



推动时代变革的高速异步DAG公链

Jeff Zhou, Trustnote Founder

Email: Jeff.zhou@trustnote.org

Telegram: <https://t.me/jeffzh>



Wechat: zhengjun0480



Blockchain Decoded

A transaction between 2 parties occurs

ENCIPHERMENT

Security Code

LEDGER

John 25
Mark 15

VALIDATION

The code of the transaction is sent to a large network where the authenticity of the code is confirmed without compromising private information and eliminating the need for a central authority for confirming transactions

DISTRIBUTION

LEDGER

John 25
Mark 15

Once a transaction is confirmed and validated by several parties, it exists on the ledger of each as a permanent and immutable record of the transaction

The transaction information is recorded in a public ledger and the transaction is completed

The diagram is divided into two main parts: "Connection of Blocks" and "Collection of Transactions".

Connection of Blocks: This part shows three blocks in a chain, labeled "Block 1 Header", "Block 2 Header", and "Block 3 Header". Each block header contains a "Hash value of Previous Block Header" and a "Root of Hash Tree". The blocks are connected sequentially, with a "10分" (10 minutes) interval between them. The "Hash value of Previous Block Header" in Block 2 is the hash of Block 1's header, and similarly for Block 3. Each block also contains a list of transactions: "TX1-1", "TX1-2", "TX1-n" for Block 1; "TX2-1", "TX2-2", "TX2-n" for Block 2; and "TX3-1", "TX3-2", "TX3-n" for Block 3.

Collection of Transactions: This part shows a hierarchical structure of transactions. At the bottom, individual transactions are listed: "Coinbase T", "TX2-1", "TX2-2", "...", and "TX2-n". These transactions are grouped into a "Hash Value" box. This process is repeated, with multiple "Hash Value" boxes being hashed together to form a single "Hash Value" box at the top, which then points to the "Root of Hash Tree" in the block header.

什么是DAG (Directed Acyclic Graph)

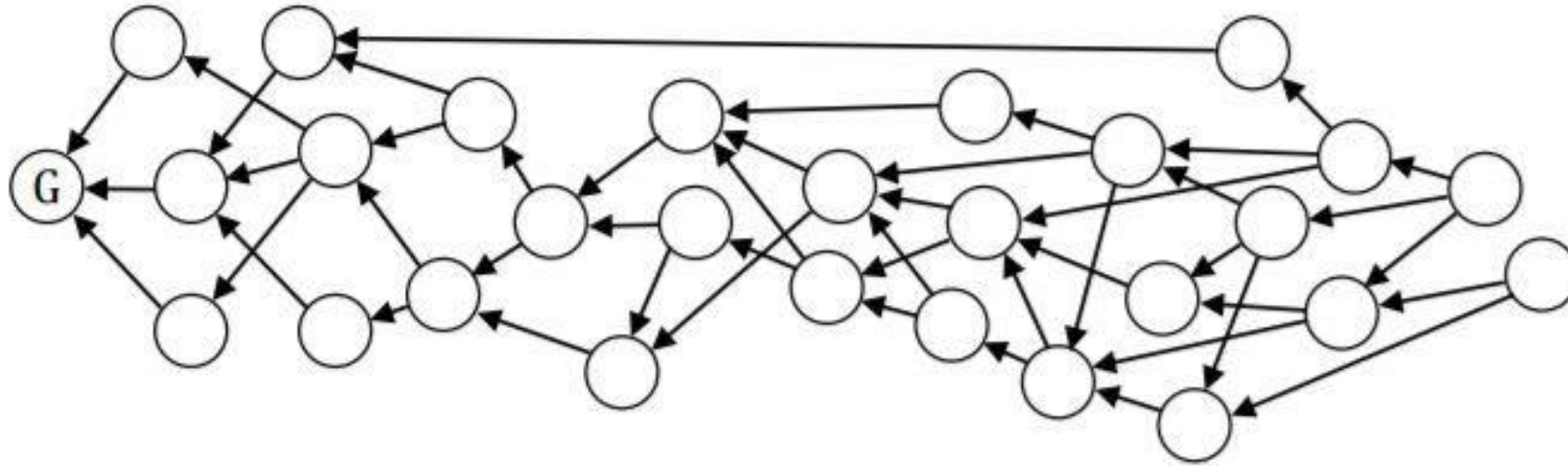


Figure 1. Storage units connected into a DAG. Arrows are from child to parent, G is the genesis unit.

Peer selects referenced transaction unit by itself, verify the reference transaction unit, the graph gets partial order

DAG利用节点间的引用校验的方法构建节点间的信任网络
区块链和DAG账本都是分布式账本技术



人类信任体系的革命





■ 并发能力是当前区块链的最大问题

- 比特币区块扩容和隔离见证的激烈争论, BTC vs BCH
- CryptoKitties 导致ethereum network 拥堵
- 比特币和以太坊的交易费太高
- 过低的并发能力导致以太坊难以被用于大规模用户应用
- Scalability问题阻碍了区块链技术真正被广泛使用



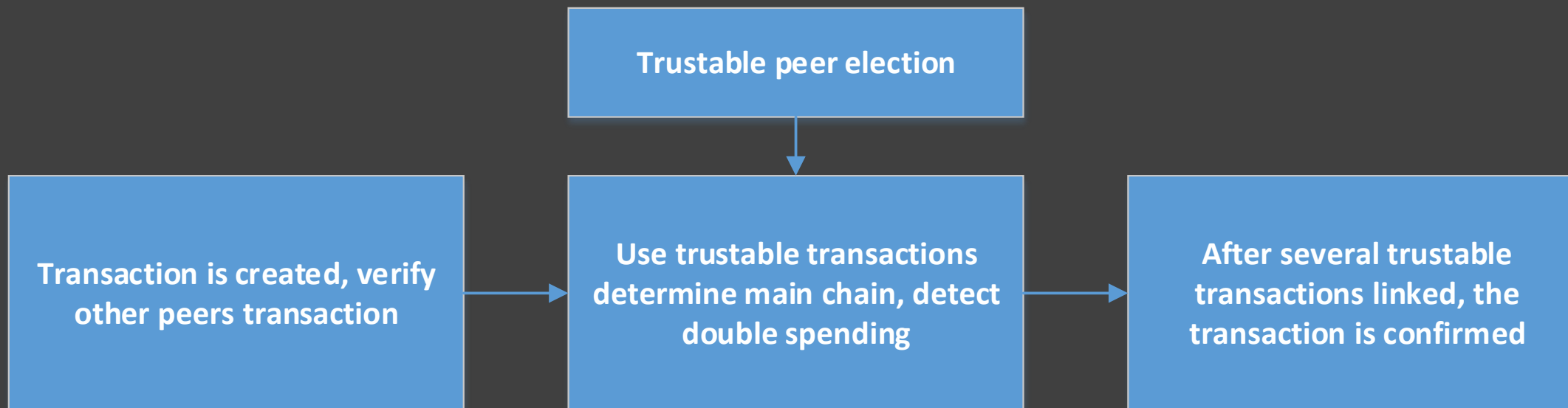
为什么区块链扩展性不好



- 每个时刻只能有一个矿工修改账本数据库
- 为了检测和防止“双花”，矿工做了太多的工作，从而成为瓶颈
- 基本上，区块链是一个分布式同步数据库，在每个区块周期，整个网络的 transactions 都是阻塞的。
- 区块时间和区块最大尺寸基本决定了TPS和transaction延迟时间



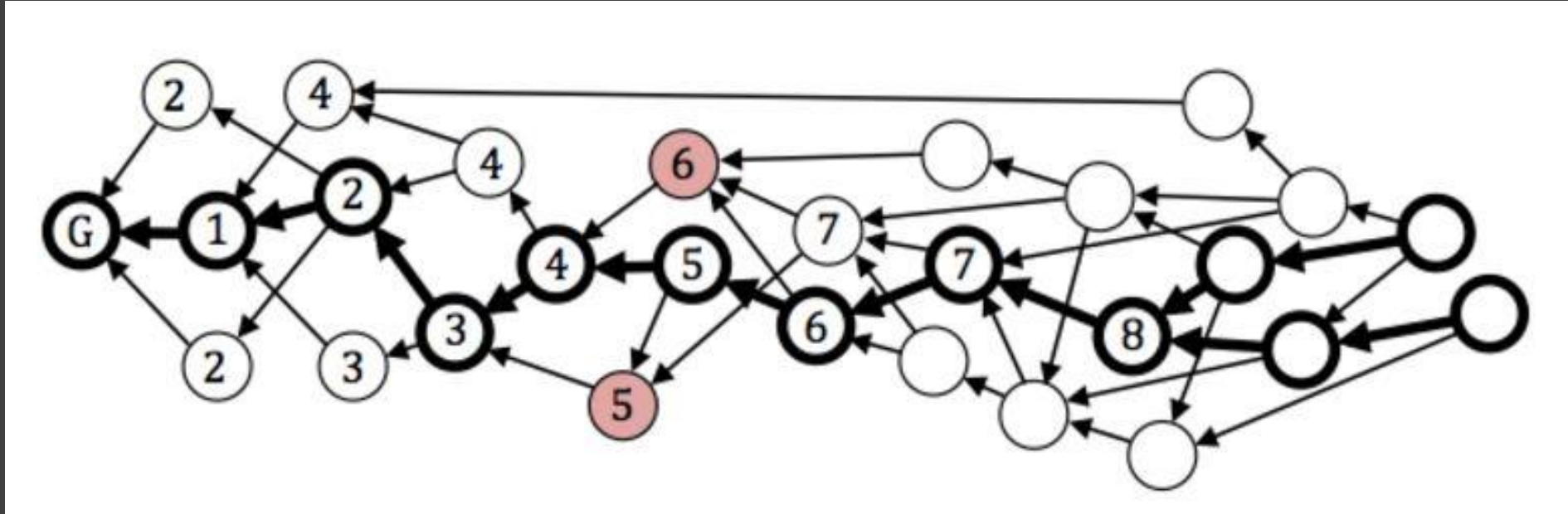
DAG 是解决并发问题的答案



- DAG使得网络节点可以并行验证transactions
- DAG是一个分布式异步数据库，区别于区块链
- Transaction验证和可信节点选择和双花检测被分开、被解耦可以并行进行，大大提高了DAG的并发能力



■ DAG如何检测“Double Spending”



If the main chain is determined, the graph gets total order

Main chain is comprised of the transaction unit send out by
“trustable peer”



■ DAG为什么高速

- DAG 是无阻塞的，无区块的，使用transaction为单位记账，记账颗粒度更细
- 并行引用、并行验证交易，真正释放了p2p网络的潜力
- 交易验证、信任节点选举和双花检测分离进行，并行展开
- 两个阶段完成验证工作
 - Partial order phase: transactions are verified and written
 - Total order phase: use trustable transactions determine main chain, then detect double spending
- DAG ledger的TPS是无限的，节点越多速度越快
- Transaction可以被任何邻居节点的交易快速验证



■ 其他DAG账本项目的问题

- 如何公平地选择可信赖节点？
 - This is like committee election of real world
 - This is key part of DAG ledger's consensus process
- 在没有正常交易发生的时候，如何发送辅助交易来协助验证？
 - The last transaction keeps unconfirmed if no new transaction happen.
- IOTA 使用Coordinator作为可信节点
- Byteball 使用12 witnesses作为可信节点
- IOTA和Byteball都不够公平、不够安全



Trustnote把DAG和PoW结合在一起

- Trustnote实现了一个双层分布式网络，包括超级节点和其他节点
- Trustnote使用Proof of Work公平选择可信超级节点，超级节点构成第一层网络
- PoW挖矿激励Super Node持续可信
- 超级节点发送coinbase transaction构成main chain
- 因为使用PoW选择可信节点，Trustnote比其他DAG链更可信安全
- 双层网络结构使得TrustNote更具有扩展性
- Super Node可以实现更多服务功能服务于轻钱包节点



■ Trustnote 针对高流量大规模App设计的

- DAG技术的使用使得Trustnote高速高并发
- Trustnote是第一个可以挖矿的DAG ledger, PoW算法是的TrustNote安全公平
- Trustnote 支持多种节点类型, 轻钱包支持手机App, 微钱包支持IoT设备
- Trustnote实现一种轻便的声明式智能合约, 更安全更高效



■ Light wallet 对大规模普及非常重要

- 许多区块链项目的钱包都太大了，无法手机安装
- 通过网站对接的手机钱包有安全隐患
- 在设计区块链底层的时候就要考虑到轻钱包协议设计
- Trustnote 已经Mobile and IoT ready

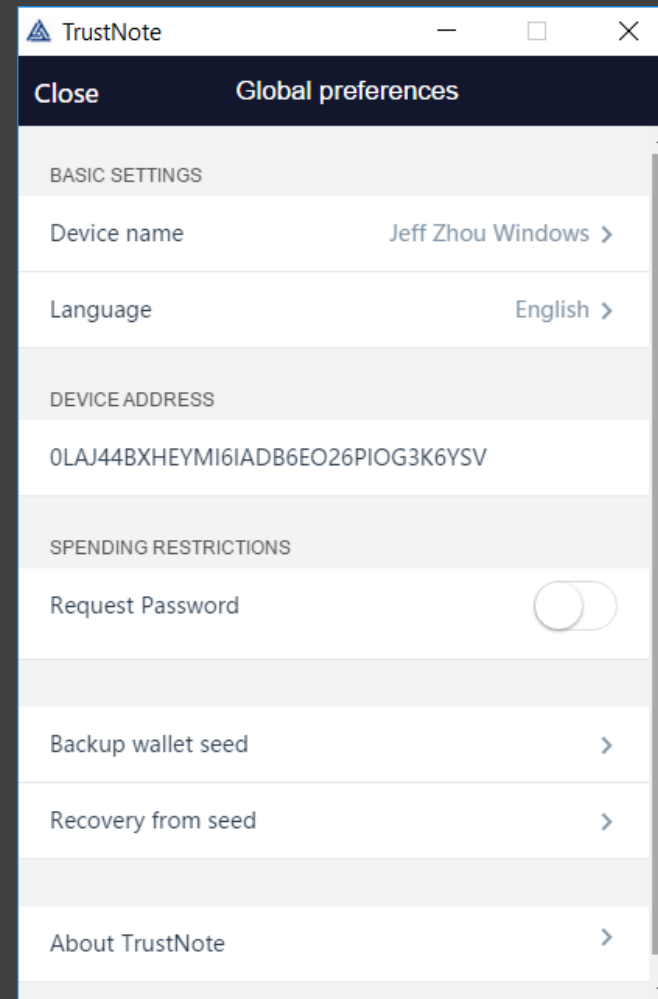
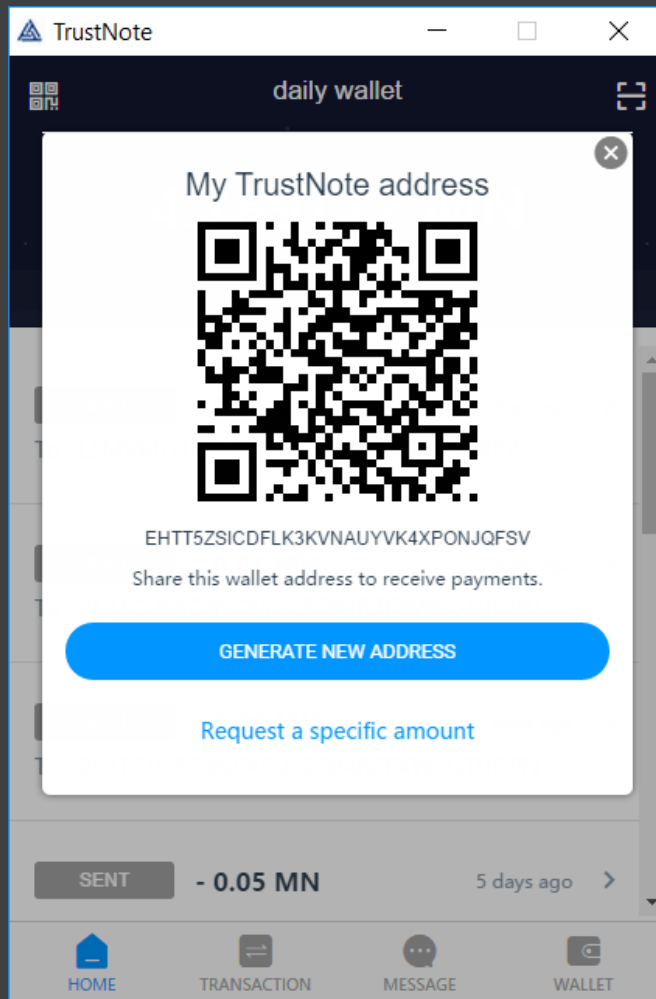
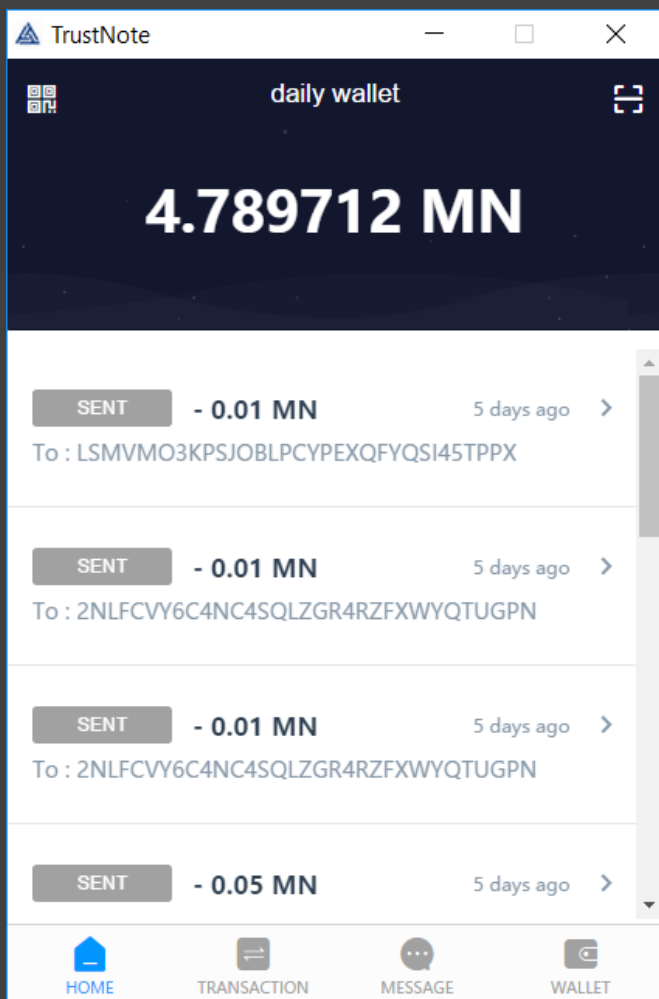


Trustnote的四种节点类型

- Super Node超级节点
 - Designed for server
 - Saves full DAG ledger database
 - Do PoW mining, send out main chain transactions
 - Support light client protocol, serves light node
 - Support micro client protocol, serves micro node
- Full Node全节点
 - Designed for PC
 - Saves full DAG ledger database
 - Support light client protocol, serves light node
- Light Node轻节点
 - Designed for mobile apps
 - Doesn't save full ledger, only save related transactions data
- Micro Node微节点
 - Designed for IoT devices
 - Uses micro client protocol access DAG ledger database



Trustnote Wallet 演示





Trustnote的轻量化智能合约

- 基于Byteball智能合约系统，Trustnote实现了轻量化声明式智能合约
- 声明式智能合约表达合约结果，而不描述合约如何实现
- Trustnote提供一个图形工具定义contract
- Trustnote将来会发布新的合约语言，保证安全、易用的同时提高表达能力和性能
- Trustnote合约系统不追求图灵完备，而是聚焦在痛证和数字资产领域，更关注安全易用



■ Trustnote的使用

- 快速Token发行，Trustnote将开发一个Token平台，用户无需编程就快速发行Token，而且和Trustnote主钱包打通
- 钱包内置交易所功能，支持去中心化OTC交易所的同时支持和大的中心化交易所对接
- 极轻极速可信赖的特点使得Trustnote成为目前唯一适合大型在线游戏和社交网络App的公有链
- Trustnote将真正释放P2P网络潜能、真正可以被主流消费端App使用的分布式账本



■ 一切都将代币化

- 每个企业、每个人都将发行自己的Token
- Token+实物商品将组成新的可流转可分割可跟踪资产
- Token将大大提高世界的价值流动性
- 万物互联时代，一切联网设备都会有内置钱包
- AI和大数据的变现时代将由区块链技术来开启
- 中心化服务机构将成为链接分布式账本公有链的价值网关
- 监管机构、中心化服务机构将最终和分布式账本和谐共处



企业如何应对区块链技术变革？

区块链在B端业务落地的三个层面：

- 数据防篡改相关业务：
 - 版权管理
 - 数据保全
 - 公证业务
 - 金融征信
 -
 - 商业业务/过程的智能化
 - 电子合同
 - 票据对账
 - 资产租赁过程管理
 - 供应链金融
 -
 - 资产流转相关业务
- 分析价值链和信任关系把握新时代方向
 - 寻找信任平台、寻找主导新时代生态的机会
 - 寻找信任网关的机会，或者调整角色做好信任网关服务
 - 提早培训储备新的信任体系、新的商业模式下的市场、运营和技术人才
 - 拥抱生态，尽早以公有链、联盟链思维做好战略布局
 - 技术研发上要拥抱开源软件开发模式



加入telegram体验TTT



Download TTT wallet at Homepage:
<https://trustnote.org>



Telegram English group:
<https://t.me/TrustNoteOfficial>



Telegram Chinese group :
<https://t.me/TrustNote>