当Graphene邂逅IoT

neomabao

Jan.2018

2018年中国石墨烯开发者大会

01 昨夜西风凋碧树，独上高楼，望尽天涯路。

2018年中国石墨烯开发者大会

IoT & Blockchain

物联网（Internet of Things，a.k.a IoT）是互联网、传统电信网等资讯承载体，让所有能行使独立功能的普通物体实现互联互通的网络。-- wikipedia

- Gartner预计到2020年将有204亿“Things”实现互联互通
- 工业4.0，中国制造2025
- 未来城市

区块链（blockchain 或 block chain）是用分布式数据库识别、传播和记载信息的智能化对等网络, 也称为价值互联网。-- Wikipedia

- 比特币（Bitcoin），PoW
- 以太坊（Etherrum），PoW -> PoS
- 比特股（Bitshares），dPoS <- Graphene

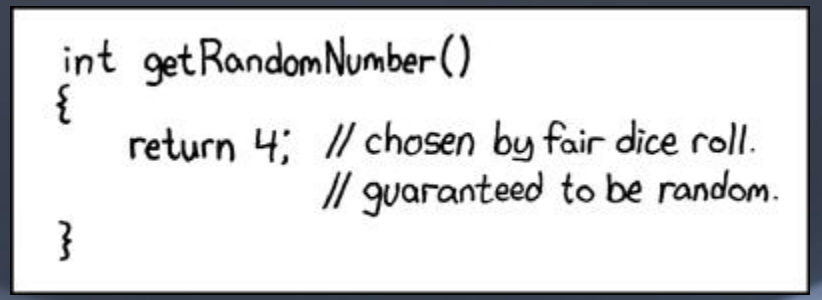
dPoS

被Bitshares，Steem等采用，多年稳定运行

- 被证实为更加健壮、安全、高效
- 大多数生产者失败，仍继续工作
- 1.5秒出块
- 99.9%的确定性

SafeCurve

- NIST P-256
  - y^2=x^3-3x+41058363725152142129326129780047268409114441015993725554835256314039467401291
  - modulo p = 2^256 - 2^224 + 2^192 + 2^96 - 1
- Secp256k1
  - y^2 = x^3+0x+7
  - modulo p = 2^256 - 2^32 - 977
- Curve25519
  - y^2 = x^3+486662x^2+x
  - modulo p = 2^255 - 19

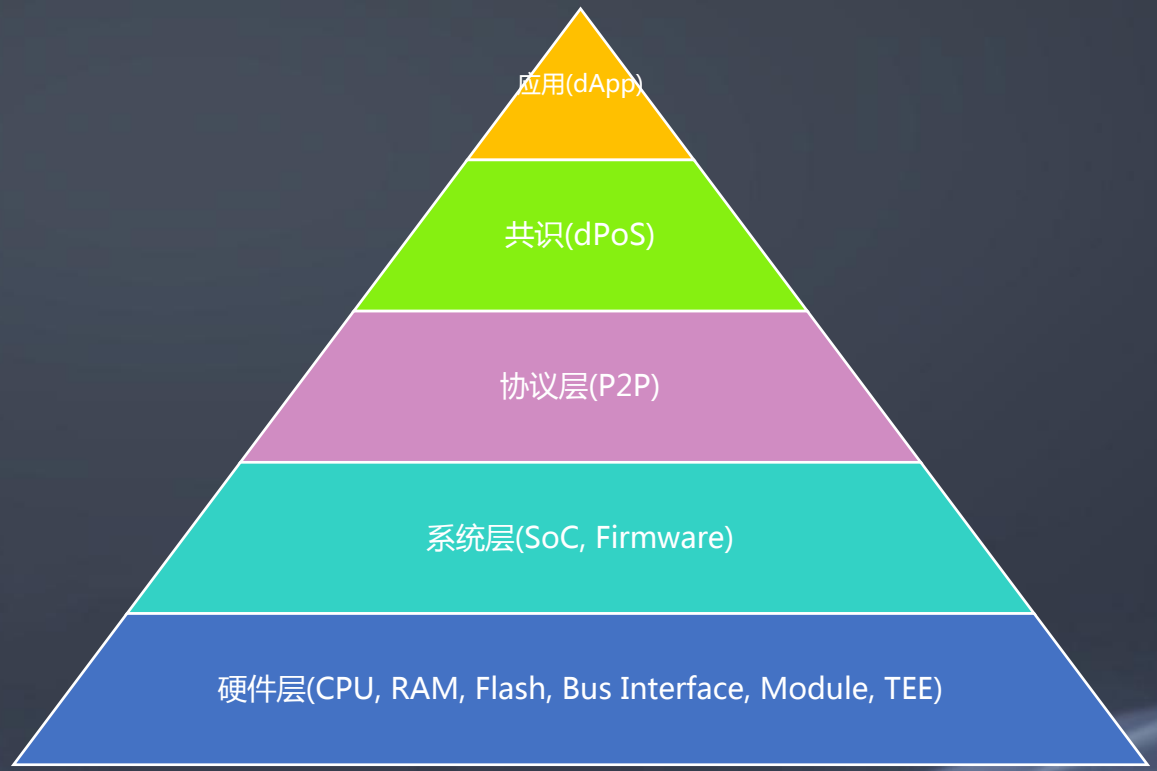


02 衣带渐宽终不悔，为伊消得人憔悴。

2018年中国石墨烯开发者大会

Trust of chain, chain of trust

- 信任根
  - 硬件?
  - 软件?
  - 第三方?
- 随机数
  - Entropy（熵）
  - “真”随机数发生器
  - EaaS
- 完整性
  - 签名
  - 哈希



Hardware Wallet

- TEE（SE，TPM，Trust Zone）
- 交互 vs 非交互
- 账户/钱包/币种管理
- 软硬件/Firmware升级
- 防丢，防黑，防意外
- 找回

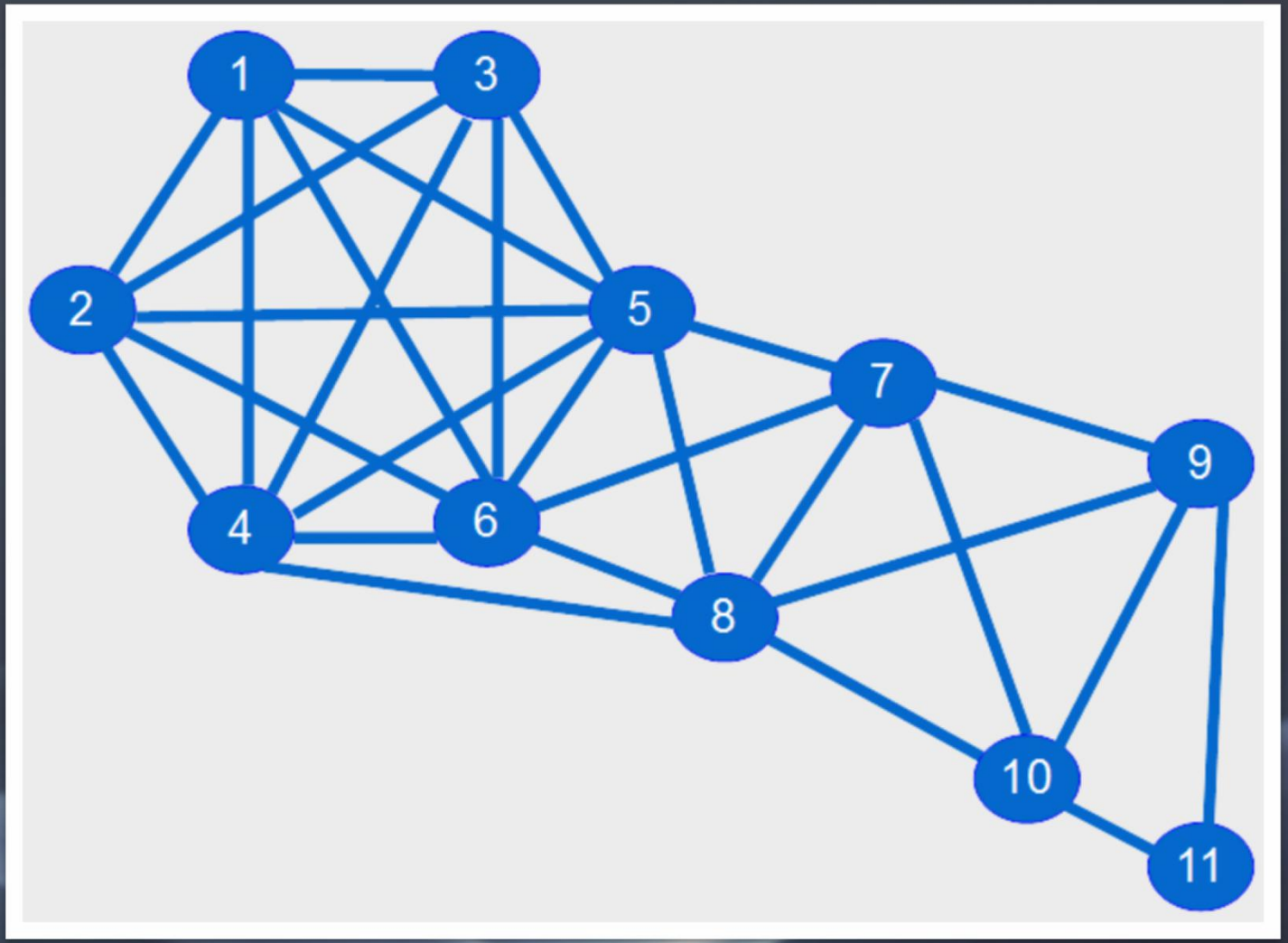
03

众里寻他千百度，蓦然回首，
那人却在灯火阑珊处。

2018年中国石墨烯开发者大会

Zone

- 局域寻址方式
- 善用Merkle tree
- 微支付
- M2M支付
- “边界节点”
  - 权限
  - 能力
  - 公私钥对
  - 冗余



Smart Contract

- 图灵完备?
- “容器”(Stack，vm，docker...)
- 开发者环境
- 安全审计(logic，stackoverflow...)
- 使用成本

Me

2018年中国石墨烯开发者大会

马宝春（Neo）

技术极客，浙江大学应用电子本科，复旦大学微电子硕士。曾就职于GE，台达电子等知名企业，长期从事各类电子产品的研发到量产工作，并参与多个高端智能硬件初创公司的建立与开拓 。具有15年硬件设计、生产相关经验，20年应用密码学实战经验。万向创新聚能城全球区块链挑战赛智能终端类第二名。


THANKS!
2018年中国石墨烯开发者大会