区块链基础

灵宗, 博士
ibm almaden 研究中心
美国加利福尼亚州圣何塞

Blockchain Ecosystem

"比特币"与区块链

议程

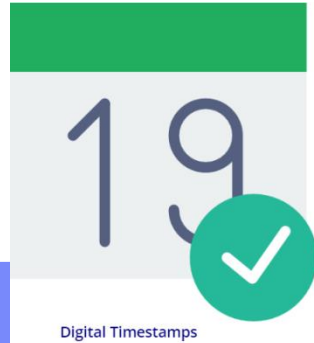
- 什么是区块链技术?
- 区块链是如何工作的?
  - 交易的独立验证
  - 已验证事务的聚合
  - 区块的挖掘
- 如果有人试图破解系统怎么办?

什么是区块链技术?

*区块链是一个**分散分布式数据库**不可变的记录, 其中事务是由强大的保护**加密算法**网络状态由**共识算法**.*

什么是区块链技术?

- 简单地说，区块链是一个包含信息的区块链。
- 这项技术最初的描述是在**1991年**并打算***时间 戳****数字文件*以避免任何记录的回溯或回火。
- 无论这项技术多么伟大，直到中本佐藤利用它创造了数字加密货币，它的真正潜力才得以实现***"比特币"***。



议程

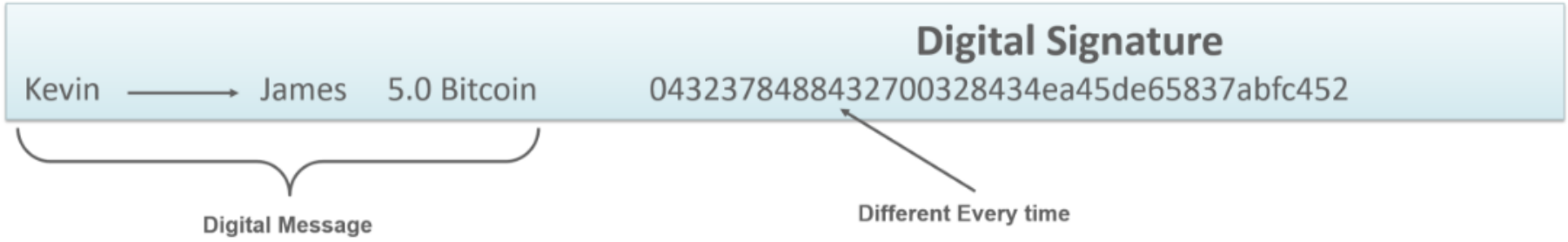
- 什么是区块链技术?
- 区块链是如何工作的?
  - 交易的独立验证
  - 已验证事务的聚合
  - 区块的挖掘
- 如果有人试图破解系统怎么办?

区块链是如何工作的?

让我们尝试了解区块链是如何在区块链网络上处理简单事务的。

区块链是如何工作的?

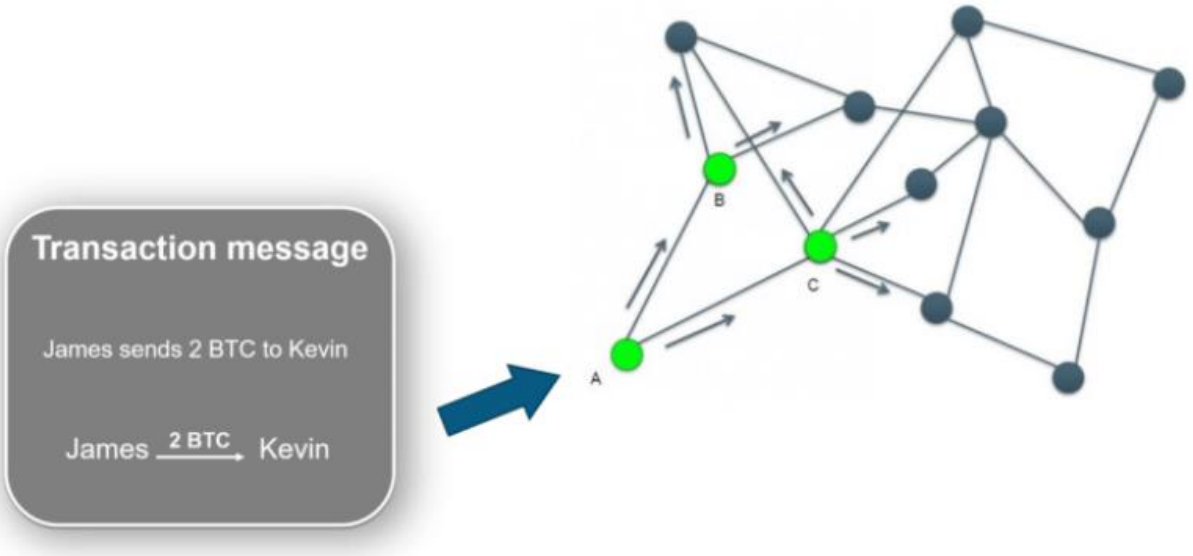
假设詹姆斯想发送**5 btc**给他的朋友凯文现在，此事务以***数字消息。***



数字消息具有唯一的签名。就像你的签名提供了文件所有权的证明一样**数字签名**提供了证据，证明**交易是真实的。**

区块链是如何工作的?

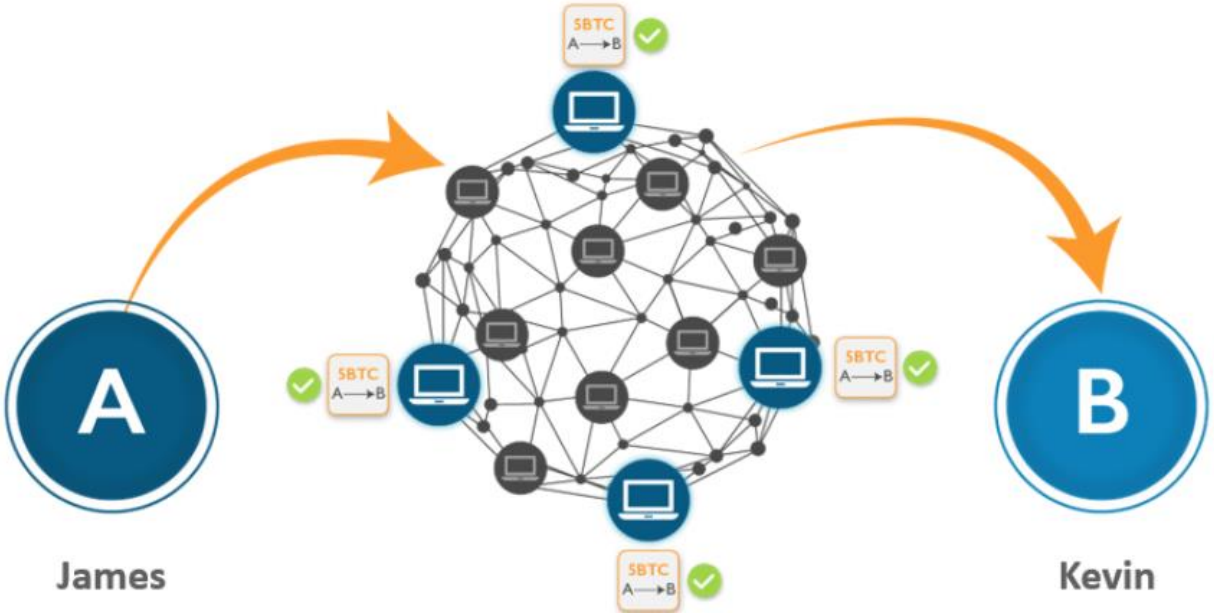
现在, 这个生成的事务被广播到它传播的网络***点对点。***



假设上述事务首先由**节点 a**在网络中。

交易的独立验证

在将事务发送到其邻居之前，获取交易记录的每个比特币节点最初将验证该事务。

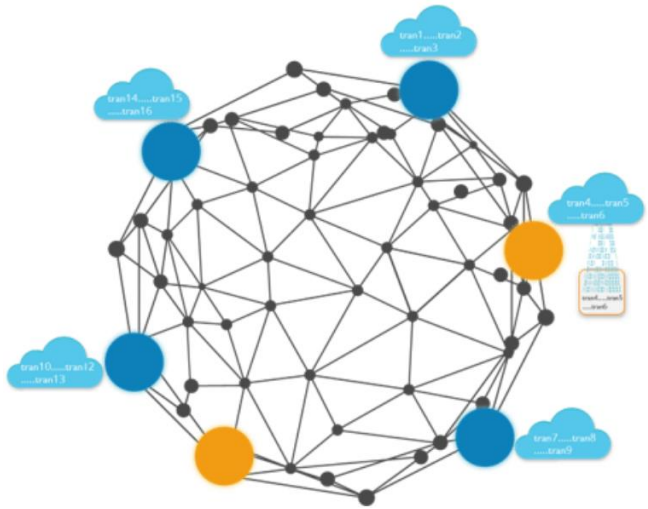


这保证只有有效事务在系统中传播，而无效事务在接收它们的第一个节点上被释放。每个节点都根据一长串的标准来确认每个事务。

Aggregation of Verified Transactions

Independent aggregation of those transactions into new blocks by mining nodes combined with exhibited calculation through a proof-of-work algorithm.

- By autonomously confirming every transaction as it is received and before propagating it, each node fabricates a pool of valid (however unconfirmed) transactions known as the **transaction pool, memory pool or mempool**
- Transaction reaches **Mining nodes** it collects, validates, and relays new transactions just like other nodes
- Unlike other nodes, miner node will then aggregate these transactions into a ***candidate block***



已验证事务的聚合

假设安迪是个矿工。(挖掘节点维护区块链的本地副本, 即自2009年比特币系统启动以来创建的所有块的列表)

Andy's node is listening for transactions, trying to mine a new block and also listening for blocks discovered by other nodes

As Andy's node is mining, it receives block (say 273816) through the bitcoin network. The arrival of this block signifies the end of the competition for the block

During the previous 10 minutes, while Andy's node was searching for a solution to block (273816) , it was also collecting transactions in preparation for the next block (273817)

By now it has collected a few hundred transactions in the memory pool

Upon receiving block (273816) and validating it, Andy's node will also check all the transactions in the memory pool and remove any that were included in block (273816)

Whatever transactions remain in the memory pool are unconfirmed and are waiting to be recorded in a new block

Andy's node immediately constructs a candidate for block (273817) . This block is called a **Candidate Block** because it is not yet a valid block, as it does not contain a valid proof of work

The block becomes valid only if the miner succeeds in finding a solution to the proof-of-work algorithm

现在, 在收集块中的所有事务后, andy 需要构造块标头。

构建块标头

若要构造块标头，挖掘节点需要填写六个字段，如表中所示：

大小	领域	描述
4个字节	版本	要构造块标头，挖掘节点需要填写六个字段，如
32个字节	上一个块哈希	对链中上一个 (父) 块的哈希的引用
32个字节	默克根	此块的事务的 merkle 树的根的哈希
4个字节	时间 戳	此块的大致创建时间 (unix 时代秒)
4个字节	难度目标	此块的工作验证算法难度目标
4个字节	Nonce	用于工作证明算法的计数器

一旦安迪的节点有所有的字段填充块标题，安迪开始*挖掘*块。

区块的挖掘

- 填充所有其他字段后，块标头现在已完成，挖掘过程可以开始
- 现在的目标是为**Nonce**导致块标头哈希小于难度目标
- 挖掘节点需要在找到满足要求的 nonce 值之前测试数十亿或数万亿个 nonce 值

现在，由 andy 的节点构造了一个候选块，现在是 andy 的硬件挖掘钻机 "挖掘" 块的时候了，可以找到使块有效的工作证明算法的解决方案了。

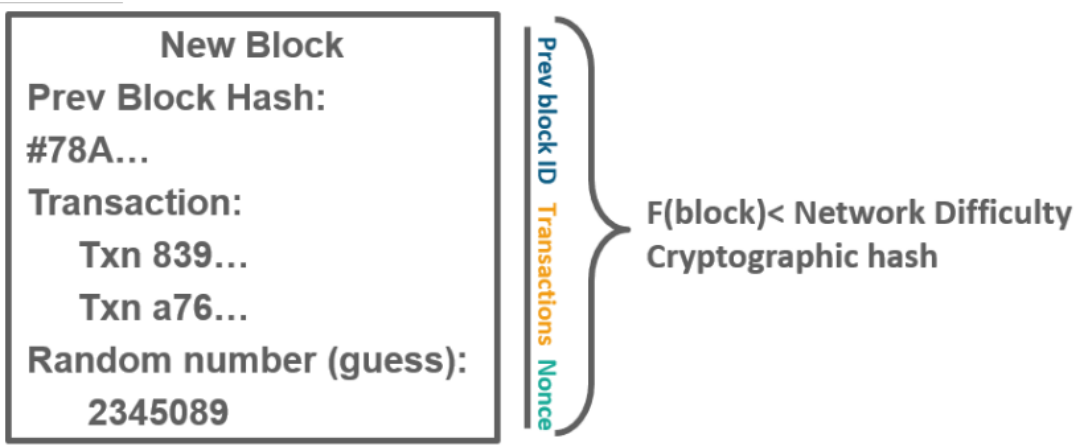
工作证明是一段难以 (昂贵、耗时) 的数据，但对其他人来说很容易验证，并且满足某些要求。

找到困惑--为什么很难?

- sha-256 是单向函数因此,**蛮 力**是实现特定输出值的唯一途径
- 平均而言, 需要多次随机猜测才能找到解决方案, 因此挑战是艰难的
- 一个人平均需要 1 0分钟左右才能找到解决方案的特殊关键

为了保持硬币的可预测分布, 当更多的人在硬币上工作时, 谜题就越来越难解决。

若要验证块, 请根据*工作证明*算法, 安迪的挖掘节点必须达到难度目标。



Difficulty Representation

- The block contains the difficulty target, in a notation called “difficulty bits” or just “bits“
- Let’s say a block has 0x1903a30c as the difficulty bits. This notation expresses the difficulty target as a coefficient/exponent format, with the first two hexadecimal digits for the exponent and the next six hex digits as the coefficient

The formula to calculate the difficulty target from this representation is:

$$target = coefficient * 2^{(8 * (exponent - 3))}$$

So, such is the difficulty coefficient that Andy’s mining node has worked really hard to reach the difficulty target.

成功挖掘块

- andy 有几个硬件采矿钻机, 每个运行**sha256**以惊人的速度并行的算法
- 在 andy 的桌面上运行的挖掘节点将块标头传输到他的挖掘硬件, 该硬件开始每秒测试数万亿的非 s
- 在开始开采块近11分钟后, 其中一台硬件采矿机器找到了解决方案, 并将其发送回采矿节点
- 立即, andy 的挖掘节点将块传输到所有对等方
- 它们接收、验证, 然后传播新块。当方块在网络上产生波纹时

现在, 该块已在网络中传播, 每个完整节点独立地验证块

每个块的独立确认

- 在**比特币的共识**机制，每个新块由网络上的每个节点独立验证
- 这可确保仅在网络上传播有效的块
- 节点通过对照必须满足的一长串条件对块进行检查来验证块

Assembling and Selecting Chains of Blocks

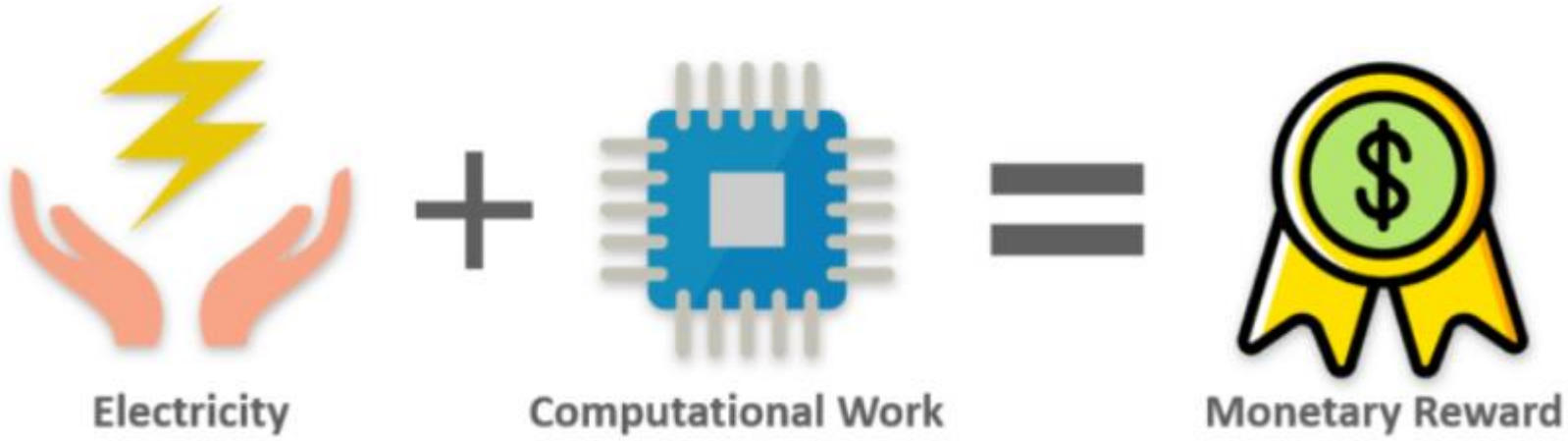
- Once a node has validated a new block, it will then attempt to assemble a chain by connecting the block to the existing blockchain

Once the block is verified by the network, it becomes the part of the blockchain and for successfully solving the block puzzle the miner is rewarded.

In the network shown above, once the node (in orange) validates the block, it assembles the chain by connecting the block to the existing blockchain

矿工奖励

- 由于矿工们使用他们宝贵的资源来验证块，他们被给予**货币奖励**
- 在比特币的情况下，他们得到一些新创建的比特币作为奖励

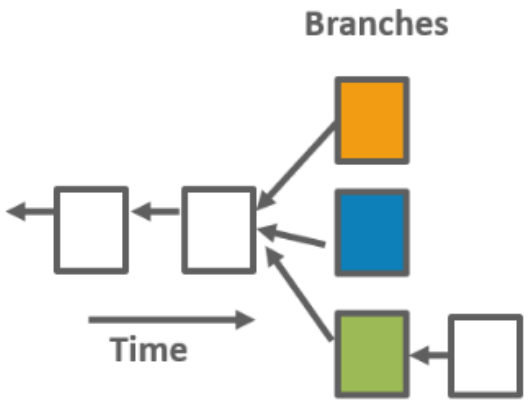


现在，问题出现了，当多个方块同时得到解决时，会发生什么？

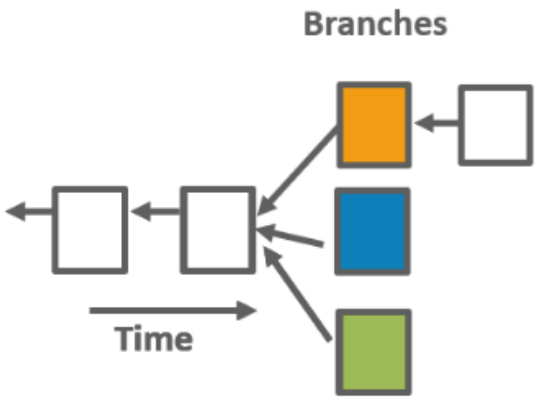
是的，这确实是可能的!在这种情况下，存在几个分支。

多个分支

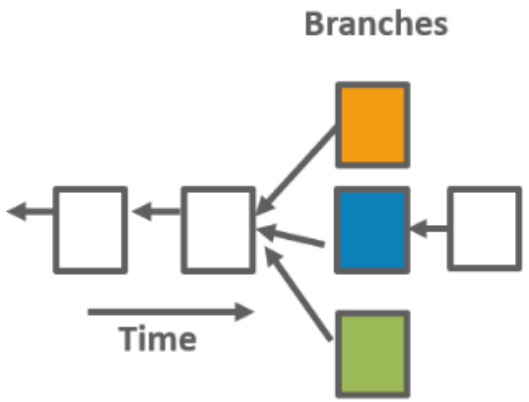
- 然而, 尽管这个问题很棘手, 但有可能同时解决不止一个街区
- **几个分支**在封锁链是可能的, 在这种情况下
- 每个人都应该简单地在他们收到的第一个方块的顶部构建块
- 其他节点可能以不同的顺序接收了块
- 他们将在他们第一次收到的街区上建造



Paul's Blockchain
Paul received green block first. Hence, he builds the next block on top of green



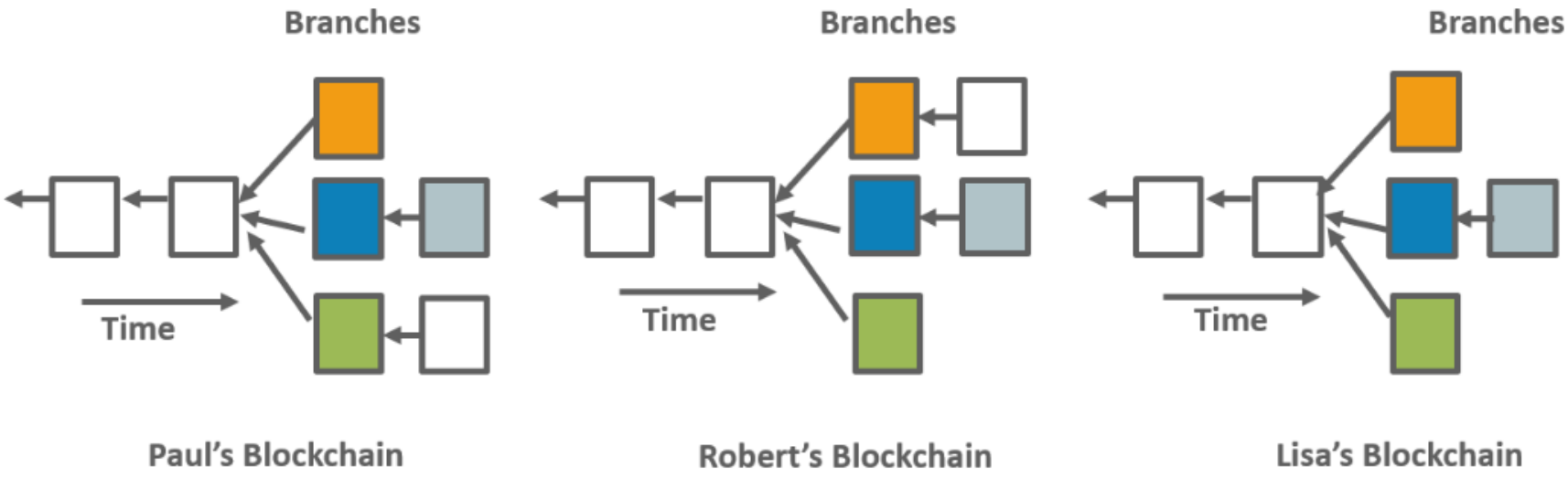
Robert's Blockchain
Similarly, Robert received orange first. Hence, he builds the next block on top of orange



Lisa's Blockchain
Also, Lisa received blue first. Hence, she builds the next block on top of blue

多个分支

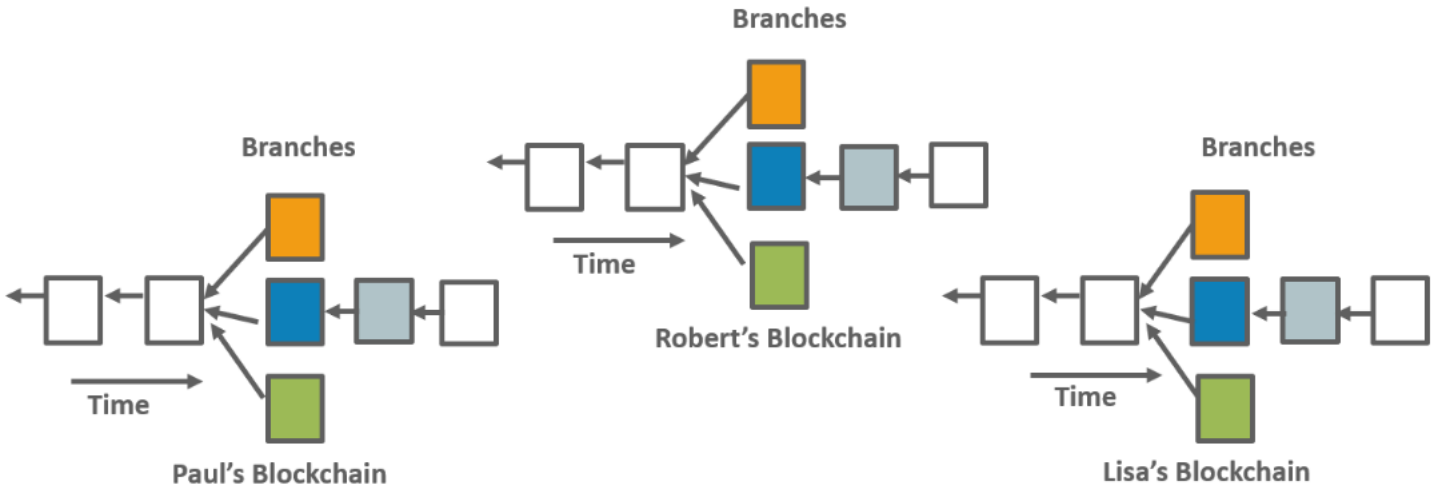
- 当有人解决下一个方块时，领带就断了，因为这种情况很少连续发生多次



- 在这种情况下，区块链迅速稳定
- 一般规则是切换到最长的链可用

多个分支

- 在这种情况下，区块链迅速稳定
- 一般规则是切换到最长的链可用



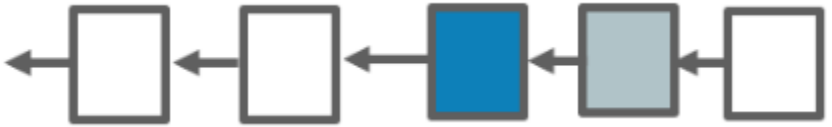
区块链快速稳定。
每个节点都与分类帐的当前状态一致。

Several Branches

- The Blockchain quickly Stabilizes.
- Every node is in agreement with the current state of the ledger.

Paul's Blockchain

Robert's Blockchain



Lisa's Blockchain

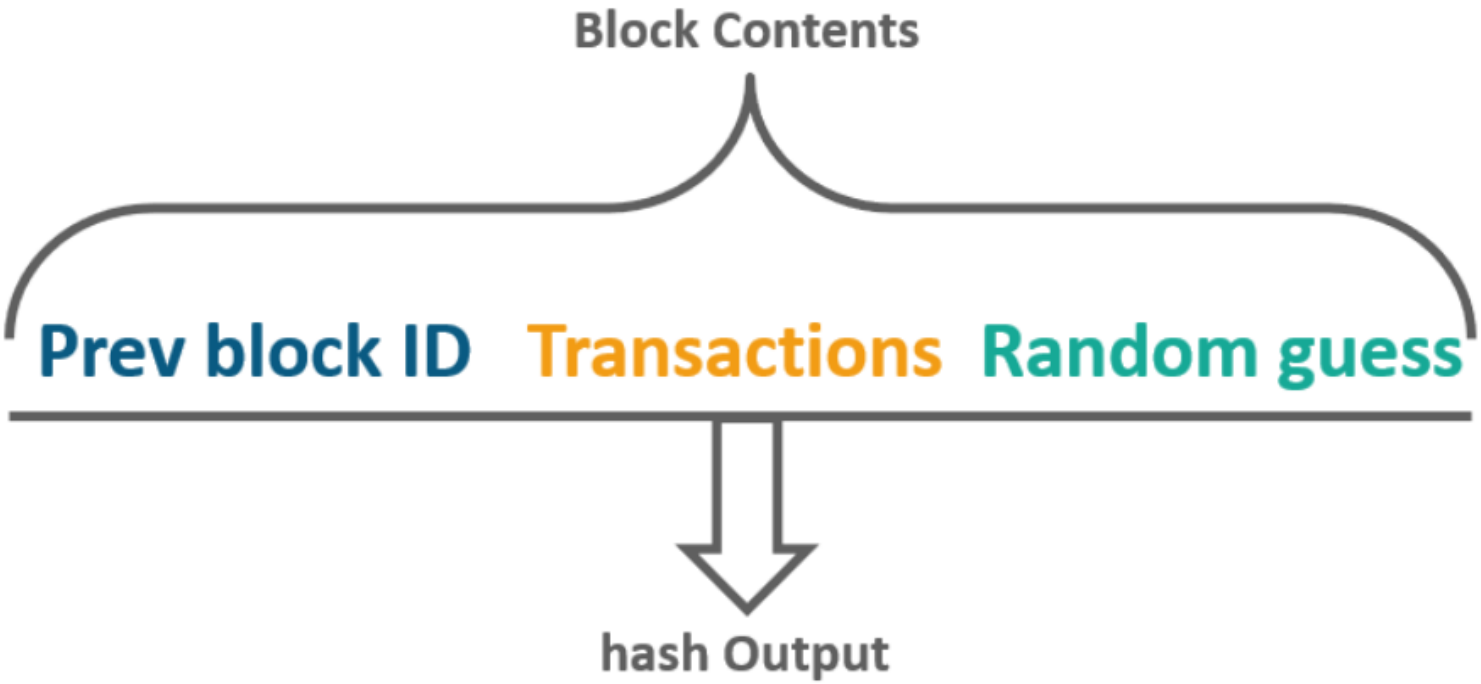
So, consensus rules save the blockchain network from such ambiguity.
Now, another question arises here, what if someone tries to alter any transaction or records in the system?

议程

- 什么是区块链技术?
- 区块链是如何工作的?
  - 交易的独立验证
  - 已验证事务的聚合
  - 区块的挖掘
- 如果有人试图破解系统怎么办?

有人试图破解系统

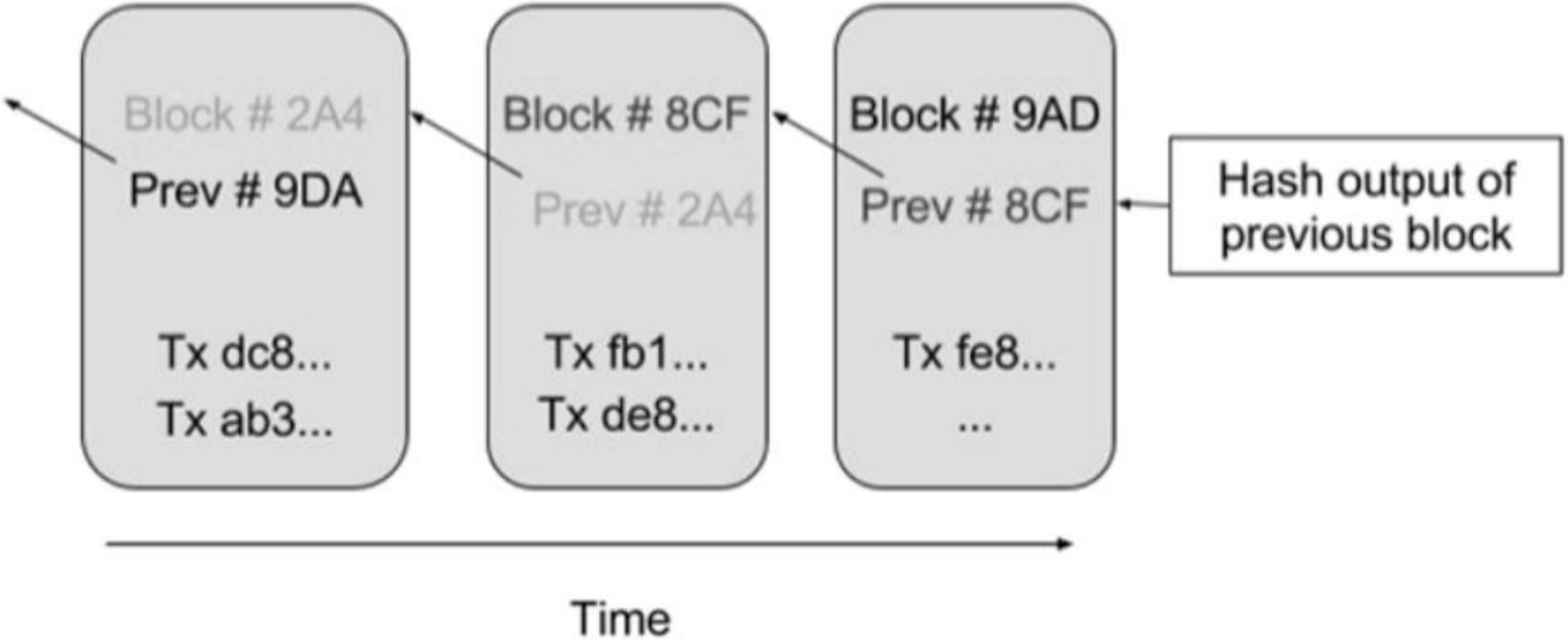
- 一旦一个块被解决，加密哈希输出就会成为该块的标识符。



因此，协商一致的规则将区块链网络从这样的模糊中解救出来。
现在，这里出现了另一个问题，如果有人试图改变系统中的任何交易或记录怎么办？

有人试图破解系统

- 由于区块链是一个反向链接的分布式记录数据库。当一个块形成时，加密哈希输出将成为该块的标识符，该标识符连接到下一个块，从而创建一个块链。



因此，区块链是由强大的加密算法来保护的，没有办法改变任何记录。*如果有人试图更改任何块中的任何事务，则块的哈希将更改，因此所有前面块的哈希将发生更改。节点将无法达成共识，因此，欺诈行为很容易被发现*

议程

- ✓ 什么是区块链技术?
- ✓ 区块链是如何工作的?
  - ✓ 交易的独立验证
  - ✓ 已验证事务的聚合
  - ✓ 区块的挖掘
- ✓ 如果有人试图破解系统怎么办?

"企业"与区块链

议程

- 什么是业务区块链?
- 区块链与业务有多关系?
  - 共识用例
  - 来源使用案例
  - 不可变用例
  - 终结用例
- 区块链业务网络

什么是业务的区块链?

当今的业务网络通常效率低下, 因为网络中的每个参与者都保留业务与之交互的所有各方之间的所有事务的记录或分类帐。 由于工作重复和中介增加了其服务的费用, 这一过程费用很高。

解决此问题的一个方法是区块链, 它提供了共享分类帐技术, 允许网络中的任何参与者查看一个记录系统, 或分类帐。 通过使用区块链技术, 企业可以从更有效的货物和服务转让中受益。

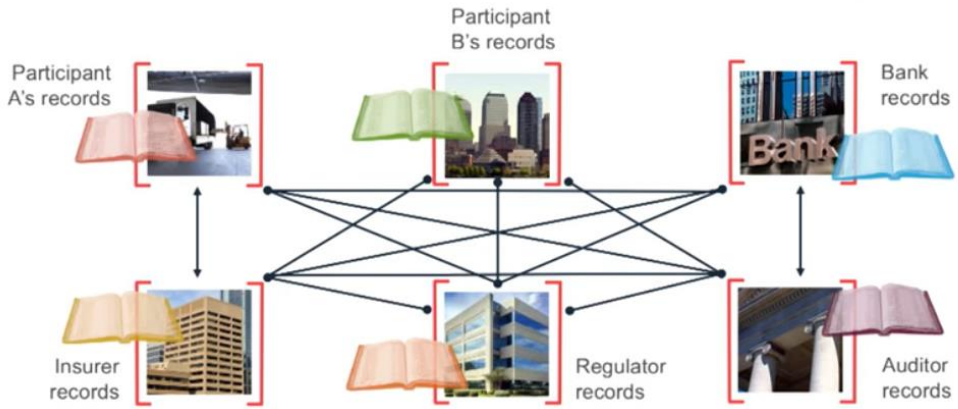
下一个模块描述业务网络和事务、 区块链可以解决的问题、 什么是区块链以及它是如何工作的, 以及关键用例。

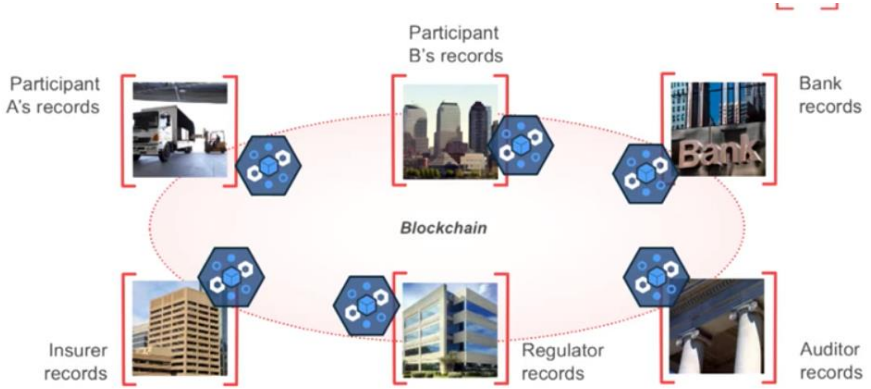
The business backdrop

- Most if not all business operate on public or private networks.
- Tangible and intangible assets must be transferred across networks to network participants.
- Ledgers are used to document all those transactions, and networks are governed by a contract.
- At the highest level, a blockchain is a trusted, distributed ledger with shared business processes.

问题区域

- 谈论当前业务网络的挑战: 多个手动分类帐。
- 这意味着网络中的所有参与者都必须更新或审核自己的分类帐, 这是低效、容易出错和不安全的。





传统业务网络与区块链业务网络

议程

- 什么是业务区块链?
- 区块链与业务有多关系?
  - 共识用例
  - 来源使用案例
  - 不可变用例
  - 终结用例
- 区块链业务网络

区块链与业务的关系

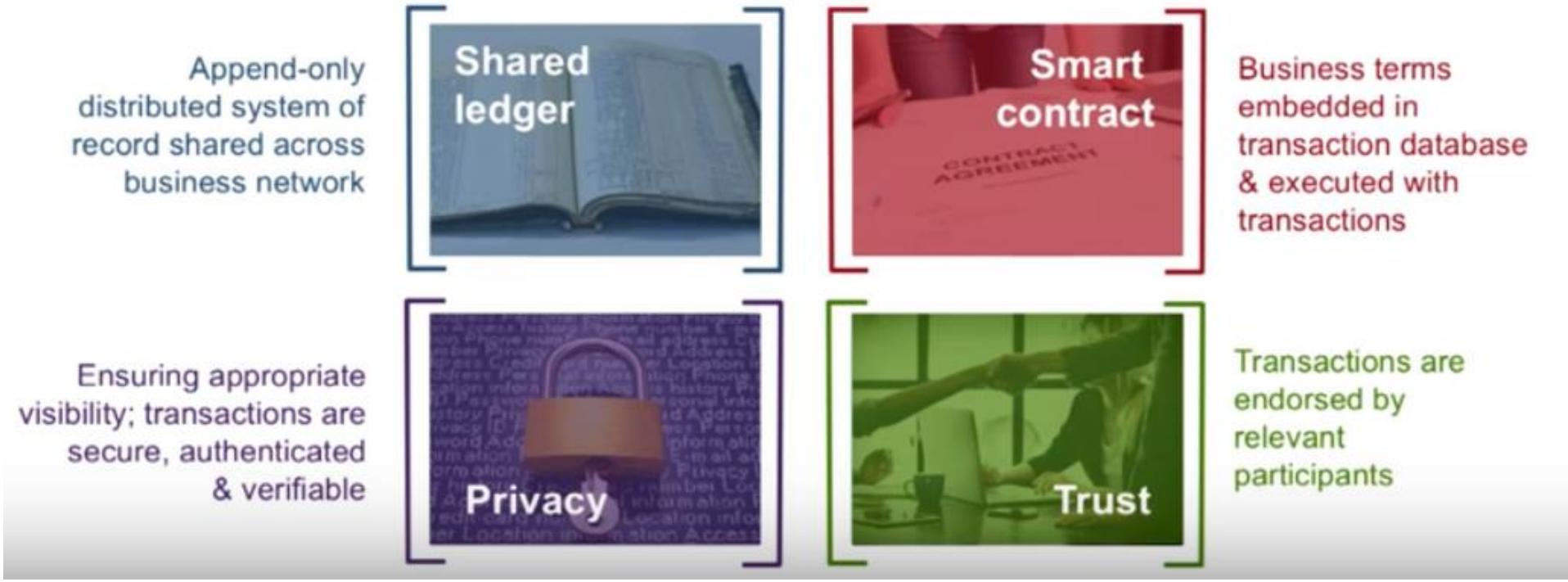
- 比特币是一种不受监管的影子货币，是第一个流行的区块链应用程序。
  - 比特币应用程序在匿名网络中工作，所以没有人知道参与者是谁。
- 本课程所涵盖的业务区块链与比特币无关，在几个方面与比特币不同。

Blockchain for business differs in key areas:

- *Identity* over anonymity
- *Selective endorsement* over proof of work
- *Assets* over cryptocurrency

业务环境中对区块链的要求

共享分类帐、智能合同、隐私和信任。



业务区块链的4个基本组件

Apply blockchain to business

Blockchain for business has several advantages:

- Saves time
- Removes cost
- Reduces risk
- Increases trust

For example, for financial services network, a business network that runs on a blockchain can speed up transaction processes and audits. That in turn reduces costs and can lead to greater customer satisfaction. A business that runs a supply chain network can benefit from blockchain by reducing errors in shipments, have better tracking or materials, and reduce the risk of illicit tampering of records.

区块链的好处

区块链提高了交易速度，降低了审计成本，降低了网络攻击的风险，并增加了信任度。

节省
时间

交易时间
从几天到接近瞬间

删除
成本

间接费用和费用中介

减少
风险

篡改、欺诈和网络犯罪

增加
信任

通过共享进程和记录保存

区块链参与者如何在业务网络中共享数据

例如，银行的路由代码可以是共享引用数据。区块链可用于管理此类数据，其中有一组数据可以更轻松地更新。

Agenda

- What is Blockchain for Business?
- How blockchain is related to Business?
  - Consensus use case
  - Provenance use case
  - Immutability use case
  - Finality use case
- Blockchain Business Network

共识用例–共享引用数据

什么？你在干什么

- 业务网络中的竞争对手合作者需要共享参考数据，例如银行路由代码
- 每个成员都有自己的代码并将更改转发给中央主管部门以进行收集和分发
- 信息子集可由组织拥有

如何

- 每个参与者在区块链网络中维护自己的代码
- 区块链创建整个数据集的单一视图

好处

1. 整合、一致的数据集可减少错误
2. 近实时的参考数据
3. 当然支持参与者之间的代码编辑和路由代码传输

通过带有区块链的供应链跟踪物料

- 这是使用区块链改进业务流程的另一个示例。
- 您可以使用区块链网络跟踪飞机的部件。
- 您可以看到资产的生命周期。
- 另一个例子是，钻石零售商可以看到钻石是否来自非法来源。

议程

- 什么是企业的区块链
- 区块链与业务有多关系?
  - 共识用例
  - 来源使用案例
  - 不可变用例
  - 终结用例
- 区块链业务网络

产地使用案例–车辆维修

什么？你在干什么

- 复杂系统中每个部件的来源难以跟踪
- 制造商、生产日期、批次甚至制造机器计划

如何

- 区块链包含每个部件的完整来源细节
- 每个制造商在生产过程中都可以访问，飞机所有者、维护者和政府监管机构

好处

1. 信任增加，没有权威 "拥有" 来源
2. 改进
   系统利用率
3. 回顾 "具体"
   而不是横舰队

How blockchain can benefit auditing and compliance in FinTech

- This is another use case about compliance.
- A bank wants to use blockchain to keep an indelible record of all key transactions over a reporting period.
- Blockchain assures that this record is private, secure, and complete.

议程

- 什么是业务区块链?
- 区块链与业务有多关系?
  - 共识用例
  - 来源使用案例
  - 不可变用例
  - 终结用例
- 区块链业务网络

不变性用例–财务分类帐

什么？你在干什么

- 分布在多个部门和地区的大型组织中的财务数据
- 审计和合规需要报告期内所有关键交易的不可磨灭的记录

如何

- 区块链从不同的金融系统中收集交易记录
- 仅适用和防篡改的品质创造高可信度财务审计线索
- 隐私功能，以确保授权的用户访问

好处

1. 降低审计和合规性成本
2. 向审计师和监管机构提供"查找和查找" 访问权限
3. 更改的性质
   合规性。
   被动到主动

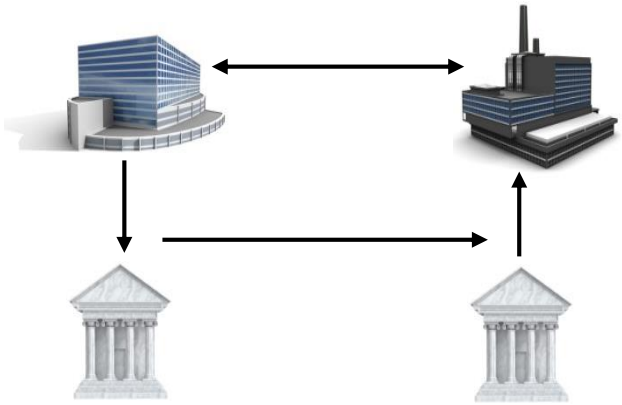
How blockchain can streamline letters of credit in FinTech

- This is a use case about compliance.
- A bank wants to use blockchain to keep an indelible record of all key transactions over a reporting period.
- Blockchain assures that this record is private, secure, and complete.

议程

- 什么是业务区块链?
- 区块链与业务有多关系?
  - 共识用例
  - 来源使用案例
  - 不可变用例
  - 终结用例
- 区块链业务网络

最终用例– 信用证



什么？你在干什么

- 银行处理信用证 (loc) 希望将其提供给包括创业公司在内的更广泛的客户
- 目前受到成本和执行时间的限制

如何

- 区块链提供共同的帐目的分类帐
- 允许所有交易对手拥有相同的交易和履行记录

好处

1. 提高执行速度 (少于 1天)
2. 极大地降低了成本
3. 降低风险，例如货币波动
4. 增值服务，例如增量支付

区块链示例: (选定) 行业

Financial	Public Sector	Retail	Insurance	Manufacturing
Trade Finance	Asset Registration	Supply chain	Claims processing	Supply chain
Cross currency payments	Citizen Identity	Loyalty programs	Risk provenance	Product parts
Mortgages	Medical records	Information sharing (supplier – retailer)	Asset usage history	Maintenance tracking
	Medicine supply chain		Claims file	

议程

- 什么是业务区块链?
- 区块链与业务有多关系?
  - 共识用例
  - 来源使用案例
  - 不可变用例
  - 终结用例
- 区块链业务网络

Blockchain for Business

Community + Code

Linux Hyperledger Project

Open Source Code: Blockchain for business;

Consensus | Provenance | Immutability | Finality

Open Governance – 100 member cross industry board

Cloud

IBM Blockchain

Blockchain managed service on IBM Cloud and z Systems;

Identity | Consensus | System Integration | Hardware-assist for Performance & Security

IBM Blockchain on Bluemix

Clients

Blockchain Solutions
Blockchain Garage

Making Blockchain real for business

Blockchain Garage;
New York | London | Singapore | Tokyo

Blockchain Services Practice

从区块链开始最简单的方法是什么?

- 需要记住的是, 封锁链仍然是一项新兴技术。
- 对于那些希望采用区块链的人来说, 一个建议是从一个简单的第一个用例开始。
- 企业主需要从小处做起, 然后寻找更多的方法来发展和扩大区块链网络的使用。
- 议长简要提到了监管机构、做市商和行业集团等企业中的一些角色。

客户采用模式

Why

高价值市场

- 高价值金融资产的转移
- 在市场的许多参与者之间
- 监管时间框架

资产交易

- 资产分享 (表决、股息通知)
- 资产是信息, 而不是财务
- 来源和最终是关键

共享的共享的莱格

- 由一小部分参与者创建
- 共享密钥引用数据
- 整合、一致的实时视图

合规性莱德

- 合规性、审计和风险数据的实时视图
- 来源、不变性和最终性是关键
- 与审计员和监管机构的透明接触

区块链采用的关键参与者

调节器

–执行游戏规则的组织

–监管机构热衷于支持基于区块链的创新

–关注的是系统性风险--新技术、分布式数据、安全性

产业集团

–通常由业务网络成员提供资金

–就行业趋势提供技术咨询

–通过向成员提出建议，鼓励最佳做法

做市商

–在金融市场中，以买方和卖方为由提供流动性

–更广泛地说，创新的组织

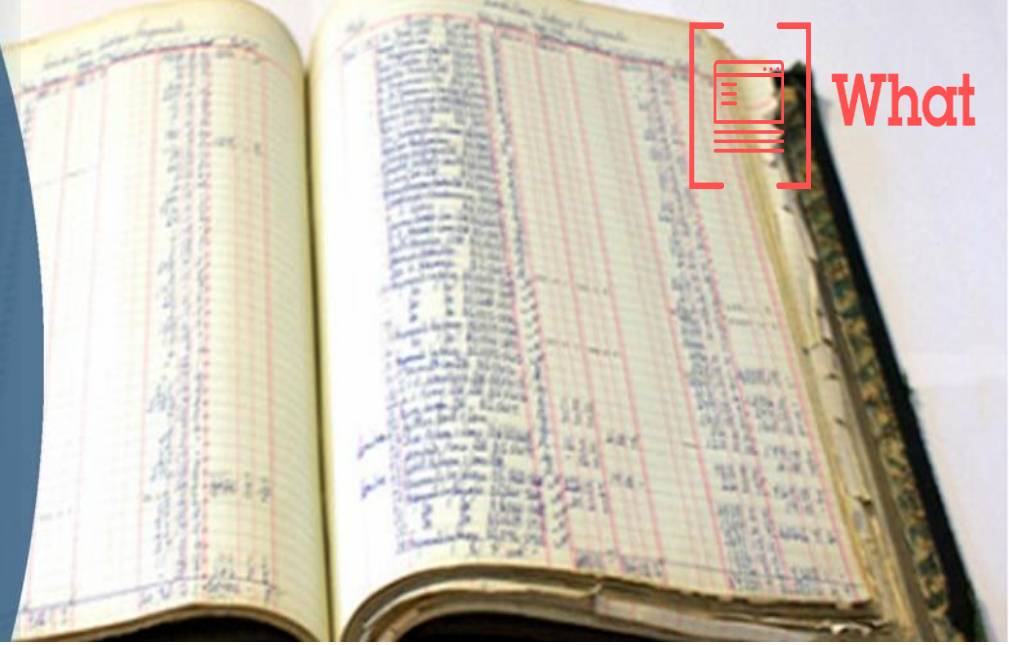
-创建新的商品或服务，以及业务流程(可能)

-为现有的商品或服务创建新的业务流程

ibm 和超级分类帐关系: 业务的区块链

- ibm 是 linux 基础超级分类帐项目的首要成员。
- ibm 还拥有其他服务和技术来帮助您构建区块链网络, 如 ibm 云 (ibm 云) 和 docker 容器。
- ibm 提供支持和参与, 帮助您构建区块链。

共享分类帐



What

记录业务网络中的所有交易记录

参与者之间共享

参与者有自己的复制副本

已保护，因此参与者只能看到适当的事务

共享的记录系统

智能合同

What

合同所隐含的业务规则. 嵌入区块链并随交易一起执行

可验证, 已签名

用编程语言编码

例子:

定义公司债券转让发生的合同条件

隐私

分类帐是共享的，但参与者需要隐私

参与者需要：

- 要私有的事务
- 未链接到事务的标识

需要对事务进行身份验证

密码学是这些过程的核心

Consensus

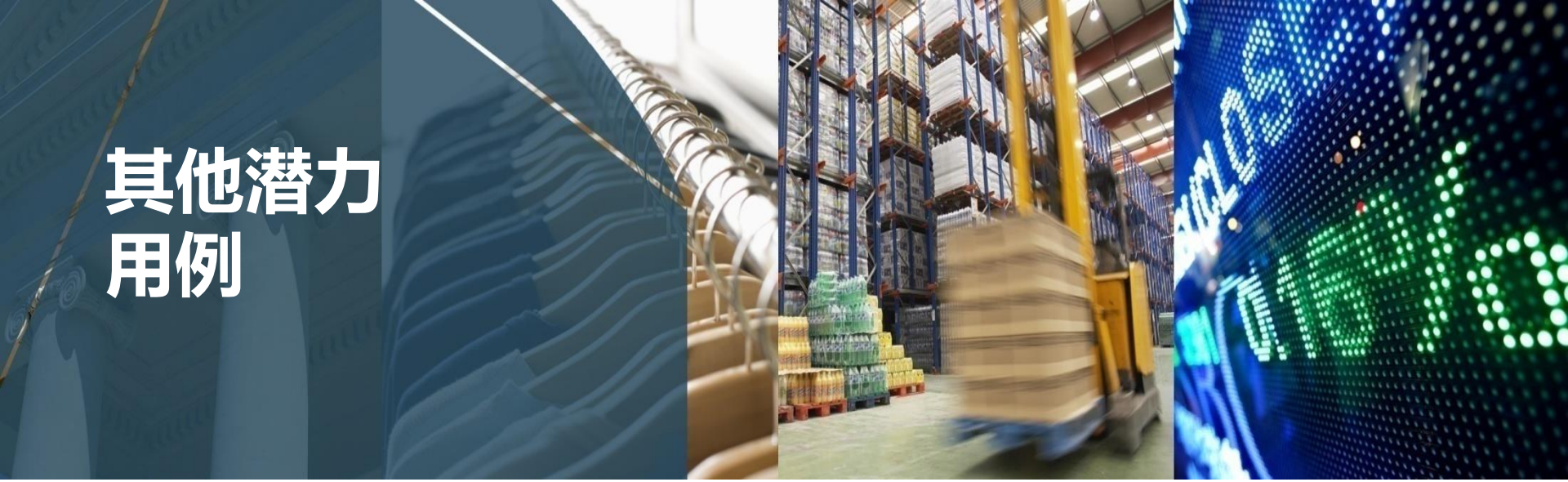
What

… the process by which transactions are verified

- Anonymous participants
  - Bitcoin *cryptographic mining* provides randomized selection among anonymous participants
  - Significant compute cost (proof of work)
- Known & trusted participants
  - Commitment possible at low cost
  - Byzantine fault tolerance (BFT)

- Multiple alternatives
  - Proof of stake, where influence is determined by risk of validators
  - Multi-signatures, validation needs consent from 3 out of 5 validators
- Industrial Blockchain needs “pluggable” consensus

其他潜力用例

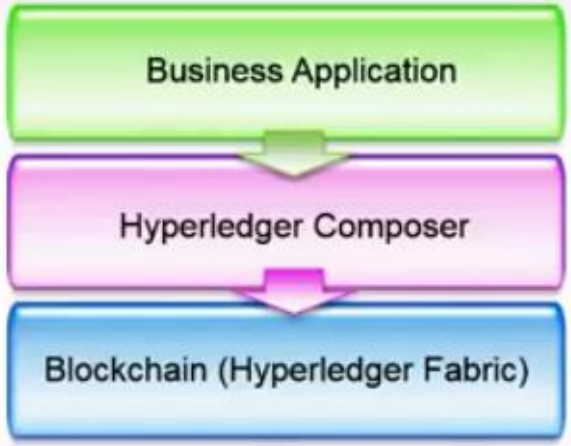


- 证券
  - 贸易后结算
  - 衍生合约
- 贸易融资
  - 提单
  - 跨币支付
- 银团贷款
- 供应链管理
- 零售银行业务
  - 跨境汇款
  - 抵押核查和合同
- 公共记录
  - 房地产记录
  - 车辆登记
  - 公民身份
- 数字物业管理

超级分类编辑器

提供了超级分类帐编辑器的高级、简要概述，以及它是如何更快、更简单地构建网络的方法，而不是使用 go 编程语言中的链代码构建。

- A suite of high level application abstractions for business networks
- Emphasis on business-centric vocabulary for quick solution creation
- Reduce risk, and increase understanding and flexibility



- Features
  - Model your business networks, test and expose via APIs
  - Applications invoke APIs transactions to interact with business network
  - Integrate existing systems of record using loopback/REST
- **Fully open** and one of eight Hyperledger projects

参与模型概述

1. 讨论区块链技术
2. 探索客户业务模式
3. 显示区块链应用程序演示

1. 了解区块链概念和元素
2. 手拉手区块链上布吕米克斯
3. 标准演示自定义

1. 设计思维研讨会，定义业务挑战
2. 敏捷迭代以增量方式构建项目功能
3. 企业集成

1. 扩大试点或向新项目扩展
2. 业务流程重新设计
3. 系统集成

远程或面对面	***远程或面对面***	***面对面***	***面对面***
免费的	***免费的***	***对于费用***	***对于费用***

区块链业务网络的参与者

除监管机构外，所有其他用户只能看到资产转让生命周期的一部分。

他们可以在拥有资产之前和拥有资产的情况下看到资产发生了什么，但在转让资产后，他们无法看到资产发生了什么。

Summary

Blockchain …

- is a shared, replicated, permissioned ledger technology
- can open up business networks by taking out cost, improving efficiencies and increase accessibility
- 解决了一系列令人兴奋的、主题化的业务挑战, 这些挑战跨越了每个行业

Ibm。。。

- 支持 linux 基础超级分类帐开放标准、开源、开放治理区块链
- 具有易于访问、成熟且增量的互动模式, 为客户提供立即开始的信心

总结

现在, 您应该更好地了解区块链如何用于业务, 以及这项技术如何增加价值。更具体地说, 您应该了解:

- 区块链和分布式分类帐系统
- 业务区块链的主要使用案例
- 如何在区块链网络中进行资产转移

查看后续课程ibm 区块链基础开发人员在这里, 您可以找到有关区块链的教程、示例代码和其他信息。
跳转到您的区块链培训的下一步, 通过参加开发人员 works 的课程ibm 区块链基础开发人员.
开始构建您的区块链应用程序超级分类编辑!

议程

- ✓ 什么是业务区块链?
- ✓ 区块链与业务有多关系?
  - ✓共识用例
  - ✓来源使用案例
  - ✓不可变用例
  - ✓终结用例
- 区块链业务网络

结束!

धन्यवाद

Hindi 印地语

多謝

繁体中文

ขอบคุณ

泰语

Спасибо

俄语

谢谢

西班牙语

谢谢

英语

شكراً

阿拉伯语

奥布里加多

巴西葡萄牙语

格拉齐

意大利语

多谢

简体中文

丹克

德语

谢谢

法语

நன்றி

Tamil

泰米尔语

ありがとうございました

日语

감사합니다

朝鲜语

莱杰斯是关键.....

帐是一个企业的记录系统。

对于他们参与的多个业务网络, 企业将有多个分类账。

交易–在分类帐上或分类帐外转移资产

约翰给安东尼一辆车 (简单)

合同–发生交易的条件

如果安东尼付了约翰的钱, 那么汽车就会从约翰传给安东尼 (简单)

如果汽车无法启动, 资金不会传递给约翰 (由第三方仲裁员决定) (更复杂)