解密区块链的力量

杨晓春 上海成趣信息科技有限公司

- 如何解决数字世界的信任问题?
- 区块链如何建立起去中心化的信任?
- 区块链1.0：比特币的原理是怎样的?
- 区块链2.0：智能合约是怎样的?
- 创新的比特币系统是如何运行的?
- 区块链的交易流是怎样的?
- 如何解决拜占庭将军问题?
- 区块链分类法是怎样的?
- 区块链有哪些核心问题？（如延迟、吞吐量、可扩展性、安全性，数据透明性与隐私）
- 如何实现保护私有区块链访问权限的责任?
- 区块链有哪些挑战？如共识机制
- 区块链如何推动更多的应用?
- 区块链有哪些行业应用?
- 区块链有哪些开源框架?

In What We Trust?

Lionel M. Ni 倪明选
University of Macau

拜占庭将军问题

- 是由莱斯利·兰波特在其同名论文[1]中提出的分布式对等网络通信容错问题。

- 在分布式计算中，不同的计算机通过通讯交换信息达成共识而按照同一套协作策略行动。但有时候，系统中的成员计算机可能出错而发送错误的信息，用于传递信息的通讯网络也可能导致信息损坏，使得网络中不同的成员关于全体协作的策略得出不同结论，从而破坏系统一致性。拜占庭将军问题被认为是容错性问题中最难的问题类型之一。

- 一组拜占庭将军分别各率领一支军队共同围困一座城市。为了简化问题，将各支军队的行动策略限定为进攻或撤离两种。因为部分军队进攻部分军队撤离可能会造成灾难性后果，因此各位将军必须通过投票来达成一致策略，即所有军队一起进攻或所有军队一起撤离。因为各位将军分处城市不同方向，他们只能通过信使互相联系。在投票过程中每位将军都将自己投票给进攻还是撤退的信息通过信使分别通知其他所有将军，这样一来每位将军根据自己的投票和其他所有将军送来的信息就可以知道共同的投票结果而决定行动策略。

- 问题：将军中可能出现叛徒，他们不仅可能向较为糟糕的策略投票，还可能选择性地发送投票信息。假设有9位将军投票，其中1名叛徒。8名忠诚的将军中出现了4人投进攻，4人投撤离的情况。这时候叛徒可能故意给4名投进攻的将领送信表示投票进攻，而给4名投撤离的将领送信表示投撤离。这样一来在4名投进攻的将领看来，投票结果是5人投进攻，从而发起进攻；而在4名投撤离的将军看来则是5人投撤离。这样各支军队的一致协同就遭到了破坏。

- 由于将军之间需要通过信使通讯，叛变将军可能通过伪造信件来以其他将军的身份发送假投票。而即使在保证所有将军忠诚的情况下，也不能排除信使被敌人截杀，甚至被敌人间谍替换等情况。因此很难通过保证人员可靠性通讯可靠性来解决问题。

POW

PBFT

- Practical Byzantine Fault Tolerance

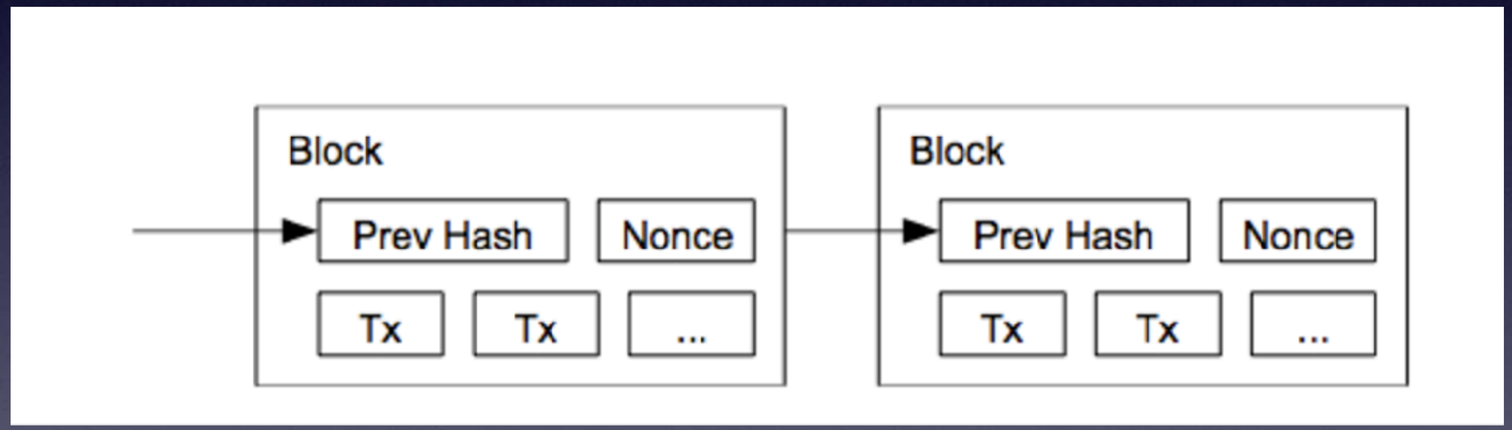
智能合约

- 不只是一个可以自动执行的计算机程序：它自己就是一个系统参与者。它对接收到的信息进行回应，它可以接收和储存价值，也可以向外发送信息和价值。
- 这个程序就像一个可以被信任的人，可以临时保管资产，总是按照事先的规则执行操作。
- 一段代码（智能合约），被部署在分享的、复制的账本上，它可以维持自己的状态，控制自己的资产和对接收到的外界信息或者资产进行回应。

Throughput

挖矿

- 即不断接入新的Block延续Block Chain的过程



区块链的特点

- 无需中介参与
- 过程高效透明且成本很低
- 数据高度安全

主要应用领域

主要应用领域	应用前	应用后
金融业 （银行、支付转账、股票交易等）	流程复杂；中心化数据存储；第三方担保	简化流程； 分布式数据存储，安全性提升； 无需第三方，降低成本
网络安全	中心服务器存储数据、转移和传递	信息传播路径改变，不可拦截
身份信息管理	银行、信用卡身份识别过程繁琐； 身份信息易被盗用	简化识别过程； 加强身份信息
公证	需要政府、公信力第三方提供背书	数学加密做信用背书，自动完成公证； 永久保存资料
投票	计票可能存在伪造； 选民身份信息保护环节较弱	过程全网公开； 选票可追溯； 选民身份保密性好
供应链	低效、产品作假、低质量风险高	供应链各环节诚信保证高； 产品信息可追溯，质量可保证

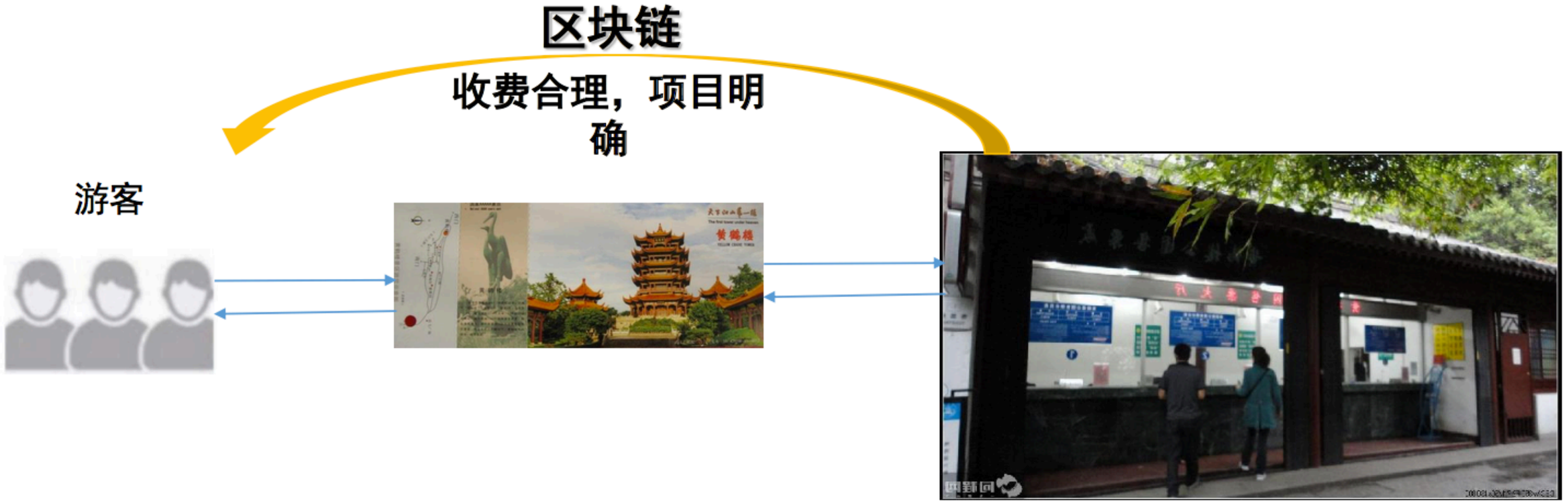
区块链如何推动更多的应用?

区块链在保险上的应用

保险公司面临的机遇	考虑事项
促进单一审计跟踪及提高透明度的特定数字身份管理	▸ 针对每项交易提供含有充分的个人隐私的公开或私有账本（分散式、加密身份管理系统） ▸ 对网络或移动设备补充数字身份验证和认证 ▸ 更加符合隐私法律法规 ▸ 落实数据保护和敏感数据的隐私
分布式基础架构	▸ 减少对集中式市场基础架构的依赖性 ▸ 产生对新法规和控制的需求 ▸ 可增加保险公司和经纪人的责任（无需明确的解决方案） ▸ 可能基于现有模式减少对政府和监管机构的透明度和控制
生态系统的可扩展性	▸ 适应当地条件且扩展至全球范围，同时加速地区化和个性化产品的分销（按地区、客户群和无保险产品的地区划分） ▸ P2P保险
欺诈与安全	▸ 区块链在技术无关性层面运行 ▸ 供应商、企业、系统和服务之间的相互作用在数据生命周期（甚至在过去）的任何时间点均具有透明度且可验证 ▸ 减少欺诈，从而减少涉及的相关方面的结算时间 ▸ 取消文书工作 ▸ 向各方提供更简便优化的数据存取

自动化	▸ 区块链技术能够实现基于时间的交易和服务 ▸ 可支持脚本化、可编程交易的数字原始系统
创新	▸ 促进获取及时且准确的大数据资源 ▸ 允许向市场引入新风险工具和资本机遇 ▸ 允许提供更多复杂形式的自保和新定制的保险产品 ▸ 分布式的风险相互化可支持有效的理赔管理和减少欺诈
数据池的机遇	▸ 在数据由多方共享的交易（配售和理赔）中，是否能够获取单一且实时的数据资源将改变买方的管理方式和为风险筹资的方式，并且还能使保险公司对理赔追偿进行定价和管制
技术中性化/无关化 一般法律和监管合规	▸ 在实际情况中要确保遵循任何国际数据保护法律法规（但是，是否需要市场监管和信任度以扩展技术，仍有待确定）

旅游



- 消费款项透明，保险等款项可以自由选择，避免旅行社欺骗消费者，出现额外收费的情况
- 导游信息记录在链，根除宰客行为

区块链有哪些开源框架?

名称	公识算法	适合场景	开发语言	智能合约	TPS
比特币1.0	POW	公链	C++	否	7
以太坊ETH 1.0	POW	公链/联盟链	GO	是	25
IBM HyperLed-ger fabric	PBFT为主	联盟链	GO	是	100K
比特股BitShare	DPos	联盟链	C++	否	500
公证通Factom	Factom自有共识机制，类Pos	公链/联盟链	C++	否	27
瑞波Ripple	RPCA	公链/联盟链	C++	否	1000
未来币NXT	Pos	公链/联盟链	JAVA	否	1000

MS的Coco(confidentialconsortium)

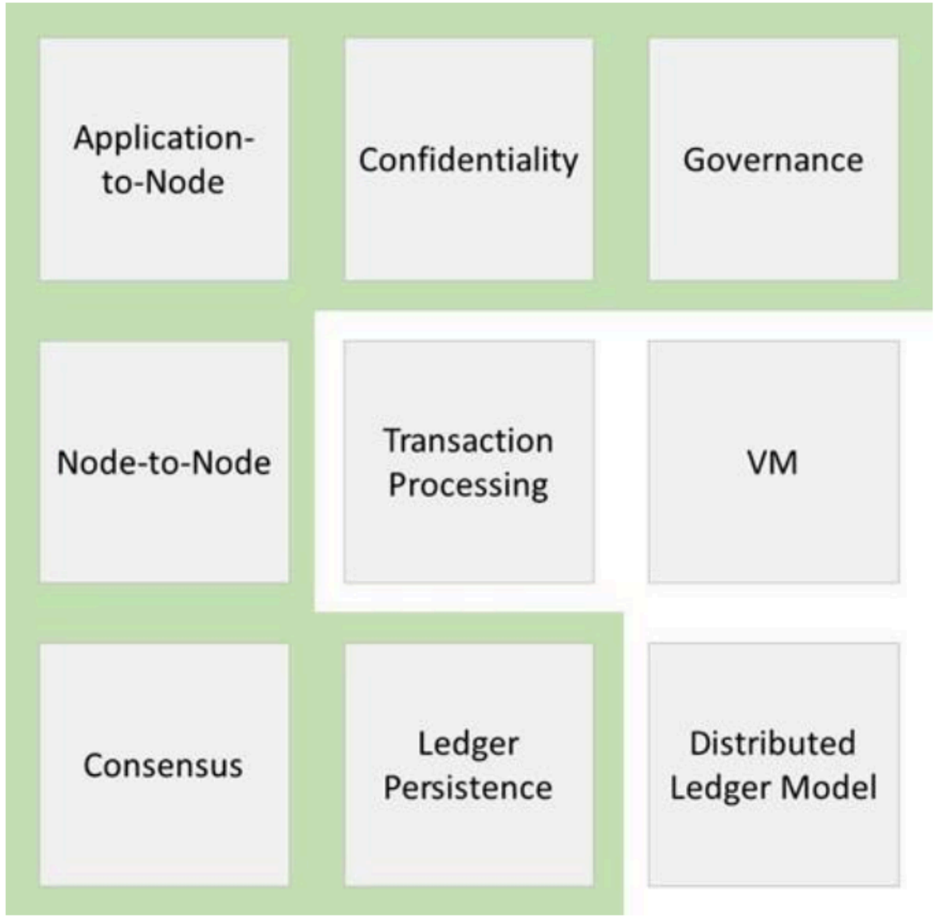


Figure 2: Logical components of a blockchain protocol (Coco components are shaded in Green).

confidentialconsortium

参考资料

- http://8btc.com/ 巴比特社区

ACM-W China

支持、庆祝和倡导中国女性充分
参与计算领域的各个方面

DevHub开发者社区

分享、启发、探索

传播IT知识文化
陪伴探索者前行

杨晓春
上海成趣信息科技有限公司
独立顾问

产品设计
技术开发、技术管理
人工智能、数据分析解决方案
物联网解决方案
医疗养老产品
DevHub开发者社区