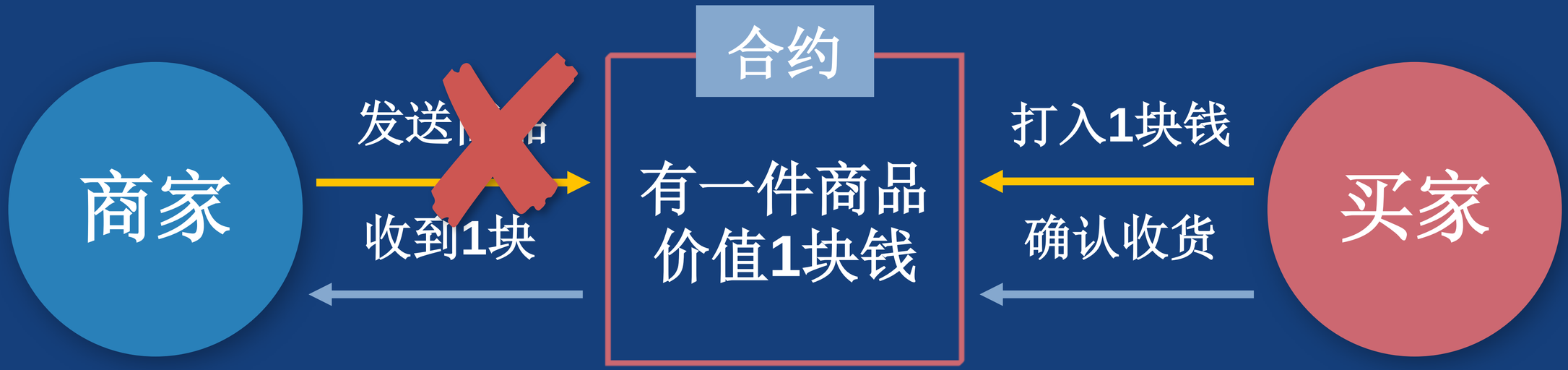
去中心化应用——DAPP

DApp ▸ 它具备分权（Decentralized）的特征

- 应用的开发者在上线应用之后，就不能随意修改升级应用内容，当然更加不可能修改数据；
- 应用本身具有博弈的特点，都把用户想象成理性经济人，做事之前考虑成本，这也是为什么大多数DApp都有它内置的代币（Token，也作通证）。

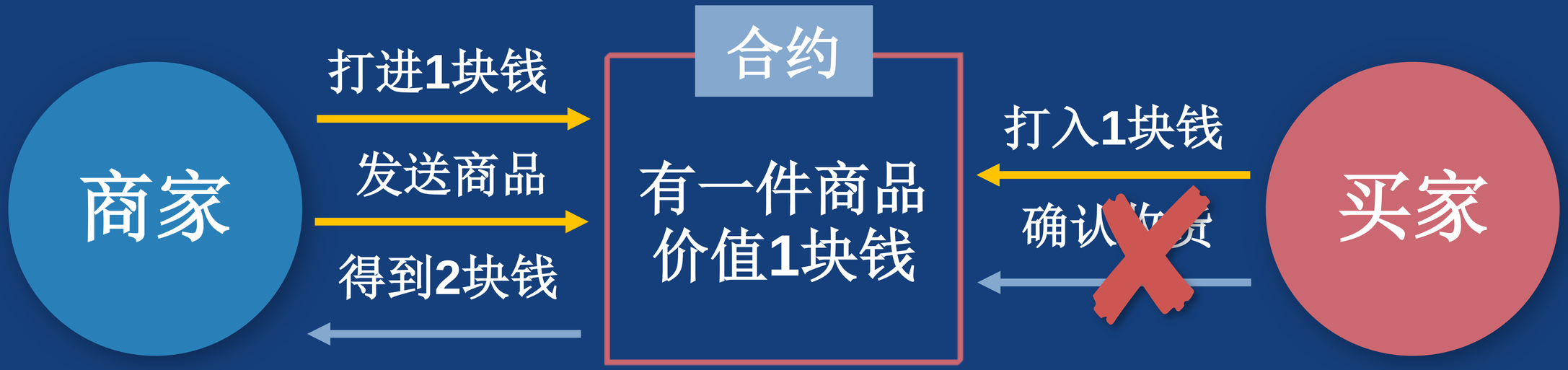
去中心化应用——DAPP

购买商品合约



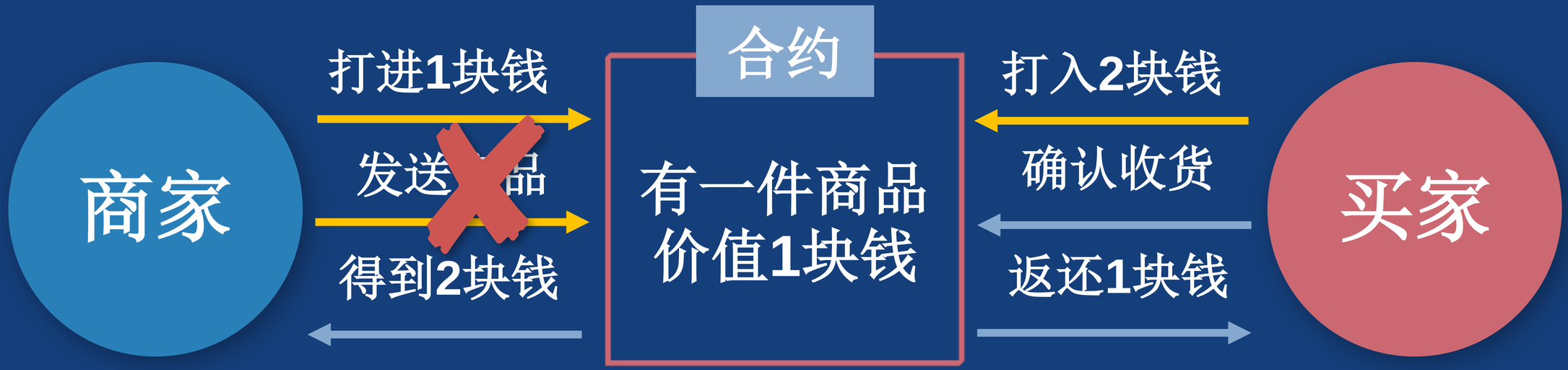
去中心化应用——DAPP

购买商品合约



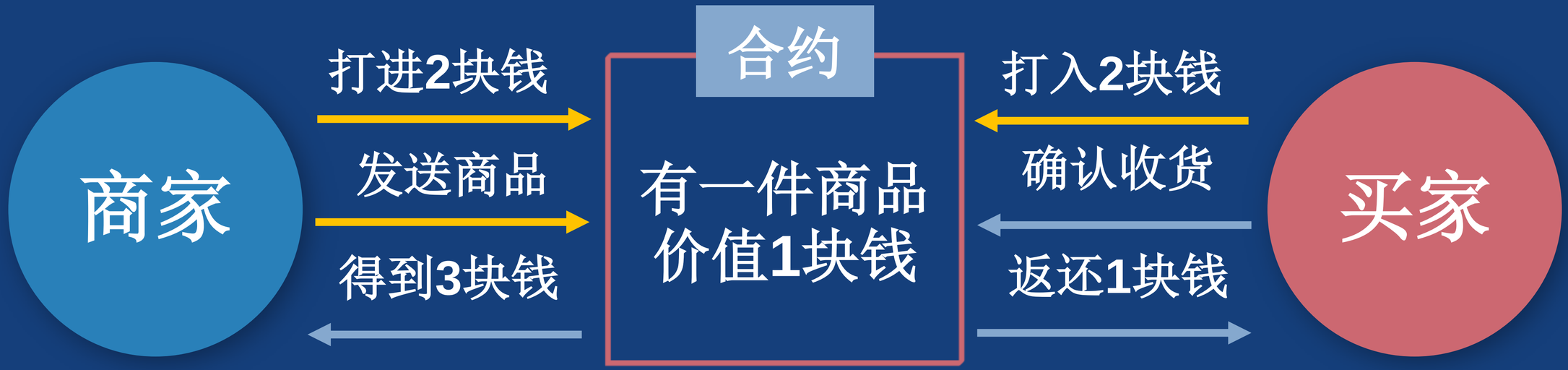
去中心化应用——DAPP

购买商品合约



去中心化应用——DAPP

购买商品合约



去中心化应用——DAPP

购买商品合约

理性经济人

商家

合约

有一件商品
价值1块钱

买家

去中心化应用——DAPP

锤子剪刀布

先出的人一定会输

因为先出的已经被记录在区块链上，那就意味着后面的人一定能看到对方的出拳结果，所以他一定会赢。

去中心化应用——DAPP

锤子剪刀布

不揭露结果

先出

- 把出拳的结果加salt然后hash才上链

后出

- 随机选择一个出拳

去中心化应用——DAPP

去中心的智能锁

智能合约 = 中间商

一把“智能”的锁

去中心化应用——DAPP

去中心的智能锁 实现逻辑：

- 房东通过智能合约Smart Lock Contract设置房屋租金。
- 租客通过查找合约地址，对所要租的房屋合约转账；
- 租客来到房屋门前出示二维码（由自己签名的消息转成的二维码）；
- 门锁上的摄像头识别二维码，并向合约验证签名的真实性以及租客的租房时间的合法性，进行开门。

去中心化应用——DAPP

以太猫（Cryptokitty）

- 是一款构建在以太坊区块链平台上的以太猫游戏

去中心化应用——DAPP

以太猫（Cryptokitty）

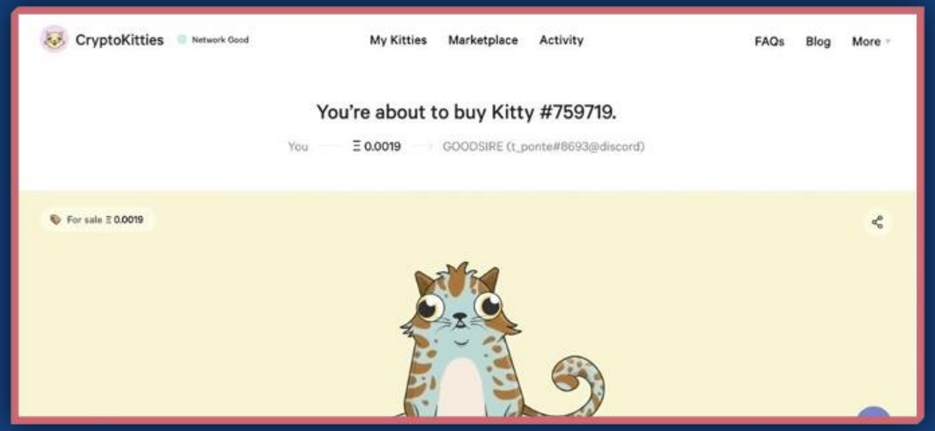
去中心化应用——DAPP

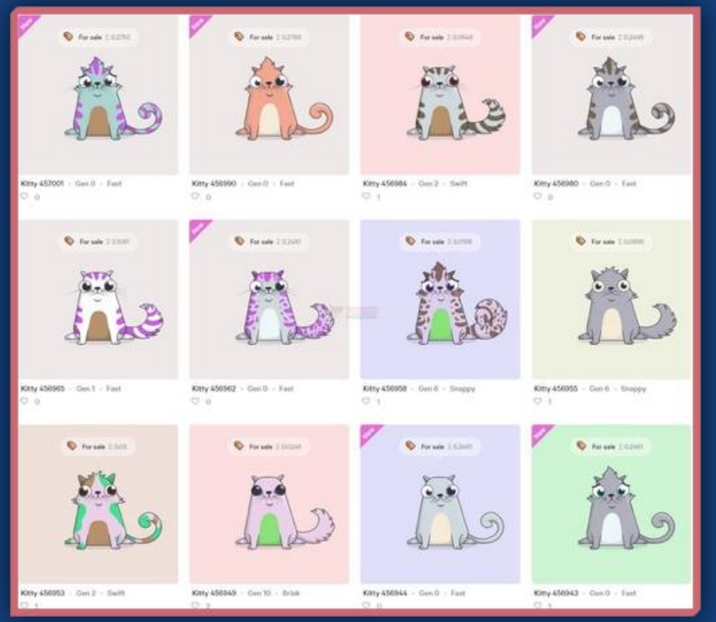
以太猫（Cryptokitty）

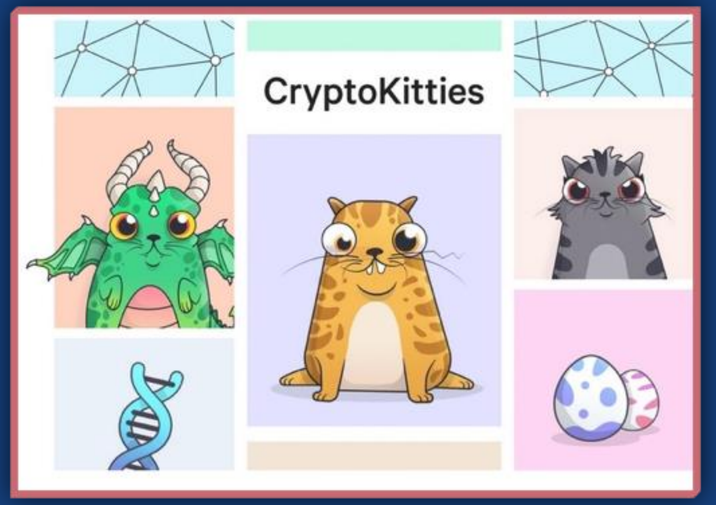
- 基于以太坊的DAPP（Decentralized Application，去中心化应用），由设计工作室 AxiomZen 设计打造，上线不到10天就迅速成为以太坊上交易量最大的DAPP。

去中心化应用——DAPP

以太猫（Cryptokitty）

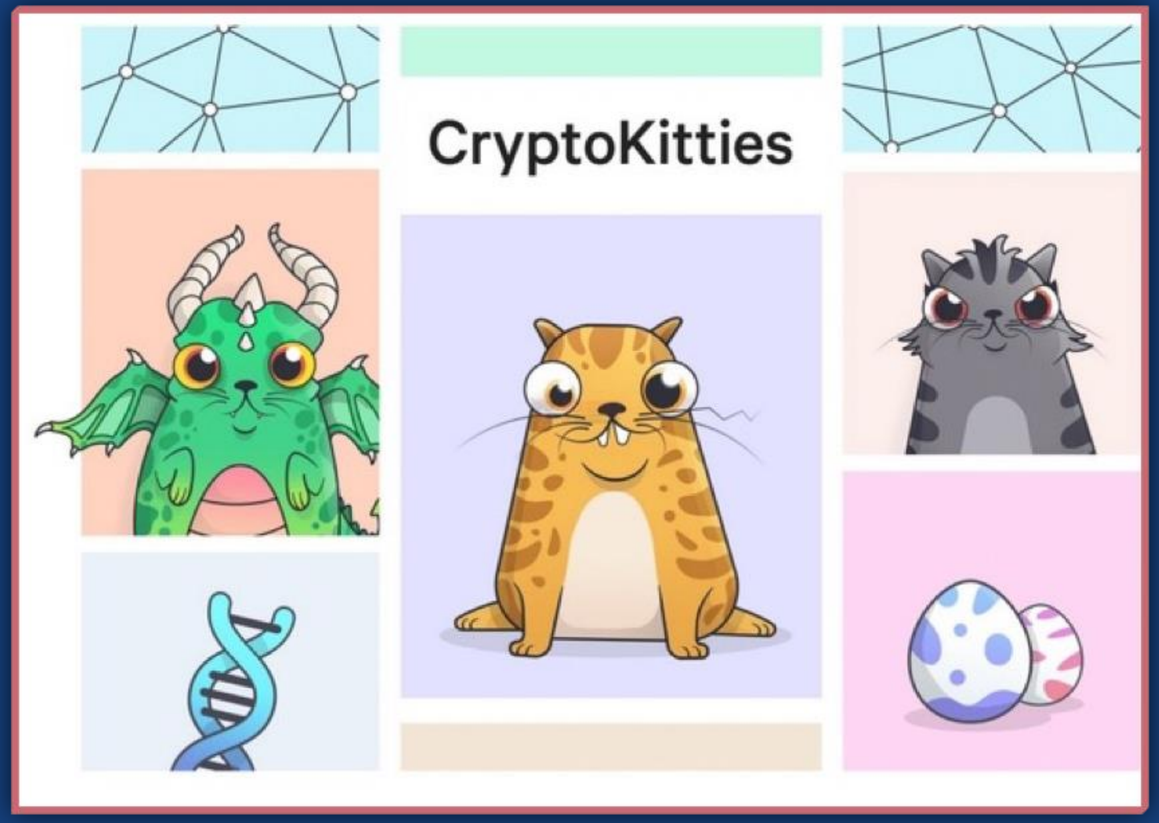






去中心化应用——DAPP

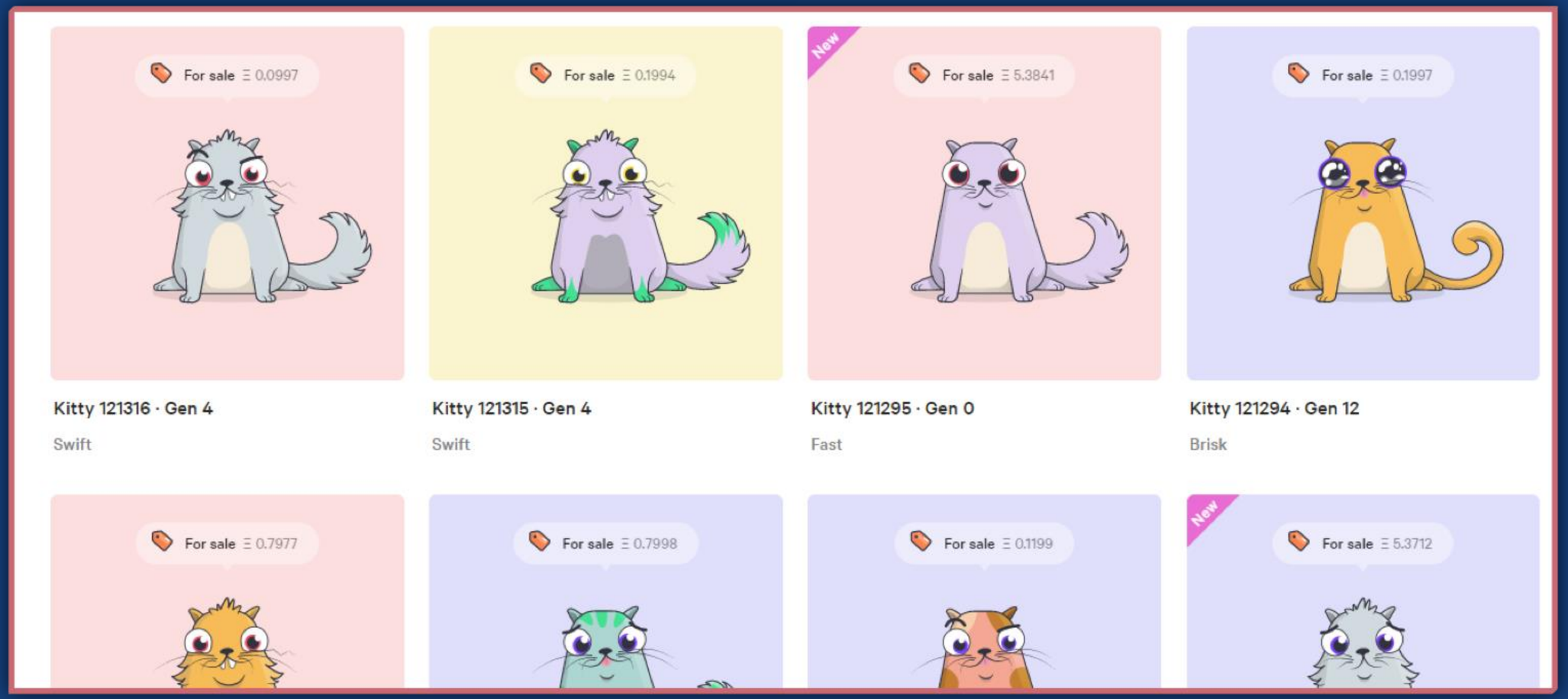
以太猫（Cryptokitty）



合法性由智能合约（Smart Contract）确定，而智能合约是无法关停的。

去中心化应用——DAPP

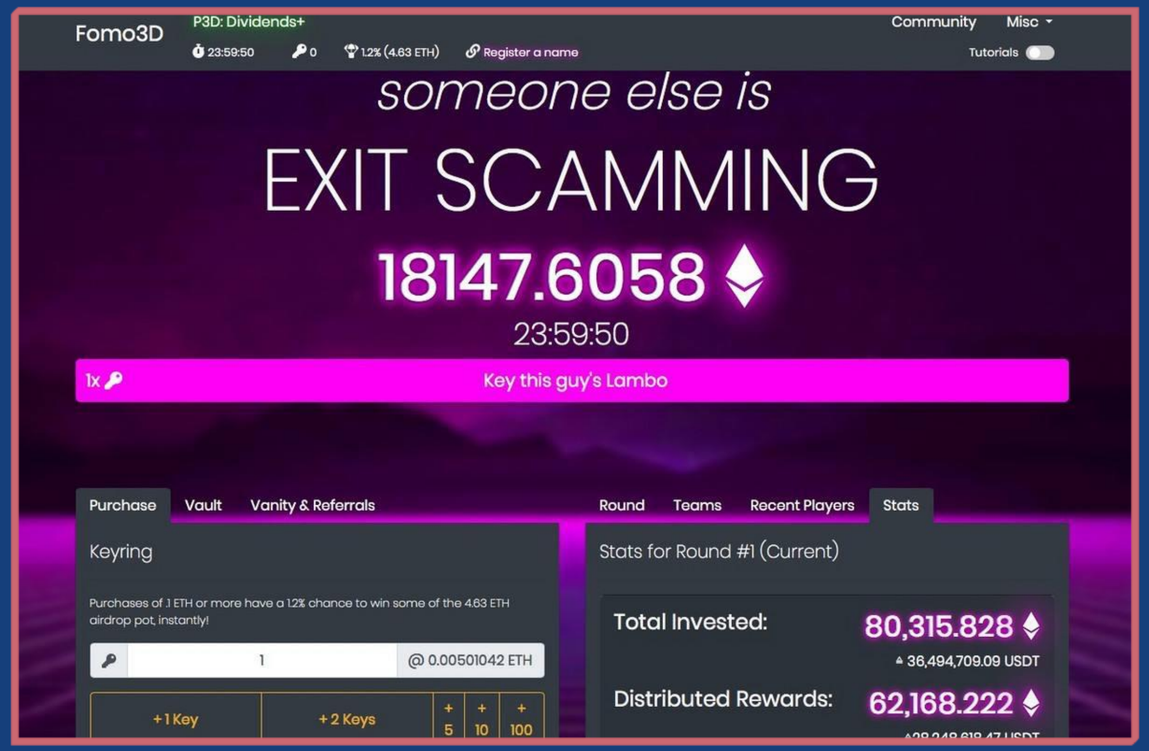
以太猫（Cryptokitty）



去中心化应用——DAPP

FoMo3D

exitscam.me



去中心化应用——DAPP

FoMo3D

设置了崩盘的上限为24小时，每个新加入这个骗局的人都会自动给游戏续命**30s**。

去中心化应用——DAPP

FoMo3D

在崩盘的时候，最后一个游戏参与者能获得之前所有参与者资金的23%，而其他的后来者需要为前面进来的人买单。

去中心化应用——DAPP

FoMo3D

代码开源，无法篡改

驱使赌局越来越大的是人的贪婪本性

去中心化应用——DAPP

FoMo3D

21,468.75ETH

9,903,536.56252刀

总结

1 智能合约是区块链进入2.0的一大重要技术成果，奠定了区块链作为一个底层技术的技术基础，智能合约本质上就是一块存储在区块链上的代码，这在交易的触发下自动运行。

支持智能合约的典型的区块链技术平台有以太坊和超级账本。

总结

2 基于智能合约的应用叫去中心化应用（DAPP）

它与传统的中心化应用如B/S架构的Web应用就在于其后端的核心逻辑与数据是存储在智能合约上的，因而去中心化应用就具备一旦部署，其执行逻辑与数据不可篡改，不能由单一组织所控制。

DApp可广泛应用于很多需要去信任的场景中