2018年9月26日 火币区块链技术学习与分享群-今日区块链技术晚报

一.Tech News

0⃣Ethereum的whisper协议

通过Whisper发送消息需要使用特定结构进行加密。可以通过监视/订阅方法（Whisper v5）收听消息通道。因此，用户可以收听特定收件人，特定主题或仅发送给您的消息。

有效负载通过以下两种方式加密：

1-仅针对一个收件人的messages将通过通过ECIES加密，收件人的公钥通过SECCI-256k1加密。

2-没有预定收件人的邮件将使用随机配置的密钥通过AES-256加密。此密钥将进一步塑造消息的主题。这些主题与信封标题内的匹配主题的相同顺序一起存储。

如果有消息中间件MQ的经验可能会非常好理解！

1.Read more on here

2.Whisper functions (RPC)

1⃣以太坊摘要：君士坦丁堡testnet前两周的进度！

文章作者梳理了现在以太坊项目的所有进度，以太坊生态的开发者值得阅读，包括最新的研究成功等。推荐阅读！

	7th Aug	14th Aug	21st Aug	28th Aug	4th Sept	11th Sept	18th Sept	25th Sept
People	41	43	43	43	42	42	43	43
Repositories	161	163	163	163	164	166	167	168
Last commit	7th Aug	14th Aug	21st Aug	28th Aug	4th Sept	11th Sept	18th Sept	25th Sept

	7th Aug	14th Aug	21st Aug	28th Aug	4th Sept	11th Sept	18th Sept	25th Sept
Forks	13K	13K	13K	14K	14K	14K	14K	14K
Watchers	4,334	4,347	4,365	4,386	4,401	4,413	4,410	4,419
Commits (last 30 days)	162	191	187	182	178	188	142	142
Closed issues (last 30 days)	320	425	512	493	461	379	304	284

github的开发者、项目数、最新提交、关闭的issues等，可以很好的看出Ethereum项目的开发进度。

1.Read more on here 君士坦丁堡testnet前两周的进度

3️⃣ 由NEO智能合约提供支持的去中心化应用现在可以在nOSNet上发布和发现，nOSNet是一个具有由nOS驱动的特殊功能的NEO Testnet（NEO测试网络），文中详细描述了怎么在NEO测试网络中创建、发布你的Dapp。有详细步骤。

1. Read more on here

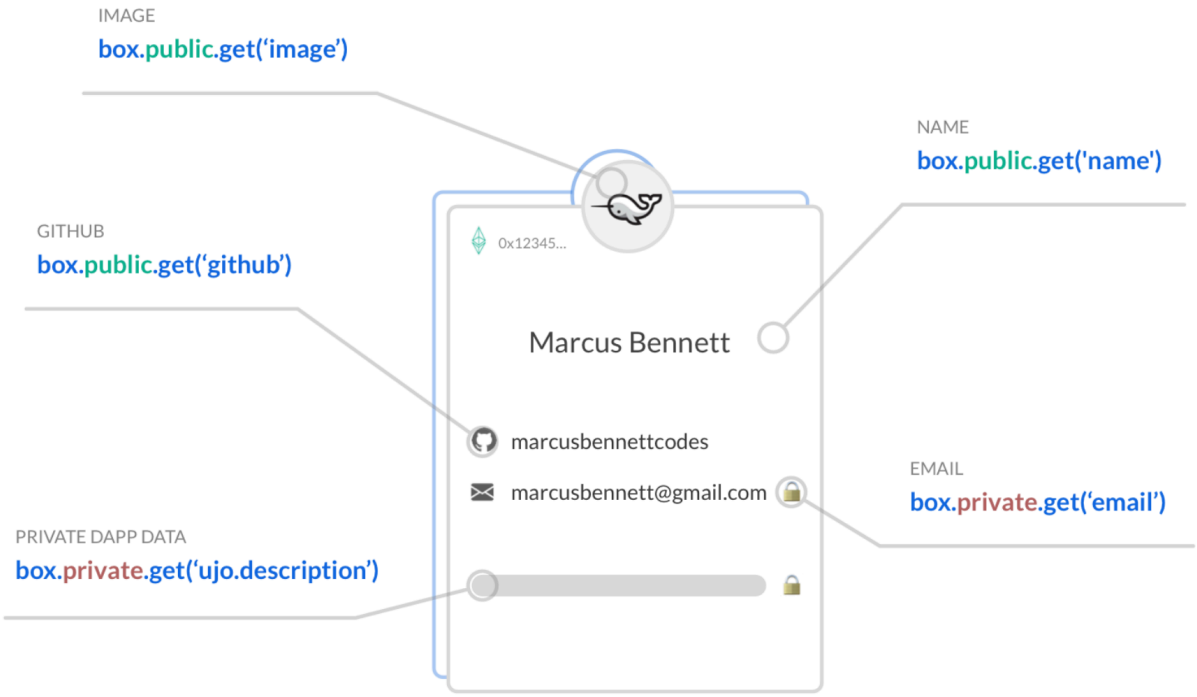
2.其官网

4️⃣Ethereum Profiles API，使用Profiles API 去构建一个使登录用户变得容易，并构建可扩展，用户友好的dapps.

3box-js是一个类库，可以方便的让开发者去set、get、remove 公有或者私有的以太坊账号数据。

开发人员可以使用3Box DB来存储用户身份数据，设置，行为数据等，并轻松地在dapps之间共享这些数据。 3Box适用于所有标准的以太坊钱包软件，如MetaMask，Coinbase Wallet，Trust Wallet，Vault等。

3Box数据存储在IPFS中的两个OrbitDB（OrbitDB uses IPFS as its data storage and IPFS Pubsub to automatically sync databases with peers.）键值对中：一个用于用户的公共数据，另一个用于私有数据。 公共数据以未加密的方式存储，而私有数据以加密方式存储，因此只能由用户授权的第三方读取。 只要用户保持对其以太坊私钥的访问权限，就可以恢复存储在3Box中的加密数据。



1.Read more onhere

2.orbitDB

5️⃣Nethereum 2.0.0 rc5—Unity3d integration, 昨天介绍了ethereum和Unity3d 开发的RPG游戏。现在就有现成的框架来给大家使用了。

1.Read more on here

2.Nethereum项目主页

3.和以太坊结合的Flappy项目源码

4.试玩一下区块链版的Flappy

6️⃣ZoKrates tutorial with Truffle -简单的ZoKrates与Truffle集成的分步演练

零知识证明是证明者说服验证者知道某些秘密信息而不泄露其详细信息的一种方式。 在传统的交互式零知识协议中，在验证者可以被说服之前，需要在证明者和验证者之间进行几轮交换。 zk-SNARK本质上是一种非交互式零知识协议，它允许证明者和验证者之间的这种交换非常短。 要在以太坊中实现zk-SNARK，您可以使用ZoKrates工具箱。 使用ZoKrates，您可以创建智能合约以充当验证者。 您还可以使用它来生成您知道某些秘密信息的证据，并使验证者相信这一点。 您只需发布确认验证智能合约到以太坊网络的事实，而不是通过某种在线渠道说服验证者。

1.零知识证明ZoKrates工具箱github主页

2.zk-SNARK的一些例子

3.Zcash 中如何使用zk-SNARK的

4.Read more on here

7️⃣来把挖矿实战把，教你在Windows本上如何挖litecoin，现在litecoin的hash rate 为247Th/s左右,2分半出一个块。

“Litecoin使用Scrypt算法减少了块时间，而比特币使用SHA-256哈希算法。 与SHA-256的一个重要区别是Scrypt可以在CPU上运行并消耗更少的能量，因此在各个矿工中很受欢迎。 Scrypt是内存密集型的，这意味着Scrypt生成的数字也会存储在RAM中，以便在提交结果之前可以连续访问它，并且速度更快。”

Read more on here

8️⃣blockchain.com/research发布了一篇关于稳定币的报告重量报告 “Shining light on The State of Stablecoins”

我们很高兴地宣布出版“The State of Stablecoins”，这是一份关注快速增长的稳定币世界的重要研究报告。

该报告首次全面审视了稳定币市场的现状 - 这是加密货币生态系统中一个未被充分讨论但日益重要的部分。这是我们期望在未来几年看到重大创新的空间。

由于稳定币与商品的价格或算法的运作联系在一起，因此它们的价格比其他密码集更不稳定。这意味着它们适用于长期的一系列用例，包括价值存储和衍生工具，以及智能合约和汇款。总的来说，这些可能价值数万亿美元。这意味着稳定币可以作为更广泛的加密资产采用的转折点。

该报告概述了目前使用的不同稳定币格式，它们的相对性能以及对监管环境的深入了解。它还预测了未来几年市场的发展方向。

报告采取了57个活跃的稳定币。

下面是几个核心的图表, 图片来自于报告 blockchain.com：

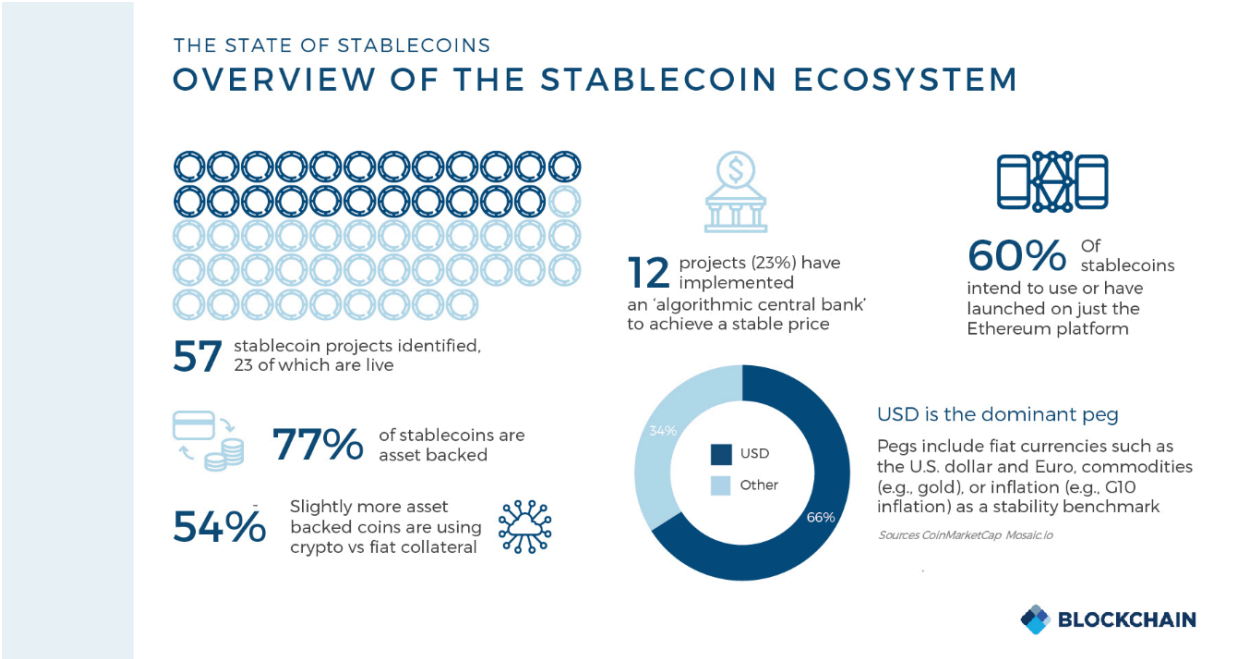
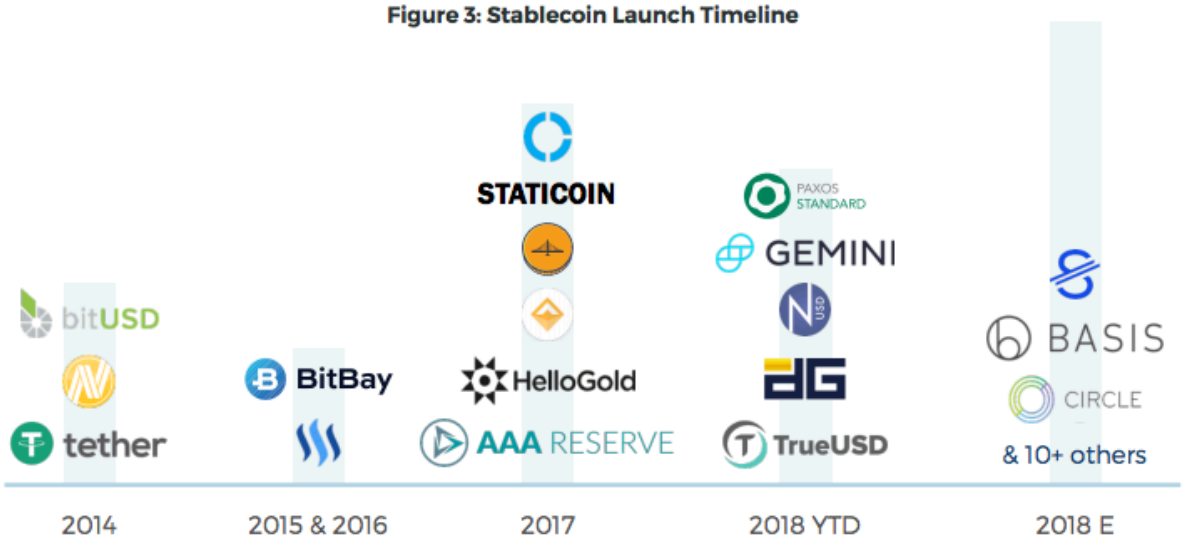


Figure 3: Stablecoin Launch Timeline



STABLECOIN OVERVIEW

		AAA Reserve	Bridgecoin	Digix Gold Token	Gemini Dollar	Globcoin
Overview	Ticker(s)	AAA	BRC	DGX	GUSD	GLX
	Launch Date	2017	Q4 2018	2018	September 2018	TBD
Format	Top-Level Category	Asset-Backed	Asset-Backed	Asset-Backed	Asset-Backed	Asset-Backed
	Sub-Category	Off-Chain Collateral Backed	Off-Chain Collateral Backed	Off-Chain Collateral Backed	Off-Chain Collateral Backed	Off-Chain Collateral Backed
	Collateral	Multi-currency, fixed-income	Fiat, crypto, IPs, physical assets, etc.	Gold	USD	15 fiat pairs & gold
	Reference Peg	G10 Inflation	USD for now	Price of 1g Gold	USD	USD, fiat pairs, gold
Legal Structure	Ownership	Arc Fiduciary LTD	Sweetbridge	DIGIXGLOBAL PTE LTD	Unknown	RCS
	Legal Entity	Non-For-Profit SPV (AAA Fiduciary LTD)	Sweetbridge, Inc.	Public company	Gemini Trust Company LLC	Reserve Currency Solutions SA, AG
	Legal Jurisdiction	Jersey (Bailiwich of Jersey	Switzerland	Singapore	United States	Zug, Switzerland
	Country Location	United Kingdom	U.S. & U.K.	Singapore	United States	Switzerland
	City/State Location	London	Phoenix & London	Singapore	New York, NY	Unknown
Tech	Platform	Ethereum	Ethereum	Ethereum	Ethereum	Ethereum
Investors, Team, & Partners	Investors	BondMason	Crowdsale outside U.S. to users	Global Brain, Fenbushi Capital	Unknown	Unknown
	Funds Raised	$3,000,000	$17,000,000	$1,300,000	Unknown	Unknown
	Partners	Not applicable	Sweetbridge Alliance including Mattereum	ConsenSys, Maker, Blockchain at Berkley, Kyber Network, etc.	Unknown	TBA
	Other Comments	AAA Reserve can only be stored and used via 3 wallets. Exchanges and financial instution partnerships are on their roadmap. There is not a full transparency as to when the product will be functional. They don't have a strong presence on social, they only publish the current exchange rate AAA/USD on Twitter.	Two coin model, BRC is coin for payments, SWC is a loyalty/rewards token	Recently open-sourced code for DigixDAO 1.0: https://github.com/DigixGlobal/dao-contracts	Audit reports (escrow and tech) online: https://gemini.com/dollar/#reports . https://gemini.com/dollar/trailofbits	Bringing stablecoins to the next level. The only coin that marries 15 currencies and gold for a deliberate purpose: to mirror the global economy. The only coin to be based on a proven and well-used model. They have a Swiss base, an experienced currency team, and a proven product.

Read more on here

这篇报告会随后一并发出。

9️⃣Google解除部分禁令，从10月份允许持有合法拍照的交易所在美国和日本发交易平台的广告

Read more on here

🔟Coinbase 宣布加密货币上市新政策，其目的是为符合交易所标准的数位资产加快上市流程。

本週二的 公告 中，Coinbase 表示除了目前提供交易的比特币、比特币现金、以太坊、以太坊经典和莱特币之外，他们也在探索增加几项新资产。

因此，Coinbase 推出 新系统 ，让任何人都可以透过填写表格申请上市加密货币。

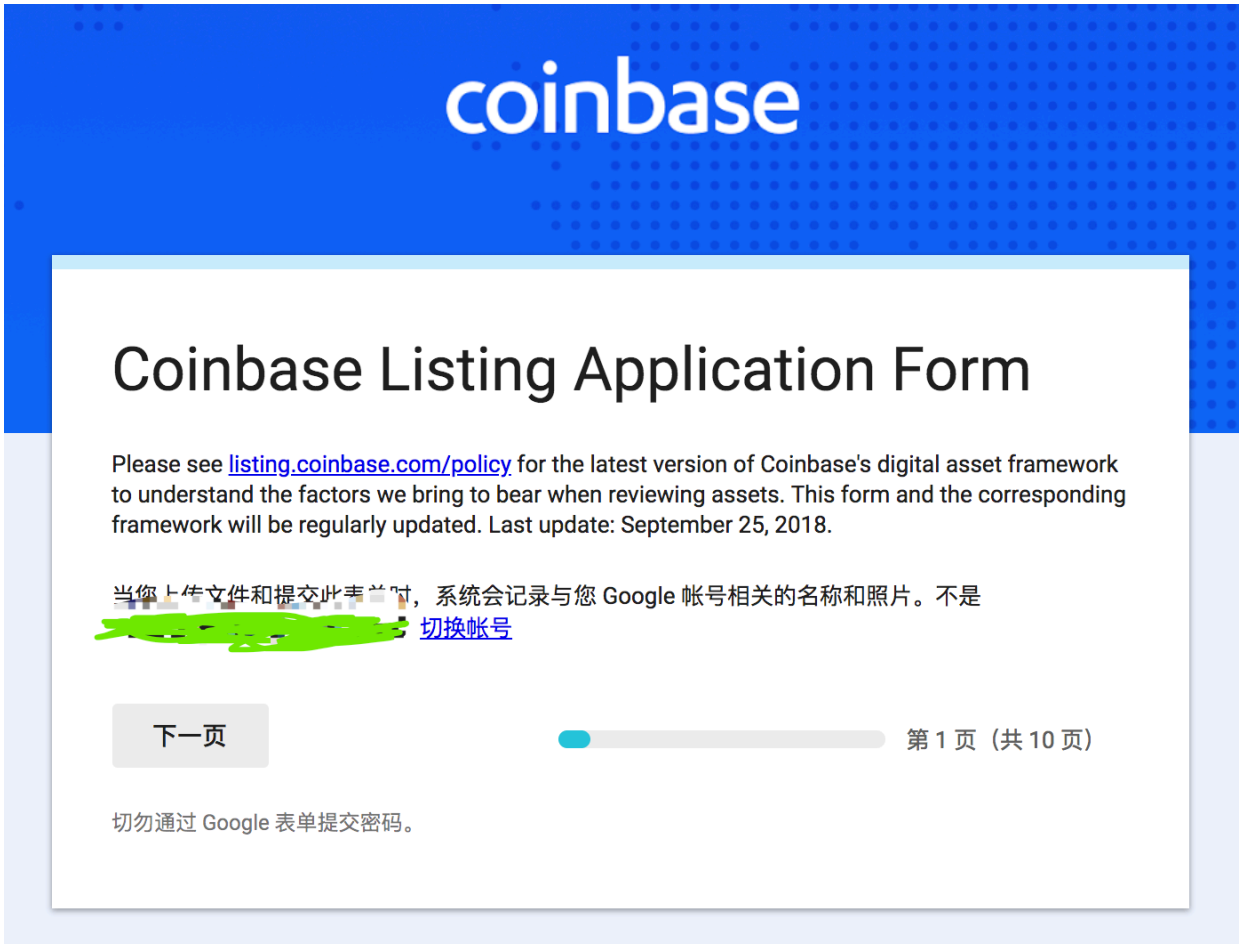
此政策有两项前提—

符合各地司法管辖：这意味着会因地区不同，而仅有在某些地区有特定数位资产。 合乎 Coinbase 数位资产框架： 符合 Coinbase 任务与价值、技术要求、合规、市场供给、市场需求、代币经济。 发行人可以透过简单的注册流程申请，Coinbase 强调将尽速评估流程，也会具体说明批准或拒绝的原因。

关于交易所经常为人诟病的上市费用，Coinbase 表示：

初期并不会有任何申请费用。 根据提交注册的数量，我们保留在未来徵收申请费的权利，以支付与上市新币种的法律评估费用以及操作手续费。

我刚尝试了申请😆



1.Read more on here

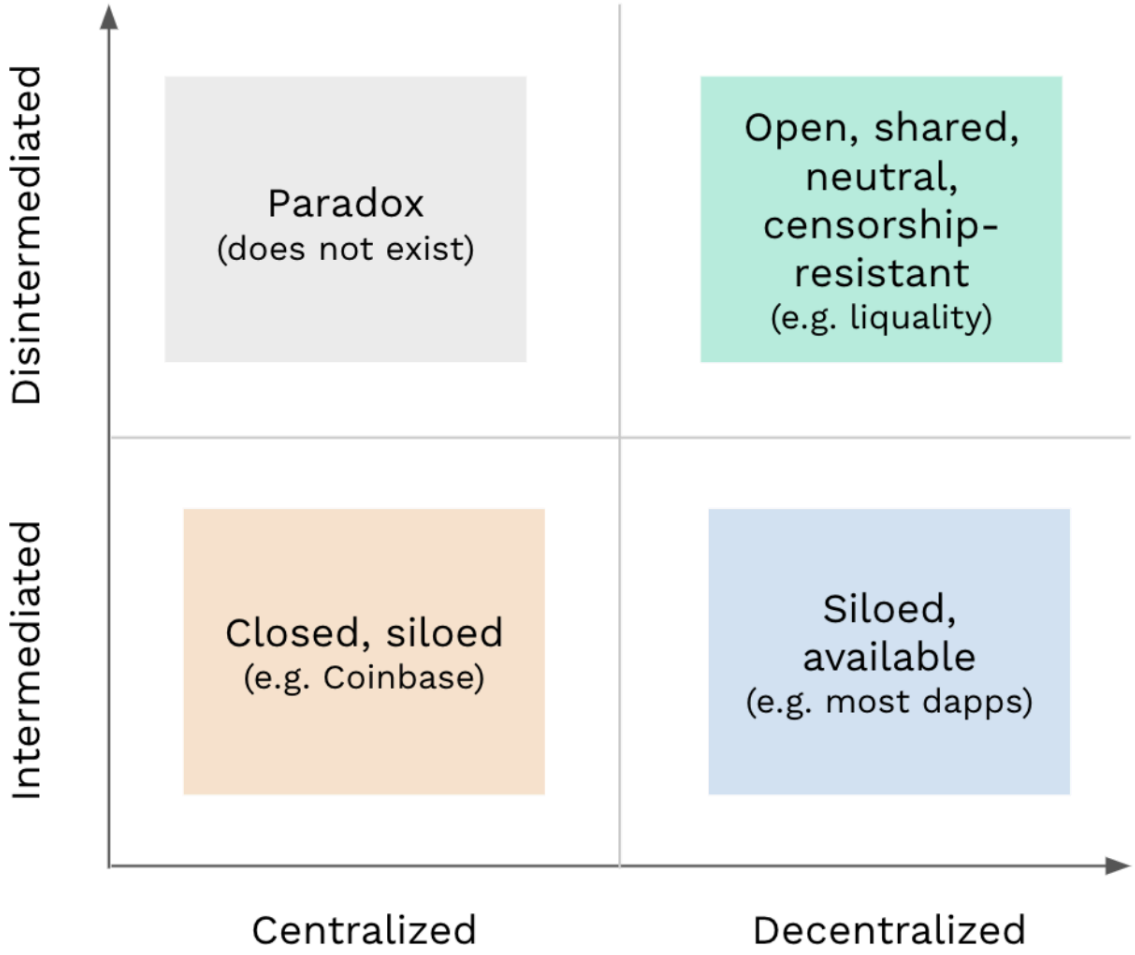
2.coinbase新系统的申请地址

1️⃣1️⃣日本社交巨头Line在发布他们的Token计划之后，发布了两款Dapp

1.4CAST 类似Augur的预测市场平台，包括体育赛事和活动等的预测。https://dappsmarket.net/other/4cast-howtoplay/

2.wizball 共享知识的Q&A平台 https://wizball.io/feed

1️⃣2️⃣Decentralization ≠ Disintermediation



Disintermediation x Decentralization

[img source ->有意思的文章Read more on here]

以上内容由火币大学整理，感谢阅读！日报汇聚地址为：https://github.com/HuobiUniversity/BlockChain_Daily_Report

欢迎大家star&watch!