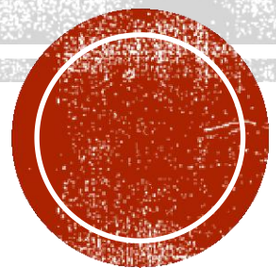
比特币与区块链

万志国

wanzhiguo@sdu.edu.cn

山东大学计算机学院



2015首届全球区块链峰会

“区块链—新经济蓝图”

上海

10月在上海举办。本次峰会预计有来自央行金融研究所、央行征信中心、上海证券交易所、陆金所、德勤会计事务所等全球约200位包括银行、支付、证券、大宗商品等金融行业及其他对**区块链技术应用前景**有兴趣的行业专业人士参加。

来源：http://www.8btc.com/wanxiang-blockchain-labs-20151015

(C) DavidKuoChuenLee

北京

2016年1月20日，央行发布消息称，该行数字货币研讨会当日在北京召开。

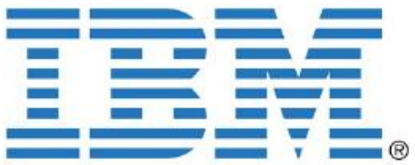
央行表示，其数字货币研究团队要积极吸收国内外数字货币研究的重要成果和实践经验，做好关键技术攻关，争取早日推出央行发行的数字货币。

而数字货币背后所承载的就是区块链技术。

(C) DavidKuoChuenLee

来源：“云计算”已成「老炮儿」，将被“区块链”所革命！

“微软和IBM宣布区块链服务开门营业”



17 Feb 2016

- IBM 宣布正式启动其数字分类账项目
- IBM的区块链云服务平台开放
- 开发者可以在平台中创建、部署和运行以区块链为基础链应用.
- 伦敦证券交易所与IBM公司合作从事开发区块链技术-

  区块链技术有助于管理风险以及给全球金融市场带来额外的透明度

微软Azure（云计算）服务

- 使用者可以将一个分布式的分类帐平台放在一起，并将其添加到Azure（云计算）服务中。
- 微软Azure和Consensys通过Azure云平台协助全世界各地的开发者，客户或商人创造出私有的，半私有的，公共的和联营的区块链网络，然后分销他们的区块链产品。

(C) DavidKuoChuenLee

来源: https://news.bitcoin.com/microsoftibmdeclareblockchainopenbusiness/

区块链应用领域


通信领域

投票领域


医疗领域


公证领域


银行领域


股权认证/交易

保险领域

域名领域

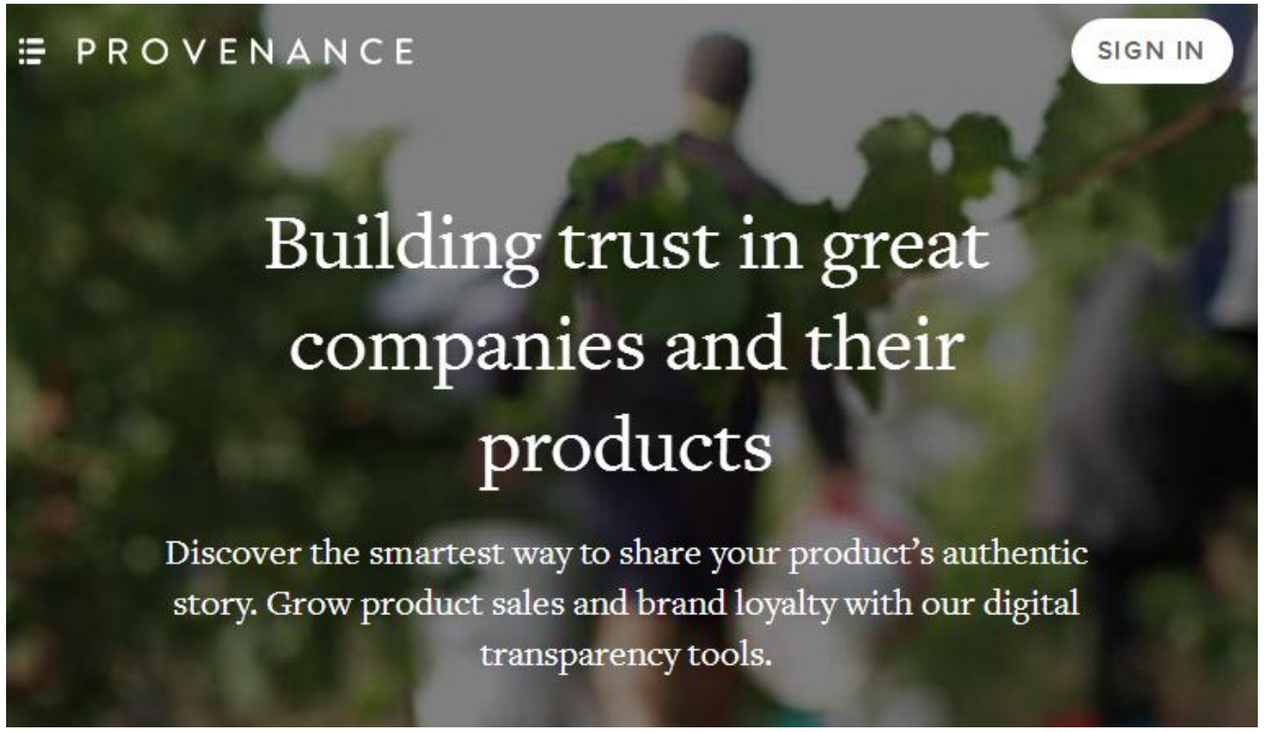

物联网

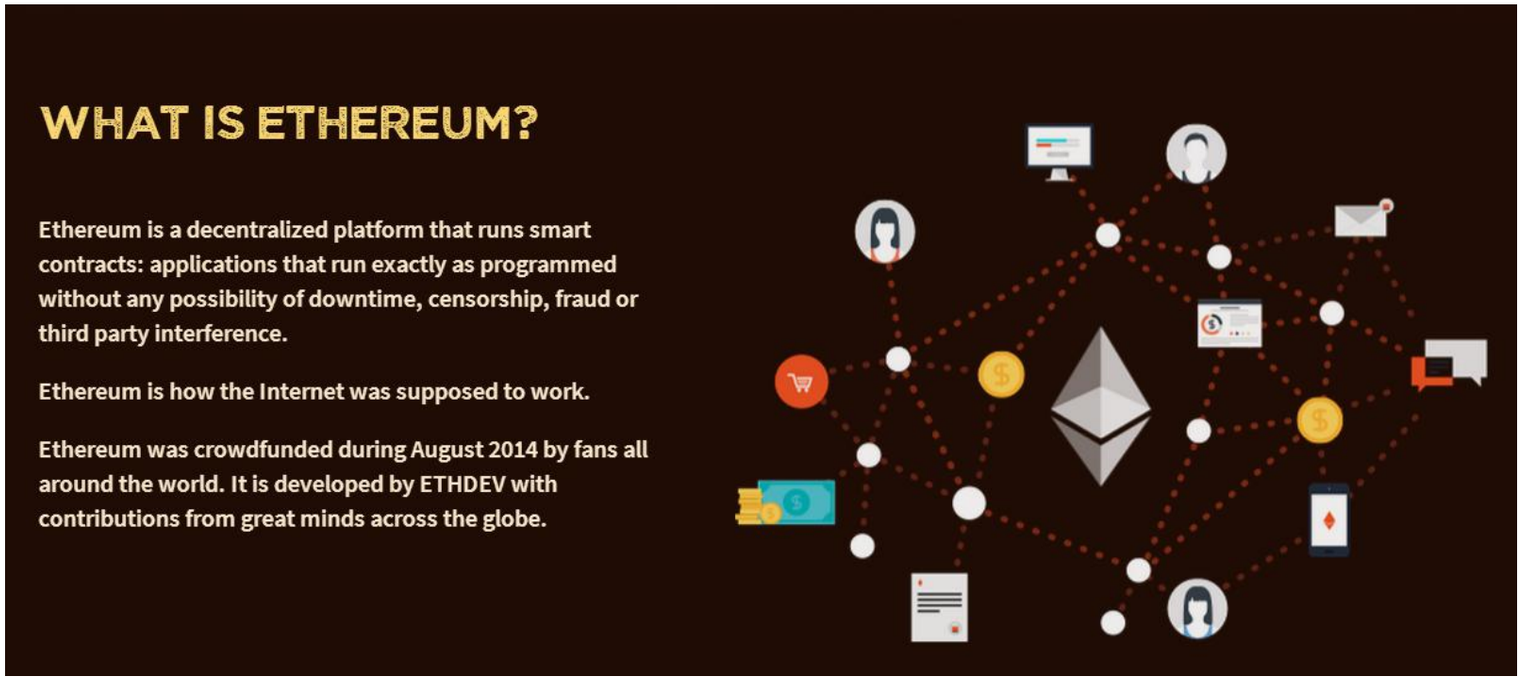
……

(C) DavidKuoChuenLee

图片来源：百度图片

创业公司





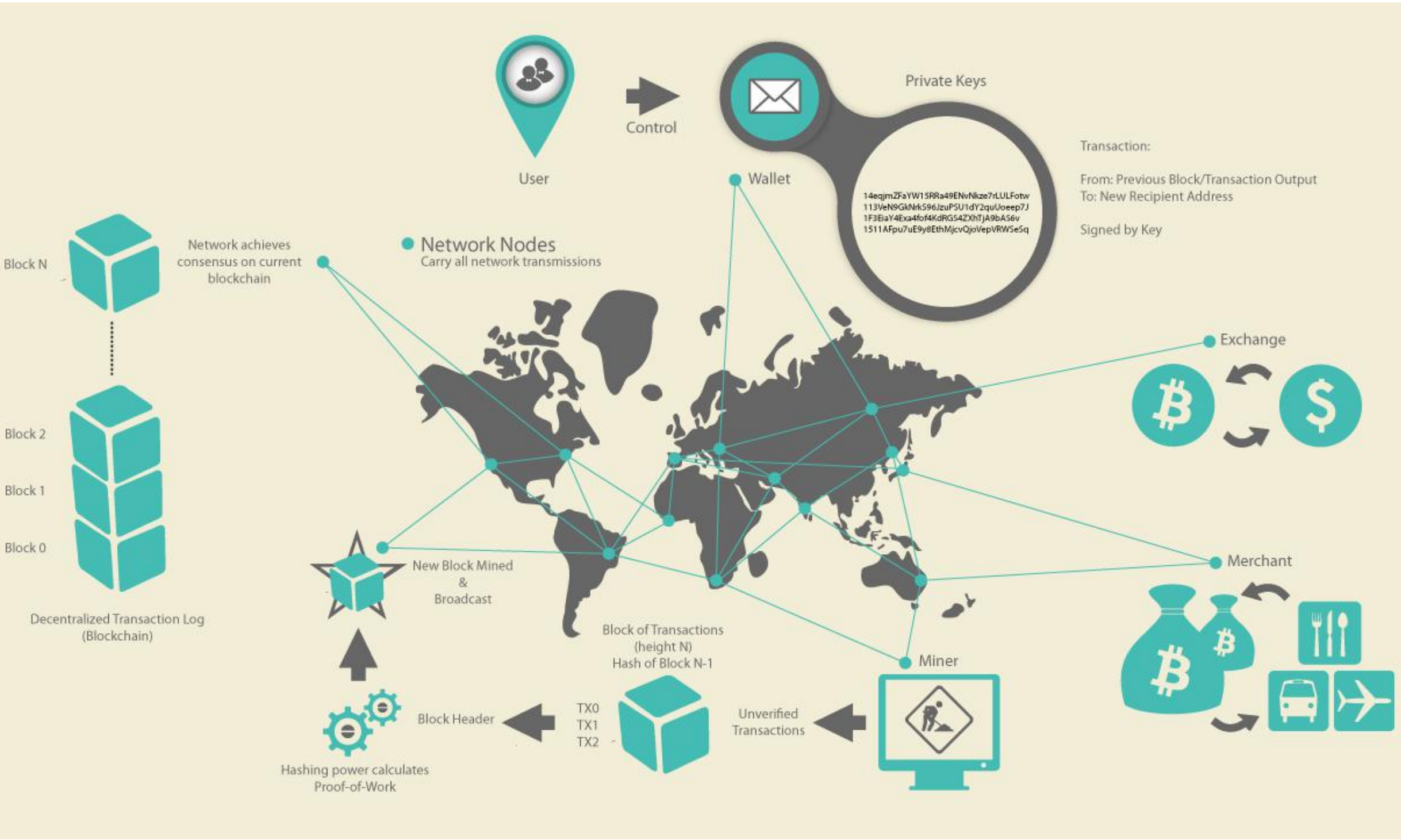
R3 is a financial innovation firm that leads the Distributed Ledger Group (DLG), a consortium partnership with 42 of the world's leading banks, to design and deliver advanced distributed ledger technologies to global financial markets.

提纲

- Basics: Bitcoin and Transactions
- Block Mining, Verification and the Blockchain
- Blockchain Innovations

Part 1:
Basics: Bitcoin and Transactions

Overview of bitcoin: a big picture



How a ₿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

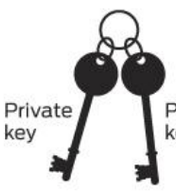
Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfDpN.

CREATING A NEW ADDRESS

Each address has its own balance of bitcoins.

Bob creates a new Bitcoin address for Alice to send her payment to.

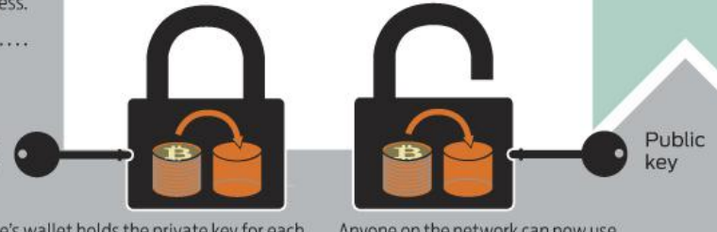


Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



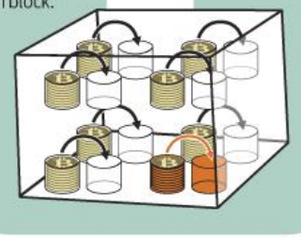
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

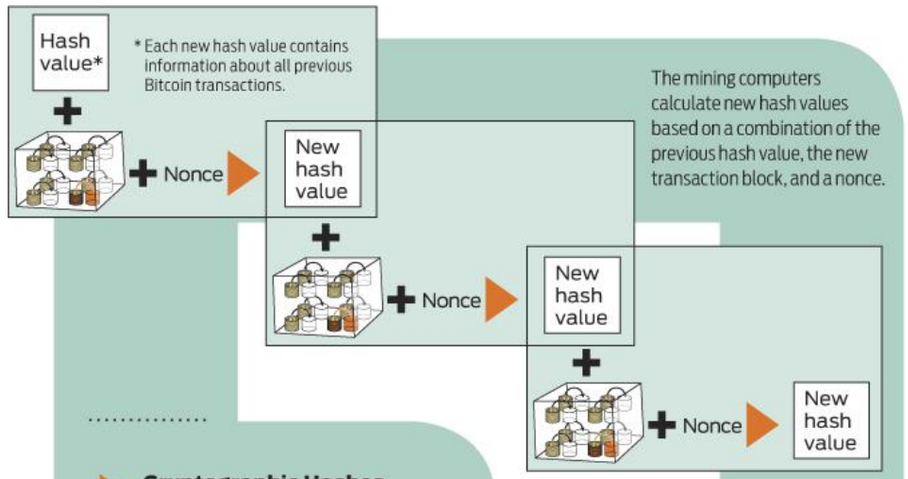
VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



The miners' computers are set up to calculate cryptographic hash functions.

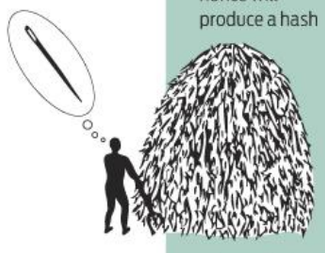


Cryptographic Hashes
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all e**u**il	486c 6be4 6dde...
The root of all v**e**il	b8db 7ee9 8392...

Nonces
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

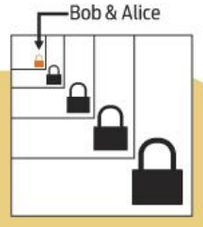
Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.



The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

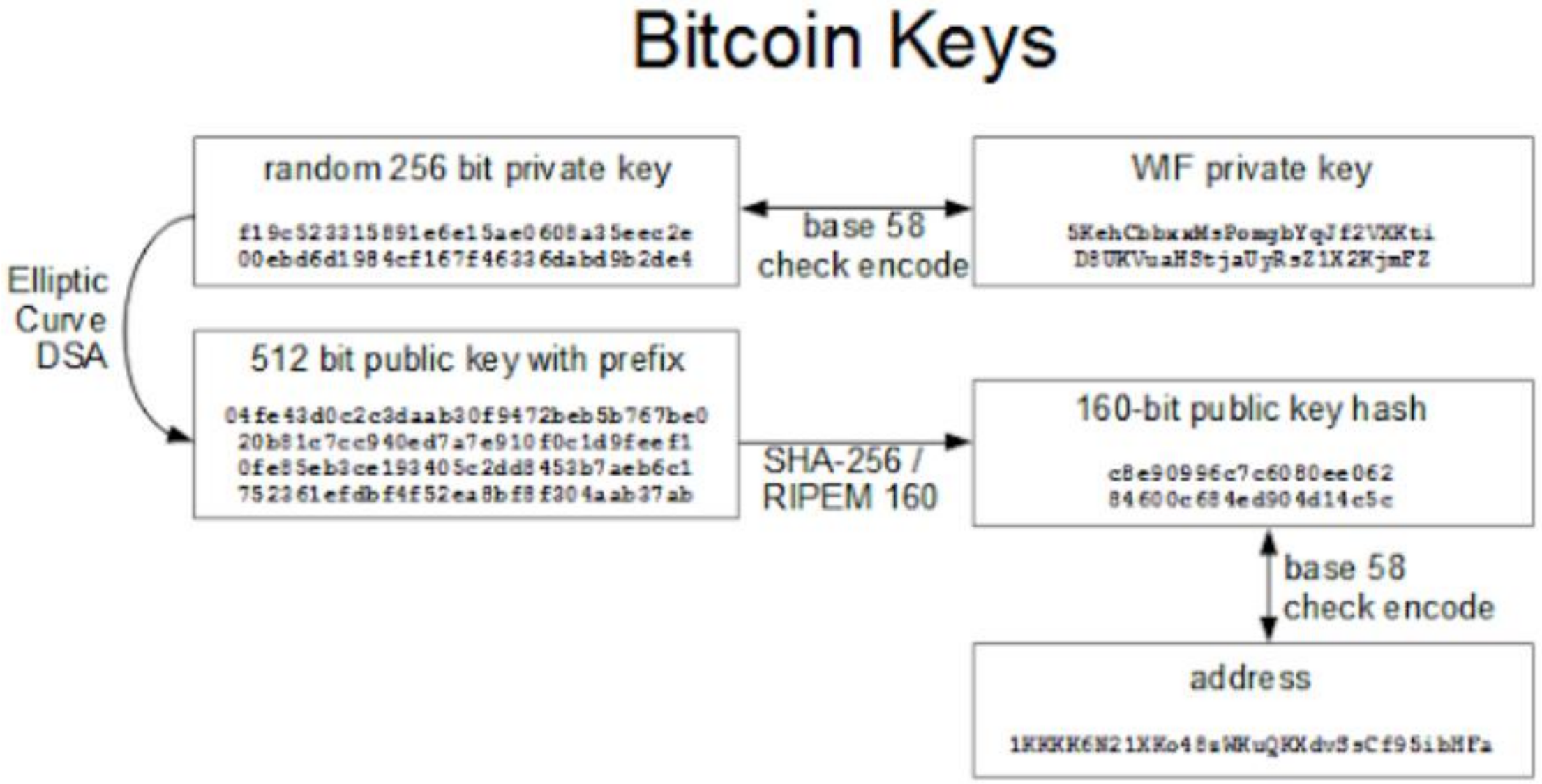
TRANSACTION VERIFIED

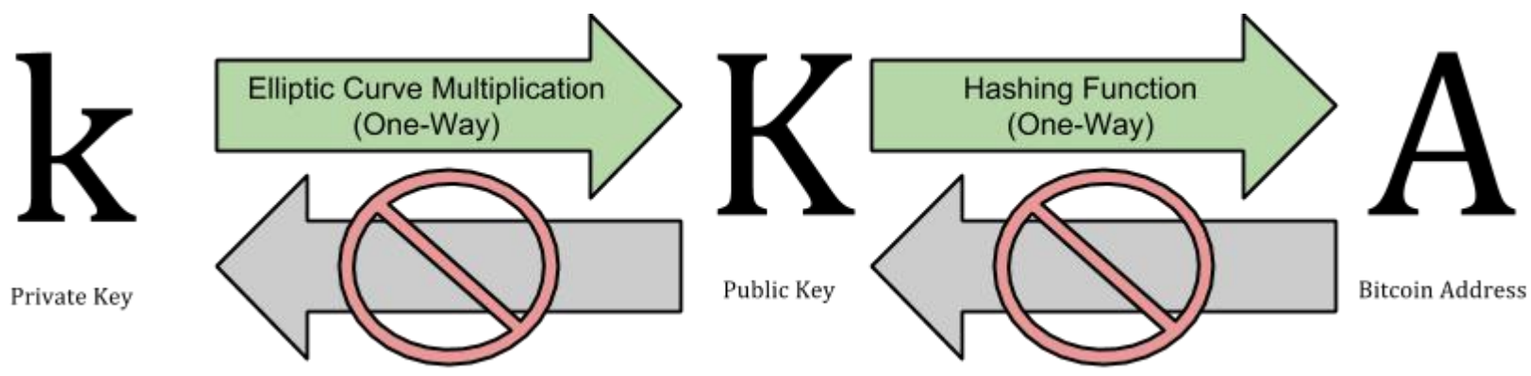


As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

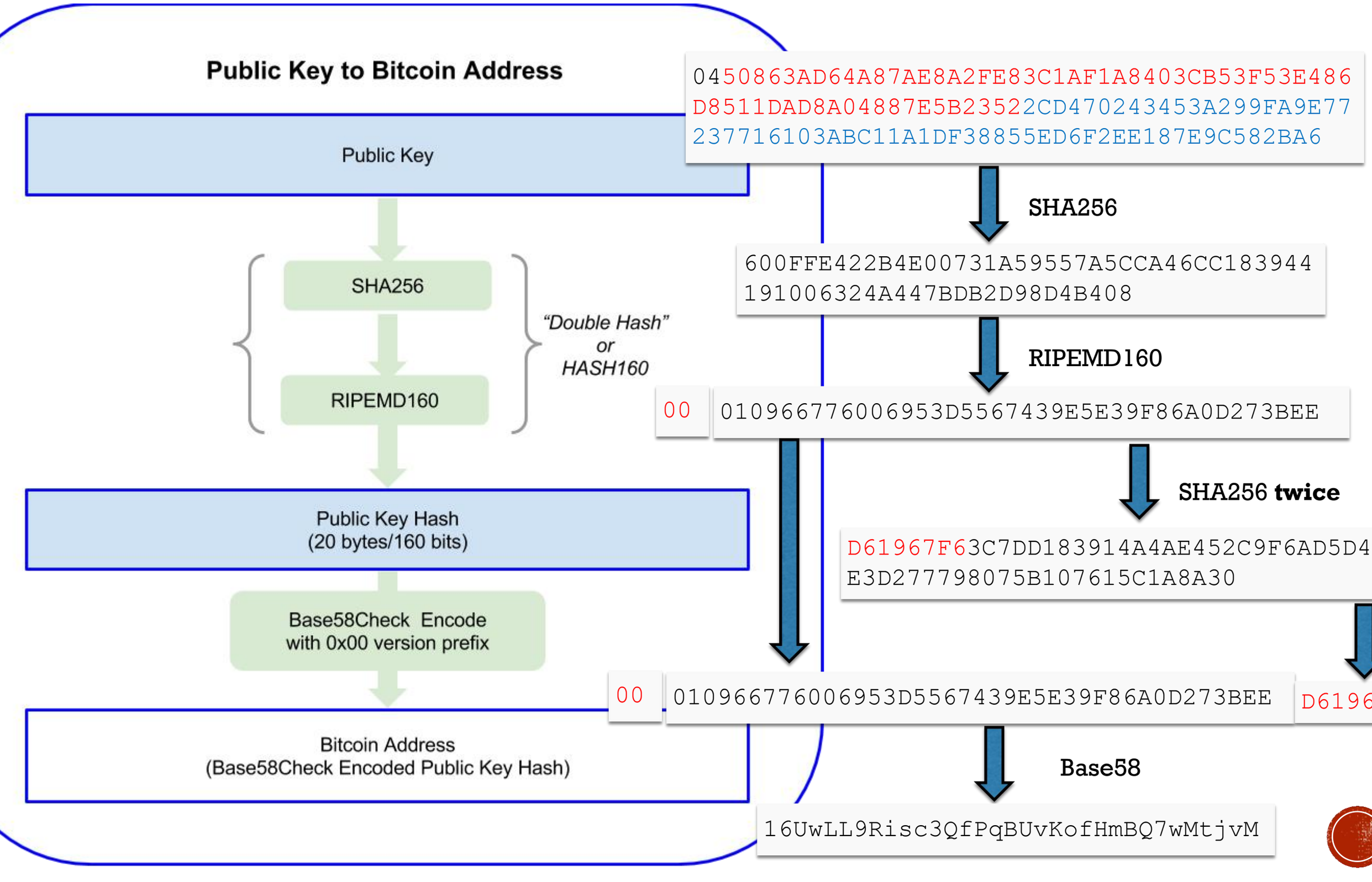
JOSHUA J. ROMERO, BRANDON PALACIO & KARL SSOWWALKER INC.

Bitcoin address and key





Bitcoin address and key



Bitcoin Transaction

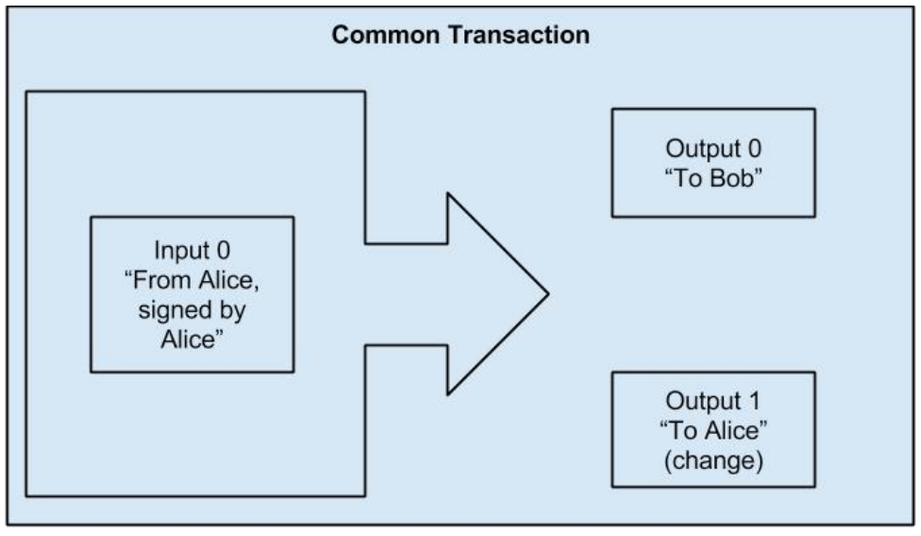
Transaction as Double-Entry Bookkeeping

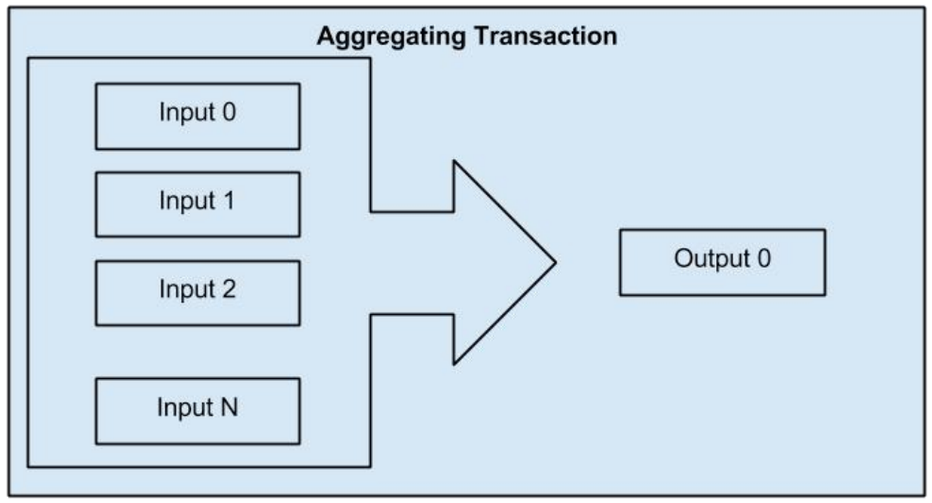
Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

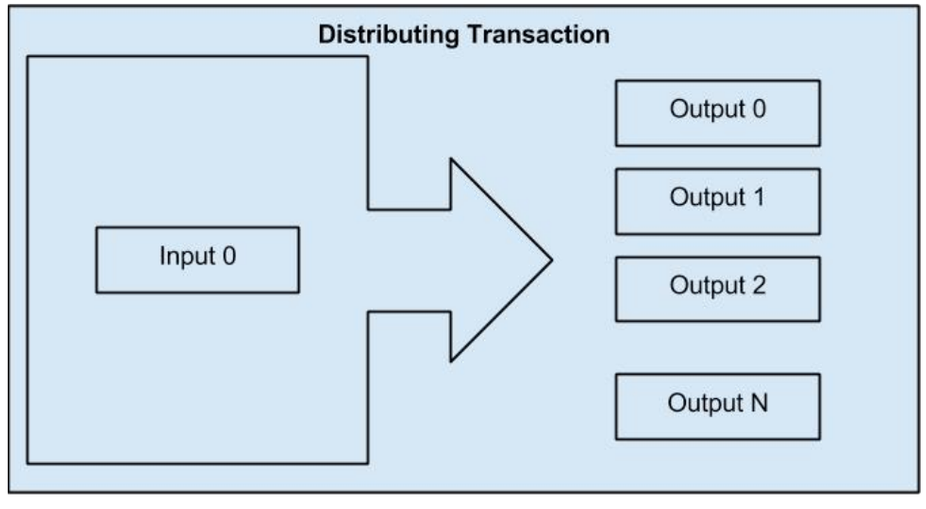
	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

Bitcoin Transaction

- Types of Transactions







Bitcoin Transaction

Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From		OUTPUTS To		
From (previous transactions Joe has received):				
Joe	0.1005 BTC	Output #0 Alice's Address	0.1000 BTC	(spent)
		Transaction Fees:	0.0005 BTC	

Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

INPUTS From		OUTPUTS To		
7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0				
Alice	0.1000 BTC	Output #0 Bob's Address	0.0150 BTC	(spent)
		Output #1 Alice's Address (change)	0.0845 BTC	(unspent)
		Transaction Fees:	0.0005 BTC	

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

INPUTS From		OUTPUTS To		
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0				
Bob	0.0150 BTC	Output #0 Gopesh's Address	0.0100 BTC	(unspent)
		Output #1 Bob"s Address (change)	0.0845 BTC	(unspent)
		Transaction Fees:	0.0005 BTC	

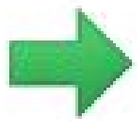
Bitcoin Transaction

http://blockchain.info

Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)



1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (Unspent) 0.015 BTC

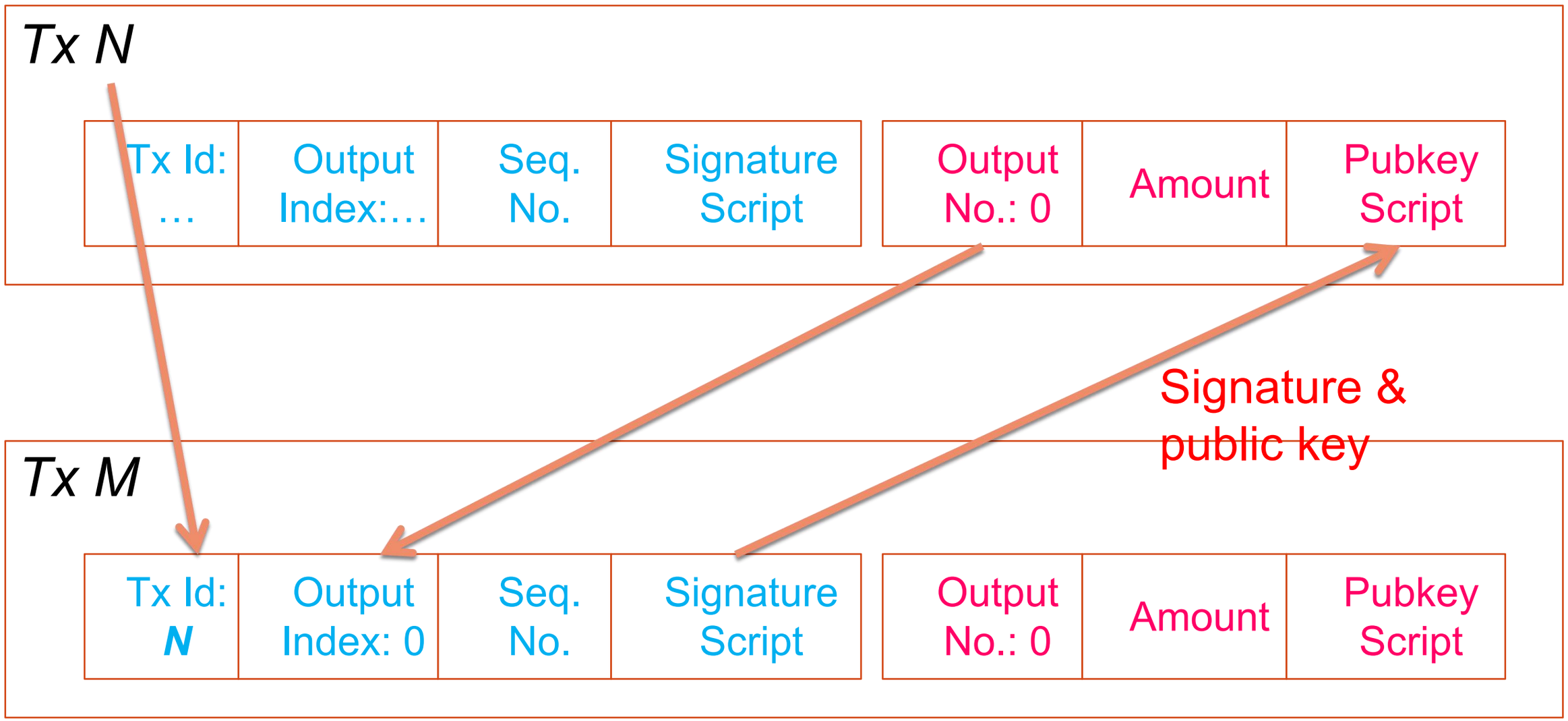
1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (Unspent) 0.0845 BTC

97 Confirmations | 0.0995 BTC

Summary	
Size	258 (bytes)
Received Time	2013-12-27 23:03:05
Included In Blocks	277316 (2013-12-27 23:11:54 +9 minutes)

Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.015 BTC

Transaction Verification



Default Pubkey script only verifies the public key and the signature

- Bitcoin address is hash of public key

References

•[1] Ken Shirriff’s blog, Bitcoins the hard way: Using the raw Bitcoin protocol

•[2] Bitcoin wiki, Technical background of version 1 Bitcoin addresses.

•[3] Mastering bitcoin, O’Reilly Publish

•[4] Bitcoin.org, Developer examples.

Part 2:

Block Mining, Verification and the Blockchain

OUTLINE

- Mining Blocks
  - Verify a transaction
  - Aggregate transactions into a block
  - Mine the new block
  - Validate the new block
  - Assemble the new block to blockchain
- Fork resolving
- Threats against Blockchain

MINING BLOCKS

- Verify a transaction
- Aggregate transactions into a block
- Mine the new block
- Validate the new block
- Assemble the new block to blockchain

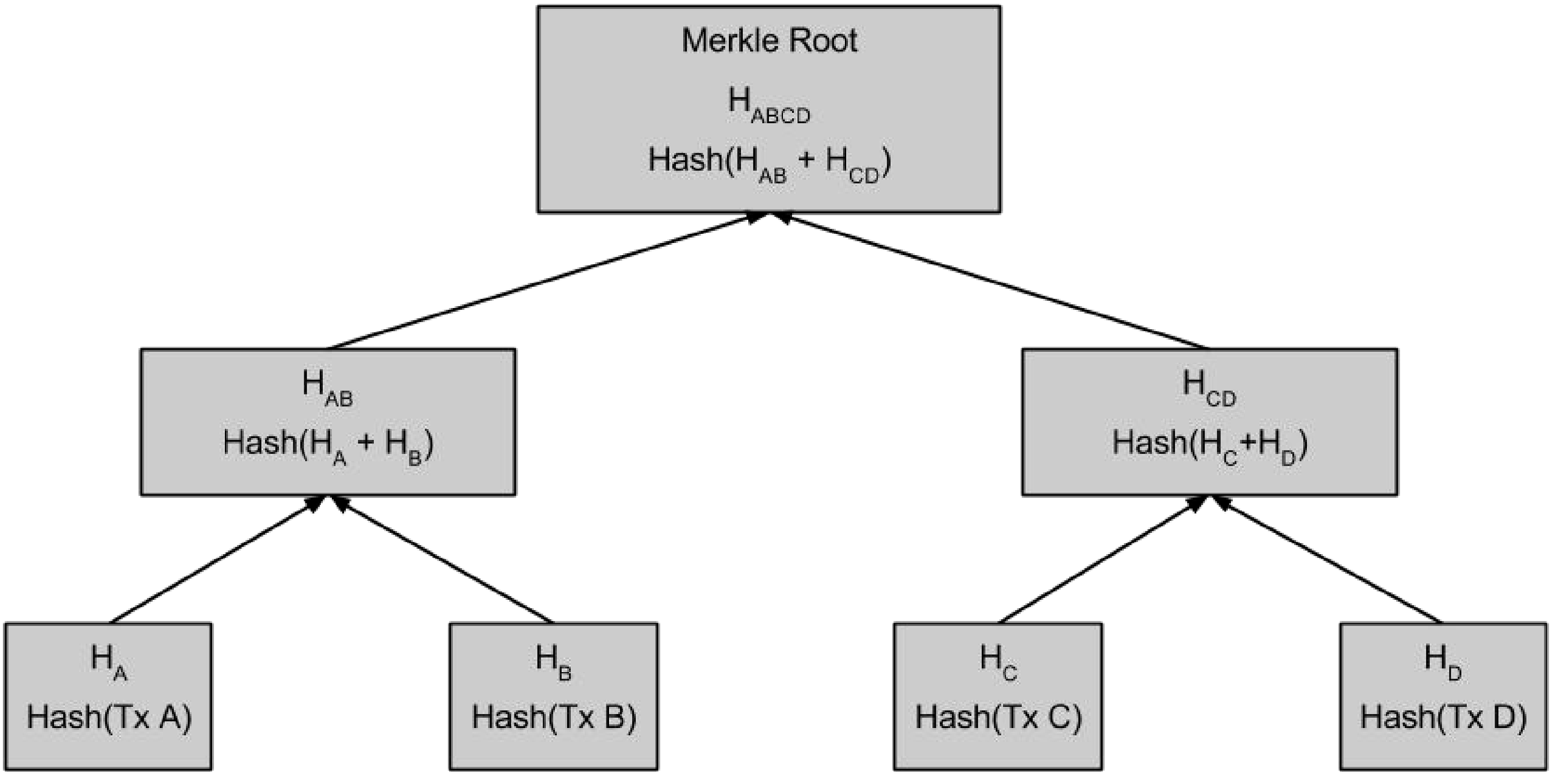
TRANSACTION VERIFICATION

- For each input, the referenced output must exist and cannot already be spent.
- For each input, if the referenced output exists in any other transaction in the pool, reject this transaction.
- Reject if the sum of input values < sum of output values.
- Reject if transaction fee would be too low to get into an empty block.
- The unlocking scripts for each input must validate against the corresponding output locking scripts.

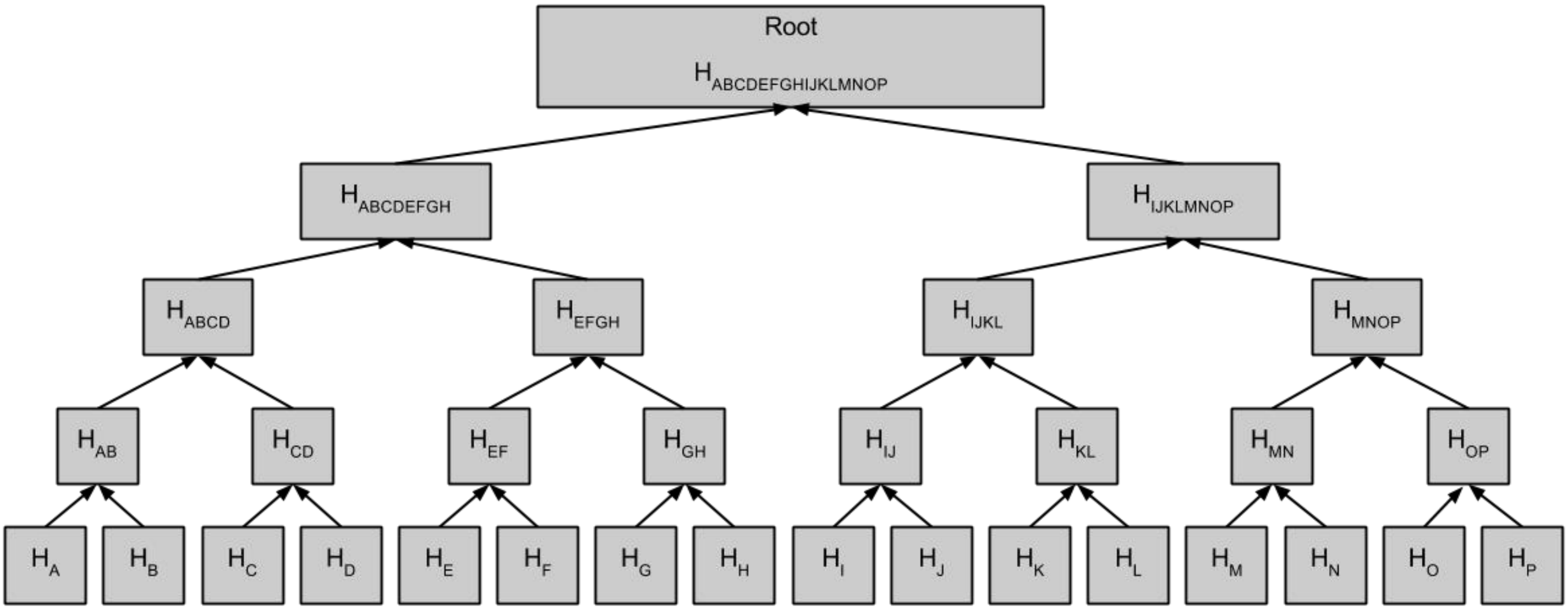
AGGREGATING TRANSACTIONS

- Old and high-value inputs to be prioritized over newer and smaller inputs.
- Prioritized transactions can be sent without any fees, if there is enough space in the block.
- Priority = Sum (Value of input * Input Age) / Transaction Size
  - Value of an input is measured in the base unit, satoshis (1/100m of a bitcoin)
  - Age: the number of blocks that have elapsed
- High Priority > 100,000,000 satoshis * 144 blocks / 250 bytes = 57,600,000

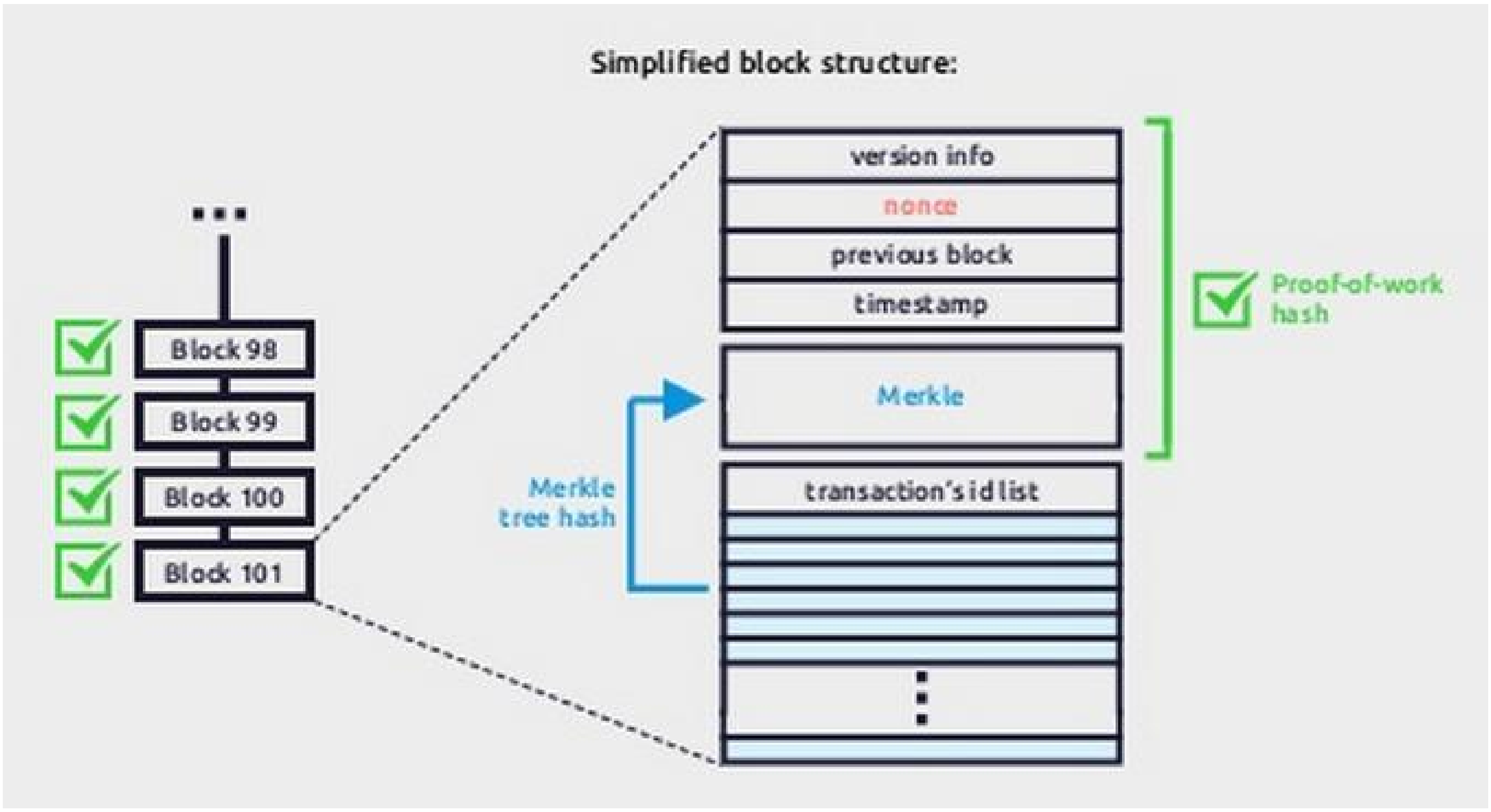
AGGREGATING TRANSACTIONS WITH MERKLE TREE



AGGREGATING TRANSACTIONS WITH MERKLE TREE



AGGREGATING TRANSACTIONS



BLOCK STRUCTURE

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c81701000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

Block hash

000000000000000 e067a478024addfe cdc93628978aa52d 91fabd4292982a50

Block Height 277316
Header Hash:
000000000000001b6b9a13b095e96db 41c4a928b97ef2d944a9b31b2cc7bdc4

Previous Block Header Hash:
0000000000000002a7bbd25a417c0374 cc55261021e8a9ca74442b01284f0569
Timestamp: 2013-12-27 23:11:54
Difficulty: 1180923195.26
Nonce: 924591752
Merkle Root: c91c008c26e50763e9f548bb8b2 fc323735f73577effbc55502c51eb4cc7cf2e

Transactions

HEADER

Block Height 277315
Header Hash:
0000000000000002a7bbd25a417c0374 cc55261021e8a9ca74442b01284f0569

Previous Block Header Hash:
0000000000000027e7ba6fe7bad39fa f3b5a83daed765f05f7d1b71a1632249
Timestamp: 2013-12-27 22:57:18
Difficulty: 1180923195.26
Nonce: 4215469401
Merkle Root: 5e049f4030e0ab2debb92378f5 3c0a6e09548aea083f3ab25e1d94ea1155e29d

Transactions

Block Height 277314
Header Hash:
0000000000000027e7ba6fe7bad39fa f3b5a83daed765f05f7d1b71a1632249

Previous Block Header Hash:
000000000000000038388d97cc6f2c1d fe116c5e879330232f3bff1c645920bdf
Timestamp: 2013-12-27 22:55:40
Difficulty: 1180923195.26
Nonce: 3797028665
Merkle Root: 02327049330a25d4d17e53e79f 478cbb79c53a509679b1d8a1505c5697afb326

Transactions

GENESIS BLOCK

- Bitcoin-cli getblockhash 0
- Bitcoin-cli getblock 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f


```
{
    "hash" : "000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
    "confirmations" : 308321,
    "size" : 285,
    "height" : 0,
    "version" : 1,
    "merkleroot" : "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
    "tx" : [
        "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"
    ],
    "time" : 1231006505,
    "nonce" : 2083236893,
    "bits" : "1d00ffff",
    "difficulty" : 1.00000000,
    "nextblockhash" : "00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048"
}
```

THE COINBASE TRANSACTION

- Coin generation

Transaction View information about a bitcoin transaction

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

No Inputs (Newly Generated Coins) → 1A1zP1eP5Q... (Genesis of Bitcoin) - (Unspent) 50 BTC

50 BTC

Summary	
Size	204 (bytes)
Received Time	2009-01-03 18:15:05
Reward From Block	0
Scripts	Hide scripts & coinbase
Relayed by IP	0.0.0.0 (whois)
Visualize	View Tree Chart

CoinBase

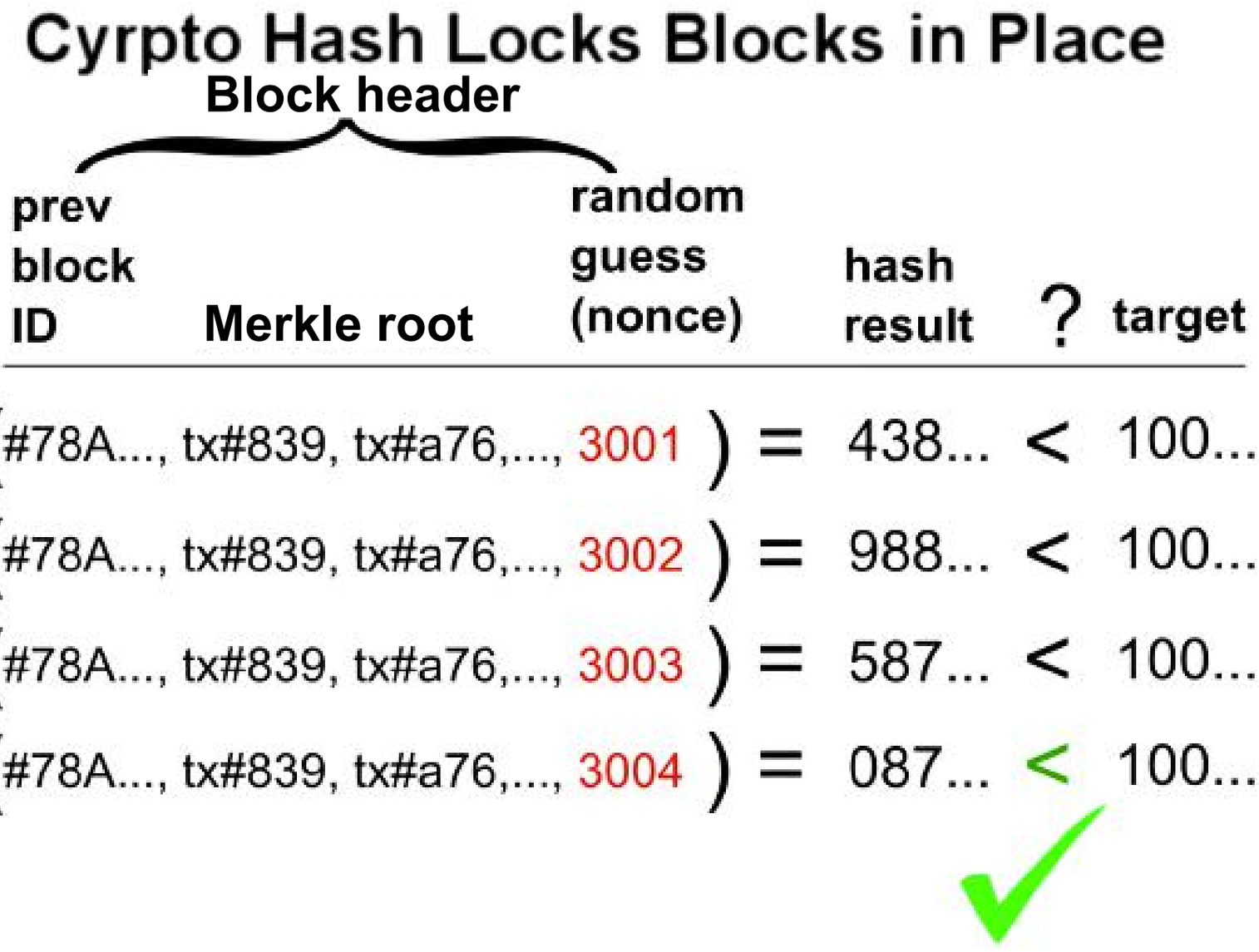
04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f75742
(decoded) ��EThe Times 03/Jan/2009 Chancellor on brink of second bailout for banks

Output Scripts

04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f C
OP_CHECKSIG

MINING A BLOCK

- SHA256(SHA256(Block_header))<Difficulty_target
- Transactions are hashed through Merkle root



DIFFICULTY OF MINING

DIFFICULTY and TARGET

- Target: E.g. 0x1903a30c
  - The exponent is 0x19 and the coefficient is 0x03a30c.
  - target = coefficient * 2^(8 * (exponent – 3))
  - For difficulty bits value 0x1903a30c, we get:
  - target = 0x03a30c * $2^{(0x08 * (0x19 - 0x03))}$
  - ⇒ target = 0x03a30c * $2^{(0x08 * 0x16)}$
  - ⇒ target = 0x00000000000003A30C000000000000000000000000000000000000
- Difficulty = Difficulty_1_Target/Current_Target
- New Target = Old Target * (Actual Time of Last 2016 Blocks / 20160 minutes)

MINING BLOCKS

- Chance of success is less than one in 10^{19}.
- Harder than finding a particular grain of sand from all the grains of sand on Earth
- Every second about 25,000,000,000,000,000 blocks gets hashed
- Total hardware used for mining cost tens of millions of dollars
- Uses as much power as the country of Cambodia

MINING BLOCKS

- Nonce size: 4 bytes, 32-bit
  - Current ASIC can exhaust all possible nonce in a second (4G Hash per second, 4 billinion).
  - Use coinbase script (8 bytes more) and timestamp as nonce source
- Pool mining: Predictable return
  - Successful blocks pay the reward to a pool bitcoin address
  - Miners get paid periodically by pool server
  - How to measure each miner's contribution?
  - Mining pool sets a lower difficulty target for earning a share, typically more than 1,000 times easier than the bitcoin network's difficulty

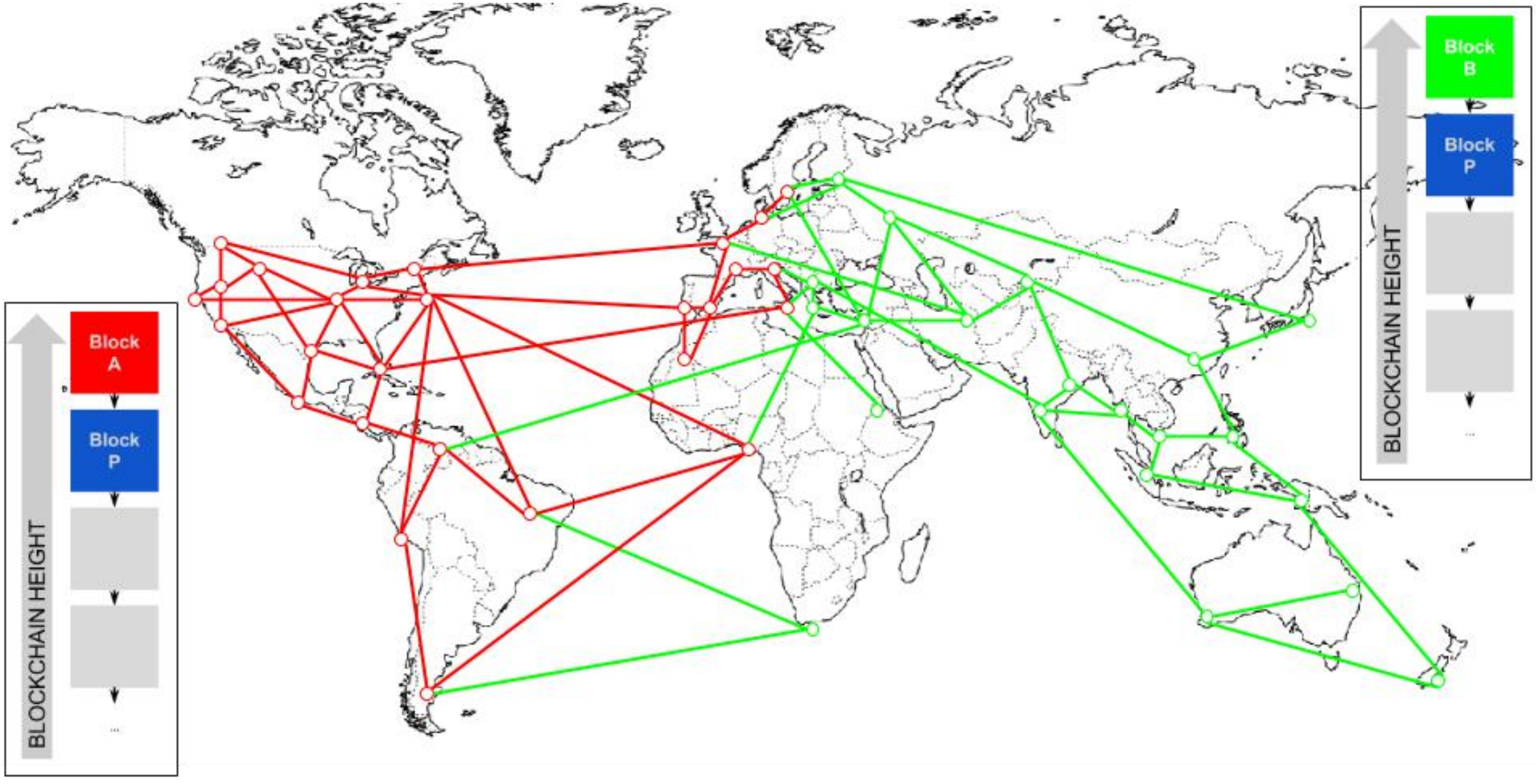
VALIDATING BLOCKS

- The block data structure is syntactically valid
- The block header hash is less than the target difficulty (enforces the Proof-Of-Work)
- The block timestamp is less than two hours in the future (allowing for time errors)
- The block size is within acceptable limits
- The first transaction (and only the first) is a coinbase generation transaction
- All transactions within the block are valid

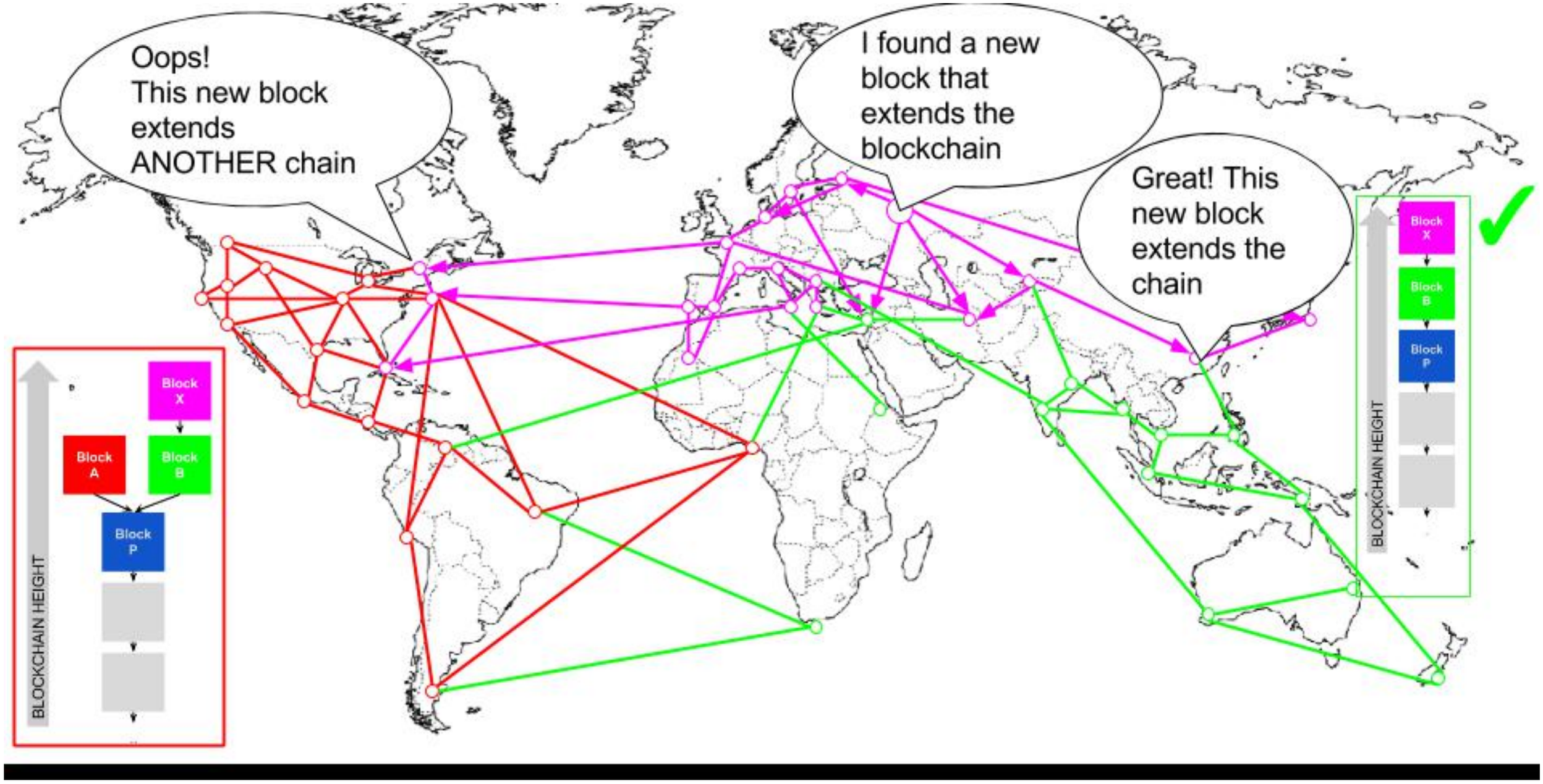
ASSEMBLING BLOCKS

- Three sets of blocks:
  - Blocks connected to the main blockchain,
  - Blocks that form branches off the main blockchain (secondary chains)
  - Blocks that do not have a known parent in the known chains (orphans).
- Blockchain forks
  - Select the chain with higher cumulative difficulty as the main chain

BLOCKCHAIN FORK

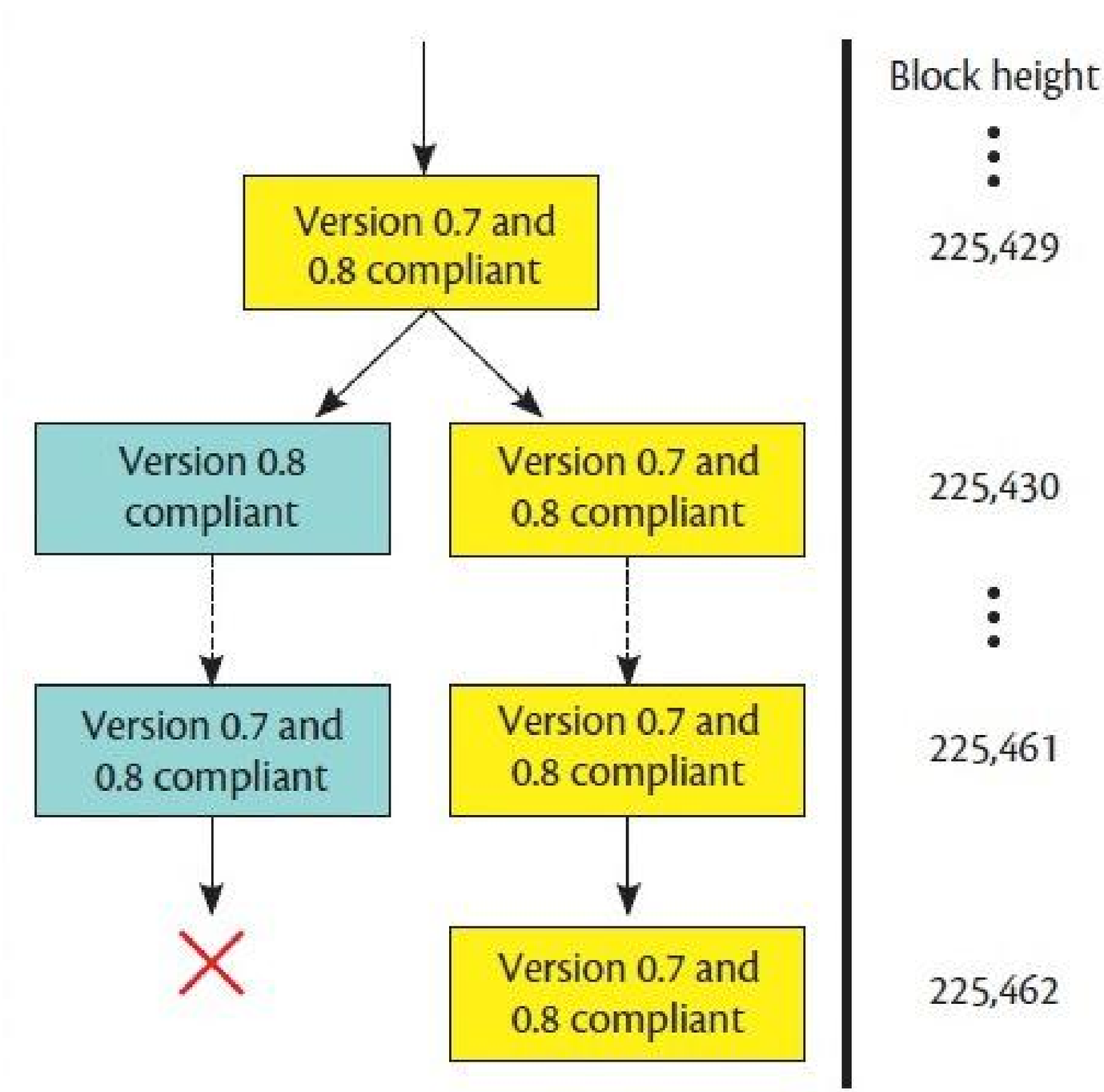


BLOCKCHAIN FORK



BLOCKCHAIN FORK

- The block chain fork that occurred on 11 March 2013.
- Despite less support from users, version 0.7 was chosen by developers to be the official chain.

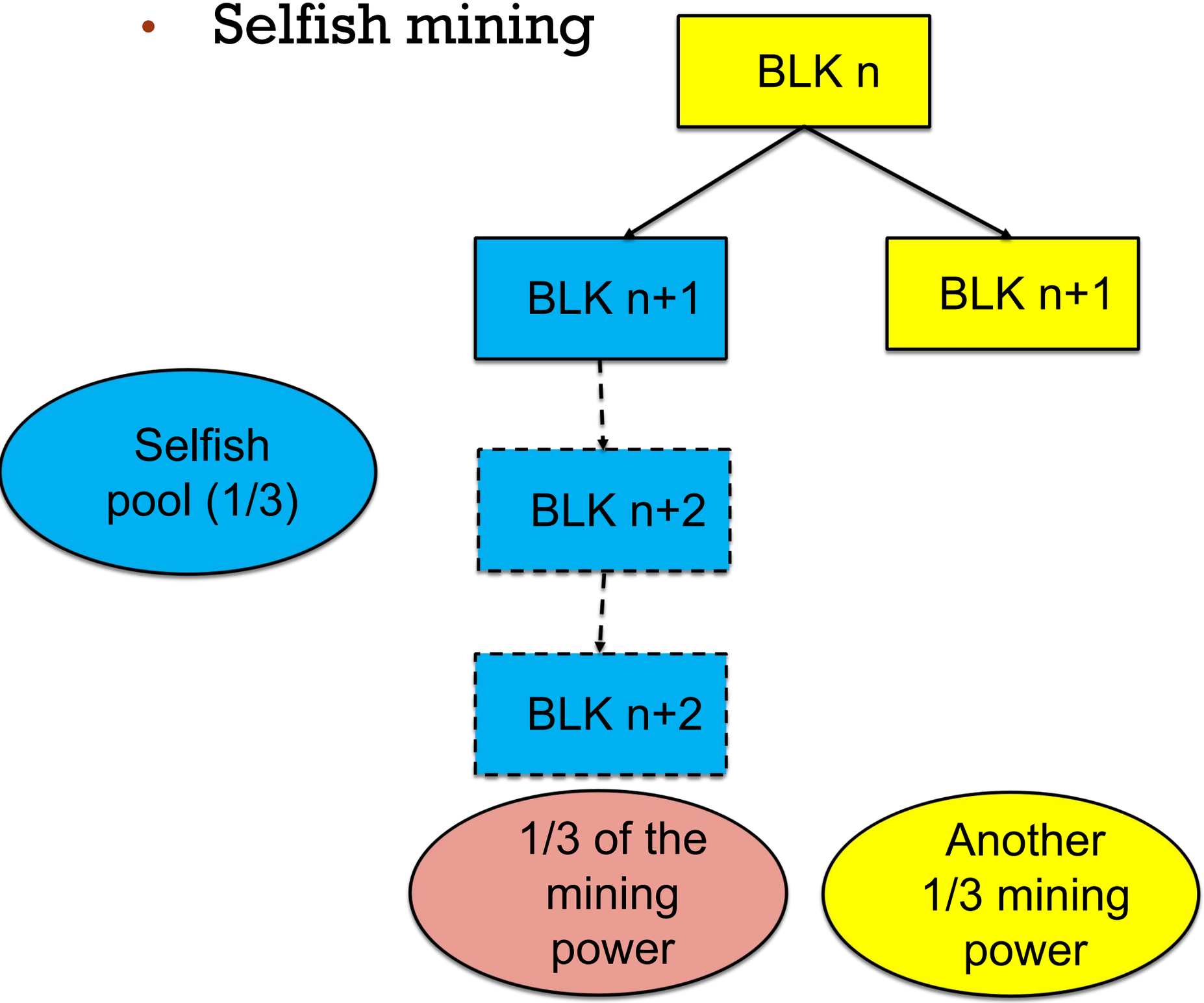


THREATS AGAINST BLOCKCHAIN

- 51% attack
  - A group of miners, controlling a majority (51%) of the total network's hashing power, collude to attack bitcoin.
  - Effects
    - Double-spend one's own bitcoins
    - Delay others' txn confirmations
    - Cannot destroy/steal bitcoins
- 33% attack: selfish mining

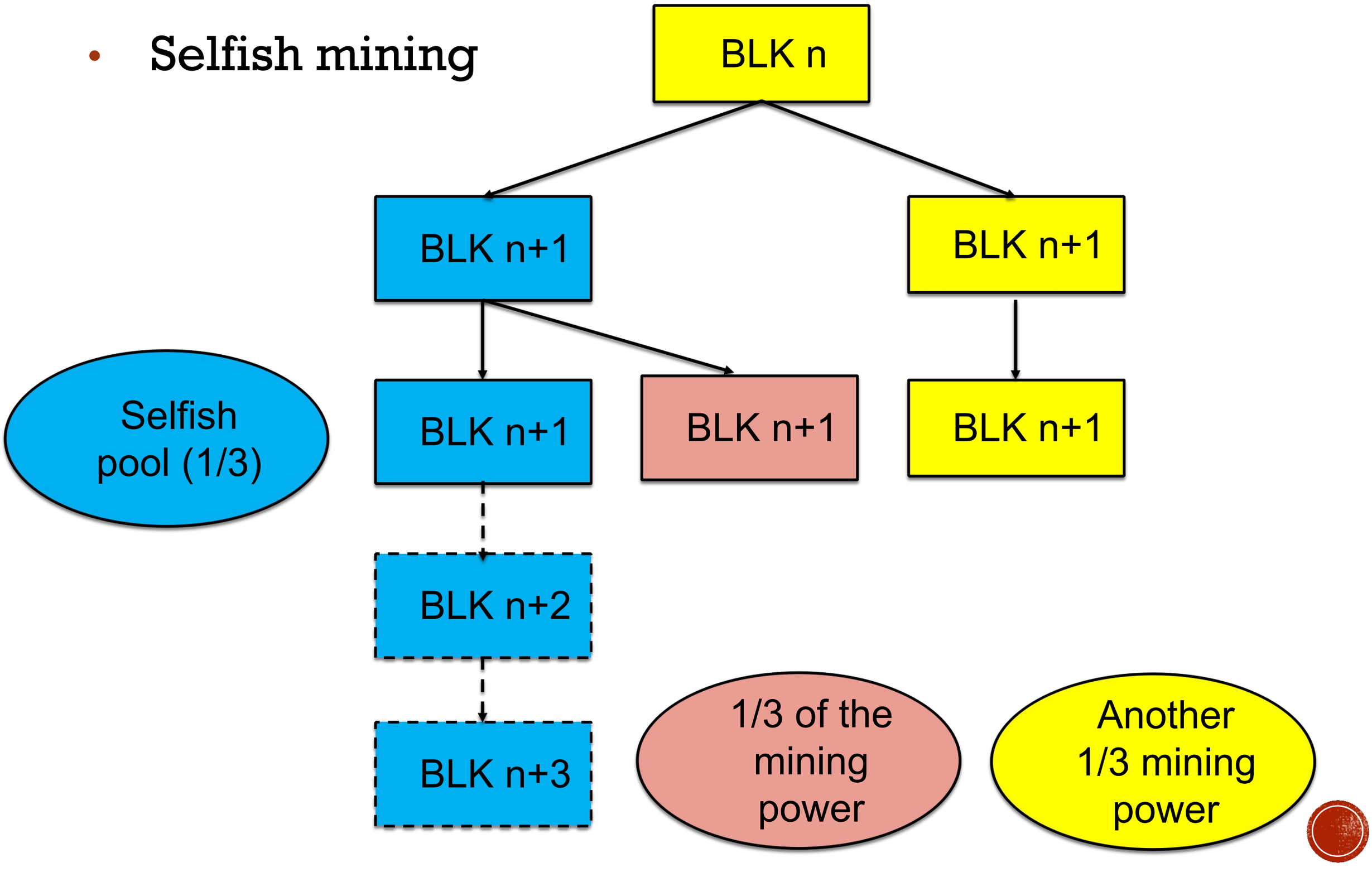
THREATS AGAINST BLOCKCHAIN

- Selfish mining



THREATS AGAINST BLOCKCHAIN

- Selfish mining

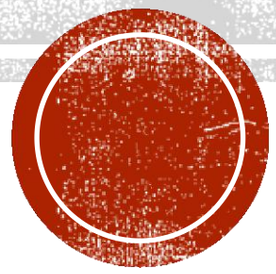


REFERENCES

- Is Bitcoin a Decentralized Currency? IEEE Security & Privacy magazine
- Mastering bitcoin, O'Reilly Publishing
- Ken Shirriff, Bitcoin mining the hard way: the algorithms, protocols, and bytes, http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html
- Majority is not Enough: Bitcoin Mining is Vulnerable, Financial crypto'14.

Part 3:
Blockchain Innovations

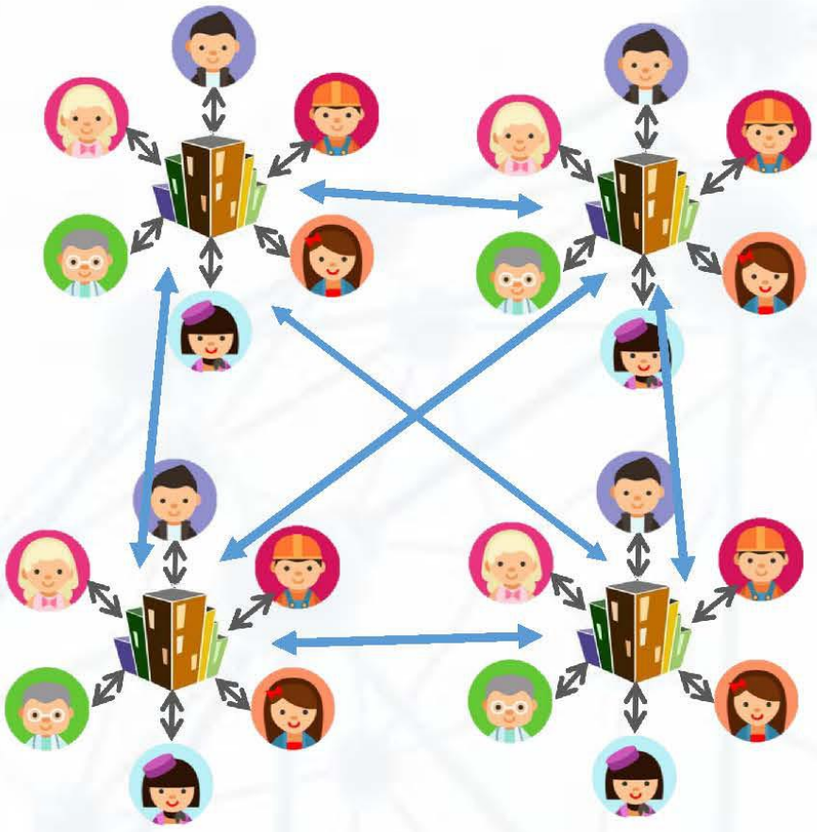
(Content from Prof. David Lee)



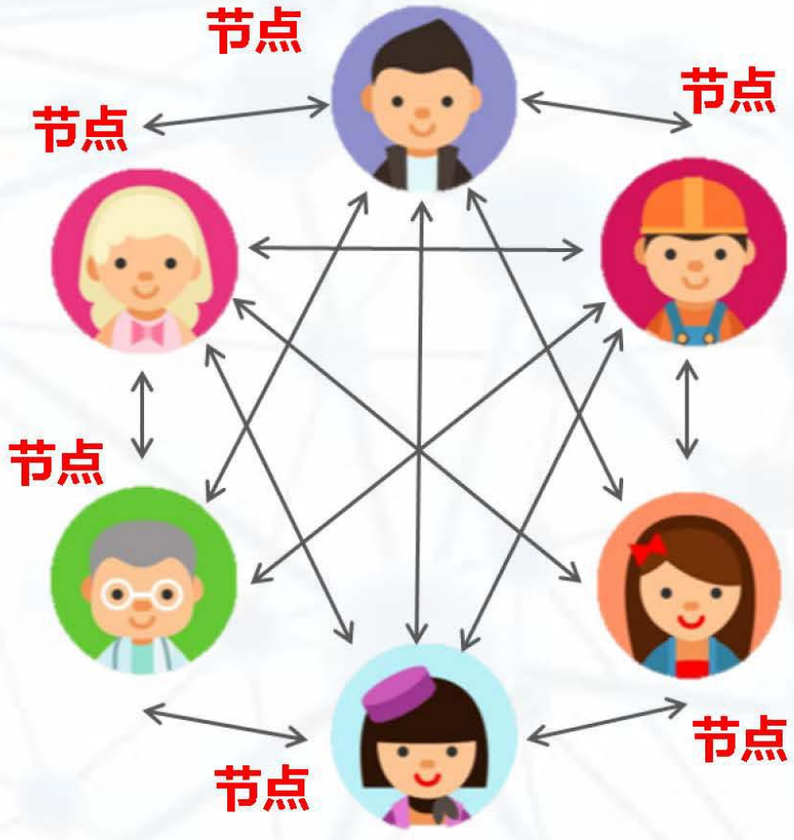
区 块 链 介 绍

集中平台 ⇒ 分布式

集中平台



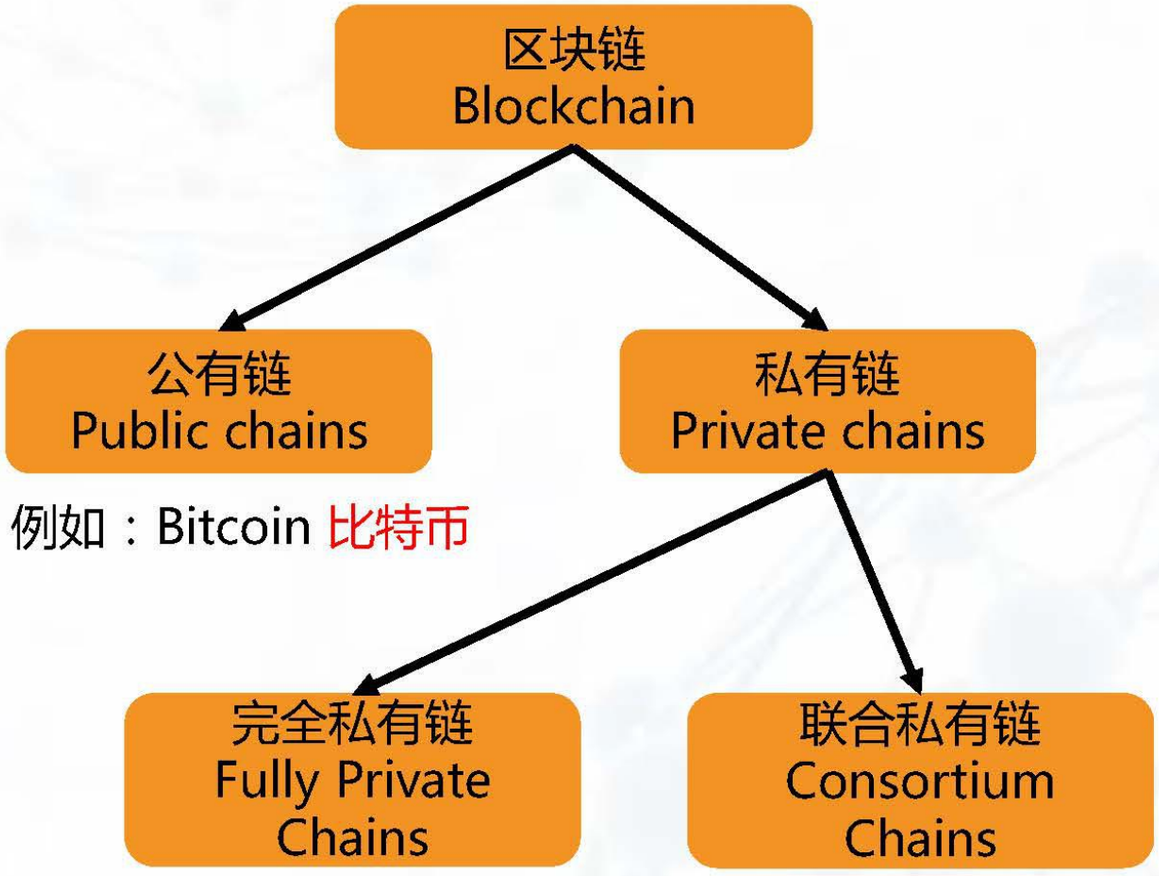
分散型(去中心化)



分布式

(C) DavidKuoChuenLee

区块链的类型



例如：Bitcoin 比特币

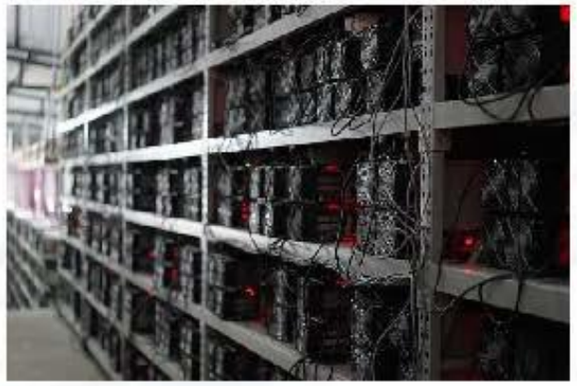
例如：R3 CEV
银行领域

区块链特点

- **分散性**
  - 每个节点遵循同一记账交易规则，规则基于加密算法
- **共识信任机制**
  - 每笔交易需要网络内其他用户批准
- **不可篡改和加密安全性**
  - 新的区块产生按照时间序列不可更改（除非可控制系统内51%以上节点），区块链内信息可被追溯
- **开放性**
  - 数据对所有人公开
- **匿名性**
  - 节点间无需公布身份，交易双方通过地址传递信息
- **跨平台**
  - 节点基于共同的算法和数据结构独立运行，任何平台都可部署计算节点

(C) DavidKuoChuenLee

来源： http://www.8btc.com/what-is-blockchain; http:// community.qingcloud.com; https://blog.ethereum.org



区块链 是分散型（去中心化）分布式数据库

(C) DavidKuoChuenLee

区块链应用领域


通信领域

投票领域


医疗领域


公证领域


银行领域


股权认证/交易

保险领域

域名领域


物联网

……

(C) DavidKuoChuenLee

图片来源：百度图片

通 信 领 域

传统的通讯工具的设计思路：
所有节点中找最短的路径或者是最快的路径

比特信实现去中心化的方式：
- 信息发给全网的每一个人，只有有钥 匙的人才可以打开
- 信息源可以避免被追踪
- 既实现从信息安全也实现了路径安全

GetGems也实现去中心化的方式：
- 通讯功能与比特信类似
- 加入了比特币钱包功能
- 用户可交易和赚取其加密货币“gems”
- 加入了新理念：用户点击广告能赚钱

(C) DavidKuoChuenLee

区块链应用领域


通信领域

投票领域


医疗领域


公证领域


银行领域


股权认证/交易

保险领域

域名领域


物联网

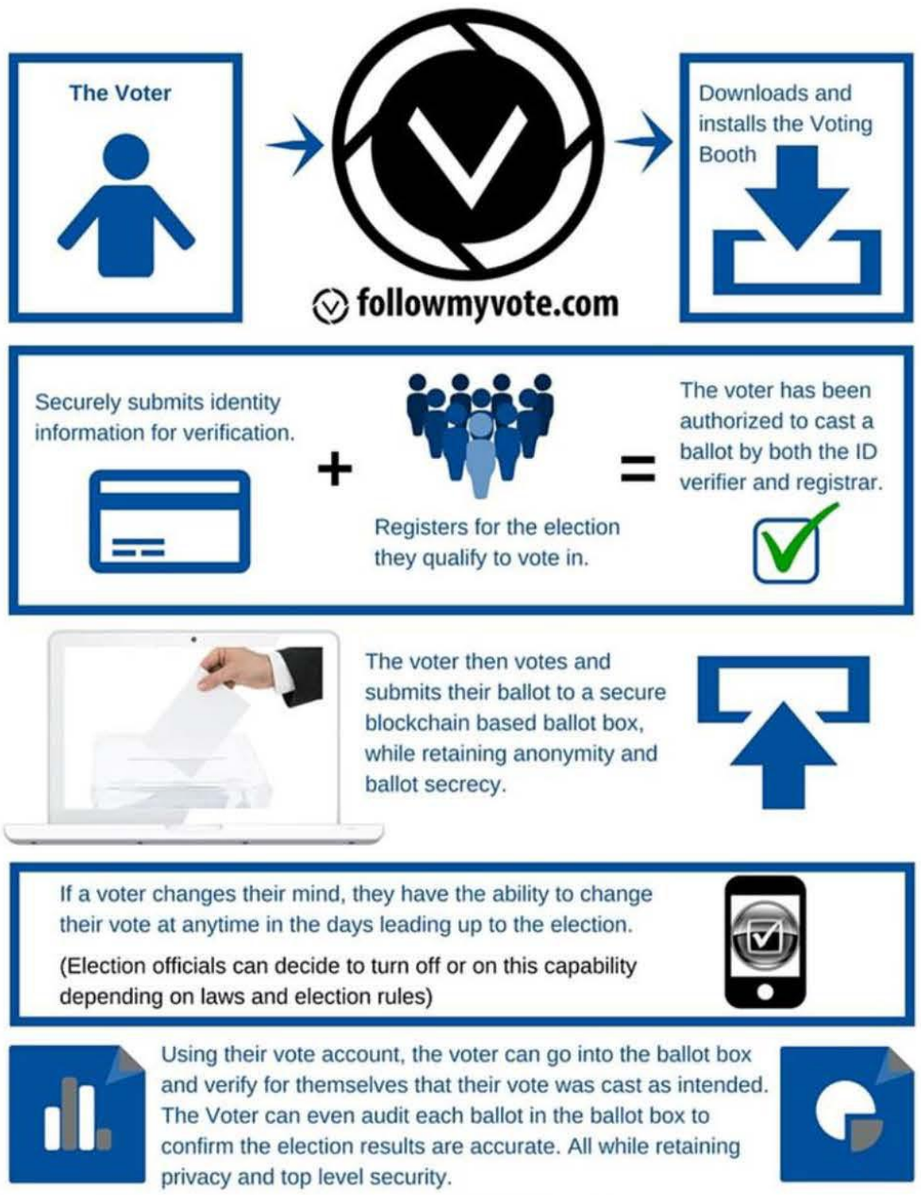
……

(C) DavidKuoChuenLee

图片来源：百度图片

投 票 领 域

followmyvote.com



流程：

- 投票人下载安装投票插件
- 保密性地验证个人身份，注册选举投票，获得ID账号
- 投票人提交其决定给投票箱，但仍有匿名性和保密性
- 如果投票人改变主意，可以在选举结束前更改投票（选举方可依据政策关闭此功能）
- 投票人可查看其投票是否已投递成功。投票人甚至可以审查每一票以确保结果精确。所有的投票仍是及其保密的。

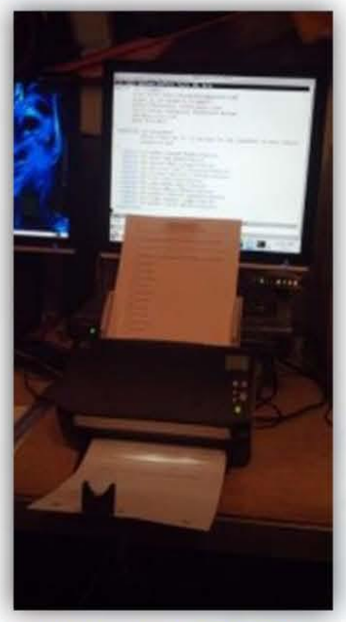
来源： https://followmyvote.com/

投 票 领 域

美国现有的投票机

美国现有的投票机技术已经很陈旧，很多州使用的机器已有十年之久，维护成本高，且有作弊的可能。基于区块链技术的投票机提供了解决方案。

BLOCKCHAIN TECHNOLOGIES CORP



区块链算法投票机：

- 完整的投票系统
- 专注于安全：多重稽核轨迹（文本稽核与区块链稽核）
- 使用前所未有的创新技术
- 提供投票者可设计的熟悉的操作界面

(C) DavidKuoChuenLee

区块链对于投票意味着:

- 投票机可检验的源代码
- 通过消除多于注册的投票人数的投票数的情况防止作弊现象
- 及时、透明和不可操纵的投票数据
- 极低的成本，易于实施

区块链算法投票机意味着:

- 对于投票机可检验的源代码
- 确认选民资格
- 防止作弊现象
- 及时、透明和不可操纵的投票数据
- 极低的成本，易于实施
- 安全性：多重稽核轨迹（文本稽核与区块链稽核）
- 防止网络攻击、恶意软件
- 确保选民记录和个人信息安全

来源:http://blockchaintechcorp.com/blockchain-apparatus/blockchain-voting-machine/

区块链应用领域


通信领域

投票领域


医疗领域


公证领域


银行领域


股权认证/交易

保险领域

域名领域

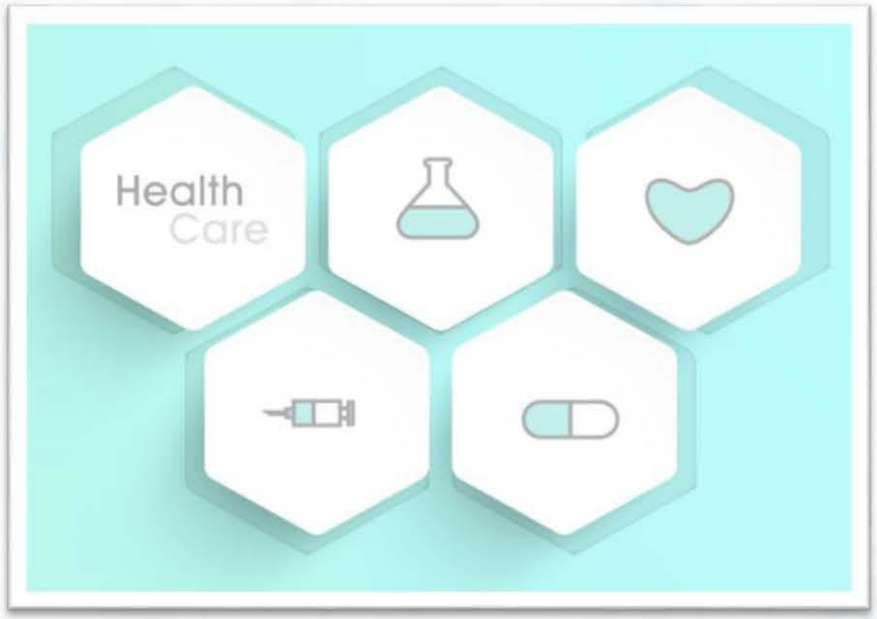

物联网

……

(C) DavidKuoChuenLee

图片来源：百度图片

医 疗 领 域



应用：

人口健康；医疗记录；患者数据

优点：

- 提高医疗服务的透明度
- 保护患者隐私（保险公司，贷款方和患者都使用同一个区块链管理支付）
  - 大规模数据泄露例子：Anthem 8000万病人和雇员的记录；UCLA Health 450万病人
- 提高医疗收费过程的效率

guardtime
Keyless Signatures for Data™

爱沙尼亚（Estonia）政府与Guardtime公司的合作

healthbank.ch
Rewarding Health.

Healthbank：区块链技术，允许个人自己掌握信息（医生和临床访问生成的患者数据）

(C) DavidKuoChuenLee

区块链应用领域


通信领域

投票领域


医疗领域


公证领域


银行领域


股权认证/交易

保险领域

域名领域


物联网

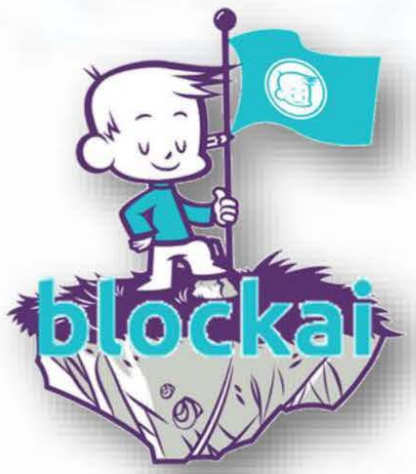
……

(C) DavidKuoChuenLee

图片来源：百度图片

公 证 领 域

区块链的不可更改的和不可伪造性使得其可在公证领域广泛的应用。



Blockai致力于打造一种新工具，允许**艺术家证明或声明自己对图片拥有版权**

Stampery 想用区块链 代替公证人，致力为**敏感文件**提供具有法律约束力的证明。

Chronicled利用区块链技术来帮助验证收藏类运动鞋

Uproov将探索区块链**时间戳的潜力**，允许任何人证明实质上的任何东西，而不需要“受信方”的参与

来源：http://www.8btc.com/blockchain-item?tagname=%E5%85%AC%E8%AF%81%E9%98%B2%E4%BC%AA

(C) DavidKuoChuenLee

公 证 领 域

区块链的不可更改的和不可伪造性使得其可在公证领域广泛的应用。

Bitproof.io

区块链公证公司Bitproof使用一种新的区块链技术打造一站式教育证书

VECHAIN
AUTHENTIC ITEM

BitSE公司发布了全球首个基于区块链技术的真假校验平台唯链（VeChain）

factom利用比特币的区块链技术来革新商业社会和政府部门的数据管理和数据记录方式。

来源：http://www.8btc.com/blockchain-item?tagname=%E5%85%AC%E8%AF%81%E9%98%B2%E4%BC%AA

(C) DavidKuoChuenLee

区块链应用领域


通信领域

投票领域


医疗领域


公证领域


银行领域


股权认证/交易

保险领域

域名领域


物联网

……

(C) DavidKuoChuenLee

图片来源：百度图片

银 行 领 域

- 例如，现金转账
  - 过去：你=>银行=>朋友
  - 未来：你=>朋友
- 国际清算银行（BIS）研究报告：
  区块链技术的发展，可能会影响目前中央银行的运作模式

银行采用区块链技术优点

- **安全**：不可篡改性，可追踪性
- **监管方便**：使用实名制区块链（赋予节点具有不同身份：联盟，发行者，一般使用者）
- **运营成本低**
- **降低金融交易清算时间**：UBS白皮书：业务处理时间缩短至15秒 - 4天
- **降低交易成本**：桑坦特Santander银行：2015年利用区块链技术可为银行业减少2000万美元支出
- **降低交易对手风险**

(C) DavidKuoChuenLee

来源：http://www.businessinsider.sg/11-banks-in-r3-consortium-use-blockchain-technology-to-trade-2016-1/?r=UK&IR=T

银行领域 R3

HSBC RBS The Royal Bank of Scotland UBS NATIXIS

BMO Financial Group WELLS FARGO TD Bank CREDIT SUISSE

CommonwealthBank BARCLAYS UniCredit

区块链在银行领域的应用：从愿景到现实

- 全球42家银行组成区块链联盟R3，共同开发区块链
- 11个成员开始用区块链进行模拟相互交易

(C) DavidKuoChuenLee

区块链应用领域

通信领域

投票领域

医疗领域

公证领域

银行领域

保险领域

域名领域

物联网

……

(C) DavidKuoChuenLee

图片来源：百度图片

股权/有价证券交易所

1 比特股系统

传统交易所的流程

去中心化的流程

- 真正实现点对点交易，整个交易完全公开透明
- 所有企业可以发行自己的可交易股份
- 系统是开源的，可实现每秒上万笔交易撮合量

2 区域链证券交易系统

- 主要用于私人公司的股权交易
- 系统未开源
- Overstock 和纳斯达克的Linq项目正在打造此系统

(C) DavidKuoChuenLee

区块链应用领域


通信领域

投票领域


医疗领域


公证领域


银行领域


股权认证/交易

保险领域

域名领域


物联网

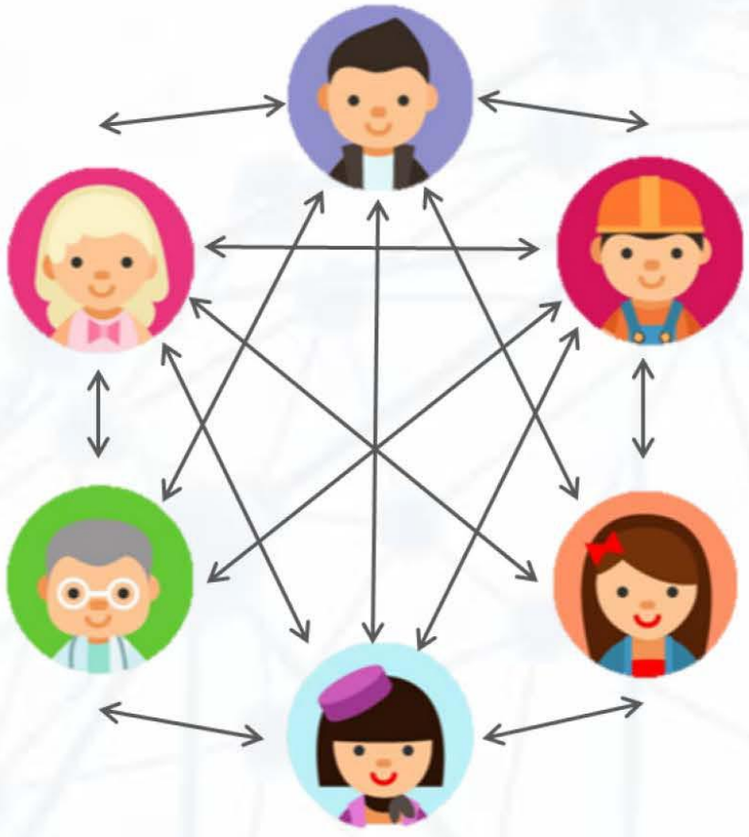
……

(C) DavidKuoChuenLee

图片来源：百度图片

保 险 领 域

传统保险流程



去中心化的流程

保险模式

- 所有数据写入区域链中
- 任何人随时都可以参与和退出
- 没有资金池

优势

- 区域链的公正和不可篡改的特性完成了自证公平
- 去中心化和去中介化，使得资金利用率达到了最高

(C) DavidKuoChuenLee

区块链应用领域

通信领域

投票领域

医疗领域

公证领域

银行领域

股权认证/交易

保险领域

域名领域

物联网

……

(C) DavidKuoChuenLee

图片来源：百度图片

域名服务器系统

区块链技术在很多领域都能产生重大影响，其中之一就是在域名和**DNS**服务器方面。

如果我们能够分散**DNS**服务的话，那么域名将会更加安全。而这一壮举会使转让域名所有权更加方便。

Blockstack公司看起就有这样的想法，因为他们已经提出了一种以区块链为基础的**DNS**系统。

http://www.8btc.com/blockstack-blockchain-decentralize-dns

(C) DavidKuoChuenLee

区块链应用领域

通信领域

投票领域

医疗领域

公证领域

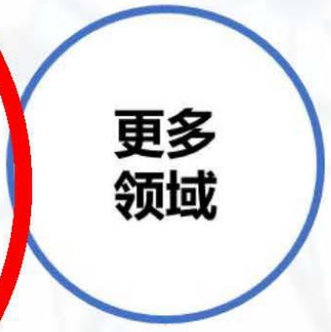
银行领域

股权认证/交易

保险领域

域名领域

物联网

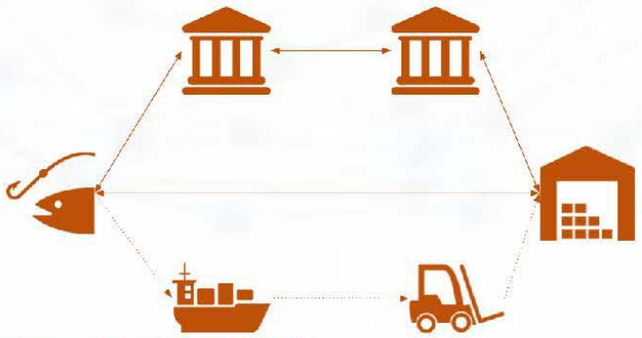


……

(C) DavidKuoChuenLee

图片来源：百度图片

物　联　网



现下的供应链，卖家买家和他们的银行都存在关系。银行之间又存在一层关系。

未来的供应链，仍会保持同样的关系链，但是物流和现金流有更高的可信度和能见度。

解决问题之一：
拉菲每年生产一万，中国却有几十万销量

- IBM 与三星联合打造 **ADEPT 系统**，打造去中心化的物联网
- ADEPT 是指去中心化的 p2p 自动遥测系统，旨在为交易提供最优的安全保障
- 支撑 ADEPT 系统的协议包括：BitTorrent（文件分享）、Ethereum（智能合约）和TeleHash（p2p 信息发送系统）
- 在该系统下，只要一个产品组装完成，生产商就可以把它注册进一个全局的区块链中，由此来表明一个产品的诞生。当这个产品售出去后，消费者可以把它再注册进一个局部性（如一座城市或州）的区块链里

(C) DavidKuoChuenLee

来源：http://www.skuchain.com/； http://www.8btc.com/ibm-ethereum

P 2 P 借 贷

首个区块链P2P借贷项目

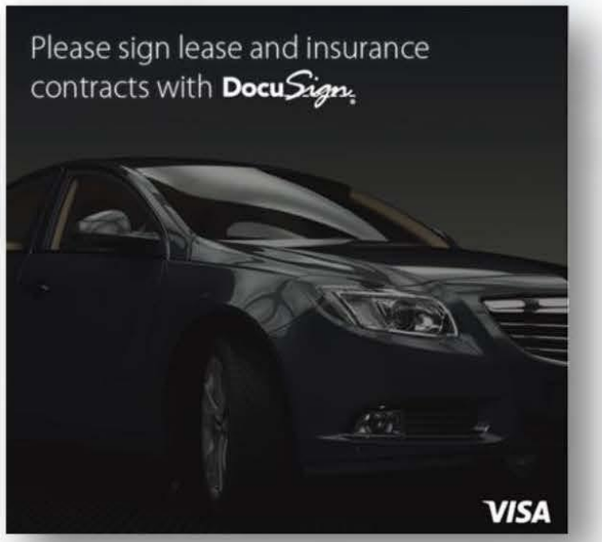
MoneyCircles 的主旨是通过智能合约，在平台上直接来验证和认证个人身份和居住点。使用智能合约的方式能够免去在借款人和贷款人之间需要中介机构或者中间人来接入和干预的情况。

- **核心优势：**没有任何暗箱操作或者资金池问题， 所有钱的流向非常公开透明， 每个人都知道相关资金是怎么流向怎么使用。
- 在欧洲，特别是在英国，无法获得信贷的人非常多，被困在低利息储蓄帐户之下。MoneyCircles 的目标就是通过调和借贷方与金融机构这两部分市场，让借款放、贷款方和金融机构之间建立一种积极的关系。

来源： http://moneycircles.com/

(C) DavidKuoChuenLee

汽车项目（Visa/DocuSign）



这是一项正在进行中的项目，它通过 **DocuSign** 独有的数字交易管理平台和电子签名，集成了 **Visa** 的支付技术，让汽车将能够在比特币区块链上进行车辆登记。

类似于 Visa 把信用卡技术集成进入苹果手表(Apple Pay），这里将信用卡“放入”车中，使车辆能够成为一种智能资产。

合同
用Docusign核实租赁与保险

报告
查看驾驶记录

车内支付
可以使用Visa卡

服务
连接APP

汽车将可支付过路费，购买披萨饼，或者是为汽车订购卫星广播等

来源：https://www.docusign.com/blog/the-future-of-car-leasing-is-as-easy-as-click-sign-drive/

(C) DavidKuoChuenLee

政 务 管 理

首个区块链政务系统将在乌克兰（Ukraine）启动

Bitnation与爱莎尼亚（Estonia）在区块链上开展政务管辖

澳洲新立的党派很时髦，推广区块链选举机制

来源：http://www.wanbizu.com/fazhan/201512015809.html；http://www.wanbizu.com/news/201602186602.html；http://www.wanbizu.com/news/201602186602.html

(C) DavidKuoChuenLee

更多领域，未完待续

(C) DavidKuoChuenLee

区 块 链 在 中 国

WANXIANG BLOCKCHAIN LABS

小蚁AntShares

布比区块链

维优咨询

井通北京 Jingtum Beijing

Canaan

Hash

BST 数贝软件

还有许多未公开项目……

(C) DavidKuoChuenLee

万向区块链实验室

万向区块链实验室（WanXiang Blockchain Labs）是一家专注于区块链技术的前沿研究机构，实验室将聚集领域内的专家就技术研发、商业应用、产业战略等方面进行研究探讨，为创业者提供指引，为行业发展和政策制定提供参考，促进区块链技术服务于社会经济的进步发展。

产　品

比特币区块链开发平台

以太坊区块链开发平台

BitShares区块链开发平台

Factom区块链开发平台

来源：http://www.blockchainlabs.org/

(C) DavidKuoChuenLee

小蚁AntShares

小蚁是基于区块链技术，将实体世界的资产和权益进行数字化，通过点对点网络进行登记发行、转让交易、清算交割等金融业务的去中心化网络协议。

应 用 场 景

股权众筹

P2P网贷

员工持股激励

签署电子合同

来源：https://www.antshares.com

(C) DavidKuoChuenLee

井通与海航集团合作区域链

井通北京 Jingtum Beijing

HNA

1 企业级钱包

采购信息→资金流传→结算

- 用区域链技术建立低成本结算系统
- 提高了流转效率

2 供应链融资

- 基于井通区域链3.0底层所提供的加密技术
- 解决供应商面临的周转难，融资难利息高困境

3 福利汇

- 海航通过“福利汇”中的“井通钱包”发放员工福利
- 企业在员工信息，资金保密不外泄的情况下，让员工享受更多优惠

来源：http://www.8btc.com/jingtong-hna

(C) DavidKuoChuenLee

布 比 区 块 链

应 用 领 域

股权
以信任为基础，
私有股权流通。

积分
多方联合开放，
积分发行及兑换，
促进积分流通。

供应链
利用不可篡改，
溯源供应链管理。

优 势 特 点

快速交易验证

高效账本存取

多种资产发行

联合签名控制

内置智能合约

链上交易所

(C) DavidKuoChuenLee

来源：http://www.bubi.cn/#page4

维　优　金　融

维优咨询

- 为不同的客户提供量身定做的区域链解决方案
- 对数字资产进行评级、风险披露和管理

产品介绍

Prometheus计划-股权管理链

- 产品：股权管理私有链或联
- 特点：实现股权在区块链上的登记、流转以及场外交易，以及可视化
- 用户：众筹平台，区域性股权交易中心，P2P平台，私募基金，其他OTC交易市场

Gaea计划-土地流转链

- 产品：土地经营权资产私有链或联盟链
- 特点：为跨区域的土地流转提供信任基础，实现土地数据验证、信息存储、交易结算电子凭证等功能
- 用户：地方政府，土地经营权所有者

Hermes计划-商业积分链

- 产品：商业积分私有链及联盟链
- 特点：多方互联，提供积分验证，积分总帐查询，即时积分结算，快捷发行积分等功能
- 用户：提供各类服务的线上和线下商家

Themis计划-监管科技链

- 产品：政府部门公开信息的公有链或联盟链
- 特点：信息不可篡改，由多方节点维护政务信息的公正透明，提升政府监管工作速率和工作效果，增加政府工作的公信力
- 用户：政府监管部门

(C) DavidKuoChuenLee

来源： http://viewfin.com/

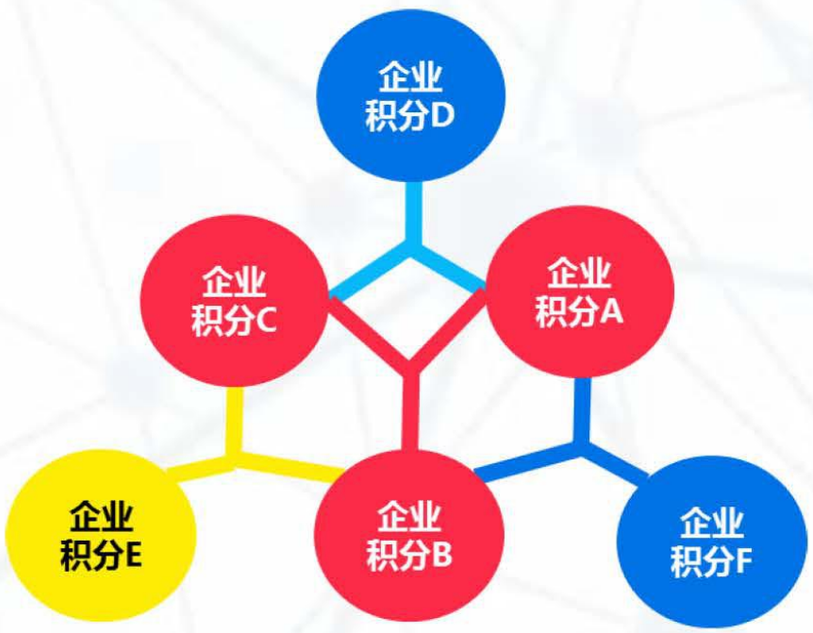
数 贝 荷 包

由**易诚互动旗下的比邻共赢公司**开发，日前，**阳光保险**已宣布应用“数贝荷包”，成为业内首个应用区块链技术的企业。针对“数贝荷包”，单独发行“阳光贝”积分，帮助阳光用户与“数贝荷包”其他平台或企业用户实现积分通兑和互换。

产品模式与优势

传统模式

- 打破企业间的积分流通壁垒。
- 用户之间都可以自由议价、互换，将积分化零为整，便利用户使用，大大提升积分的流通效率
- 盘活企业库存积分，提升用户流量和活跃度，商户的经营也得到升级



数贝钱包模式

(C) DavidKuoChuenLee

来源：http://m.caijing.com.cn/api/show?contentid=4090411

清华长三角研究院

清华长三角研究院杭州分院联合嘉楠耘智、数贝投资、矿池科技、算力科技等公司共同发起成立了中国区块链应用研究中心，致力于区块链应用拓展。

合 作 公 司 介 绍

Canaan

- **嘉楠耘智**成立于2013年，是全球领先的超算芯片及数字区块链计算设备制造、区块链计算整体方案提供商，也是全世界第一家研发出SHA256专用计算设备的公司，产出的设备销往全球超过150个国家和地区，售出芯片到全球重复计算领域专用设备的30%

Hash

- **矿池科技**的全球重复计算领域专用设备的30%是专注于比特币及区块链领域应用服务平台
- 致力为用户提供专业，可靠，安全，便捷的比特币应用及最新行情价格应用网站

BST 数贝软件

- **数贝投资**提供的应用服务平台包括智慧北京信息资源共享交换云服务(PaaS)平台、政务信息资源目录管理云服务(SaaS)平台、北京市物联网实时数据交换支撑服务平台
- 两大产品：数贝DXS-Cloud及iTaxonomy

来源：www.btc798.com/article-8759-1.html； http://canaan.io/zh/%E7%BD%91%E7%AB%99%E9%A6%96%E9%A1%B5/ ； http://www.synball.com/synball/home/； http://www.1hash.com/index.html

(C) DavidKuoChuenLee

潜力区块链项目

以太坊Ethereum

ethereum

区块链2.0：以太坊Ethereum

ethereum

Ethereum（以太坊）是一个平台和一种编程语言，使开发人员能够建立和发布下一代分布式应用。 Ethereum可以用来编程，分散，担保和交易任何事物：投票，域名，金融交易所，众筹，公司管理， 合同和大部分的协议，知识产权，还有得益于硬件集成的智能资产。

- **目的**：简化利用到区块链技术或者去中心化共识技术的应用的开发。
- **特点**：以太坊坚定不移专注于区块链技术，并且拥有自己的区块链，这一点更加吸引了企业与客户。以太坊区块链还添加了智能合约——虽然智能合约同样也能在比特币上使用——和能够创建去中心化自主组织的能力，这两点使以太坊更加具有使用价值。

区块链2.0：以太坊Ethereum

以太坊要解决什么问题？

把传统合同合约变成智能合约， 通过自动化解决了传统合同的纠纷等棘手问题。

区块链2.0的核心

区块链2.0重要的是智能合约、智能资产，而智能合约领域最有影响力的开发平台就是以太坊，2016年基于比特币区块链的智能合约平台Rootstock发展也很快，最近得到了比特大陆领投的100万美金。

哪些机构在支持以太坊？

以太坊正被一些金融机构、银行财团（比如 R3），以及类似三星、Deloitte、RWE 和 IBM 这类的大公司所密切关注。

(C) DavidKuoChuenLee

基于以太坊的去中心化应用

自行车租赁服务Slock.it:

自行车的所有者会将一个 Slock（智能锁）安装到他们的自行车上，并且在以太坊区块链上给自行车注册一个智能合约（一段程序代码）。接下来，任何人都可以向该**智能合约**发起一个发送一定数量数字货币的请求，合约在接到这个请求之后，会自动将这笔数字货币转发给自行车的所有者，这样发送者可以获得2个小时的使用权。

来源: http://www.8btc.com/7-dapps-based-ethereum

(C) DavidKuoChuenLee

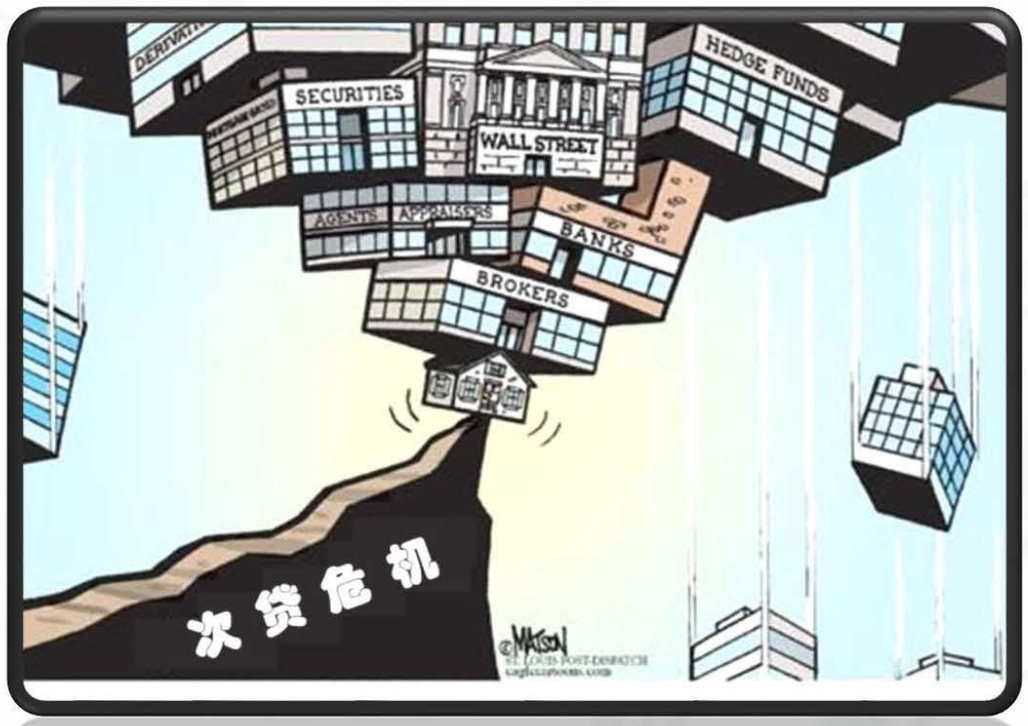
开创“零信任”时代

公　　证　　通

“诚信是具备颠覆性的”　– 保罗·斯诺

(C) DavidKuoChuenLee

“诚信是具备颠覆性的” – 保罗•斯诺



- **在当今的全球经济中，信任是稀有的。**这种信任的缺乏，造成了大量资源的投入来进行审计和记录核查，从而降低了全球效率，投资回报率和经济繁荣。
- 如2010年美国的次贷危机等事件表明，**目前的审计和核查流程是非常不准确和低效的**，容易造成问题。
- Factom提供了世界上首个准确的，可核查的和不可更改的审计公证流程和方法，**从此我们不再需要盲目信任。**

(C) DavidKuoChuenLee

公　　证　　通

Factom使用区块链提供认证服务，能对所有的文件、文书或者是一些数据资料进行公证。它最大的优势是，并不依赖于这个公司提供信用，这个公司只是提供一个解决方案，通过这个解决方案，能让更多的人把数据信息指纹，保存在分布式的比特币区块链上。

应 用 场 景

- 利用比特币的区块链技术来革新商业社会和政府部门的**数据管理和数据记录方式。**
- 利用区块链技术**助力各种各样应用程序的开发**，包括审计系统，医疗信息记录，供应链管理，投票系统，财产契据，法律应用，金融系统等。

网 络 价 值

维护了一个永久不可更改的、基于时间戳记录的、区块链数据网络。大大减少了进行独立审计、管理真实记录、遵守政府监管条例的成本和难度。

存在性证明

某一时间段的文档

过程性证明

和最近更新相关联的文档

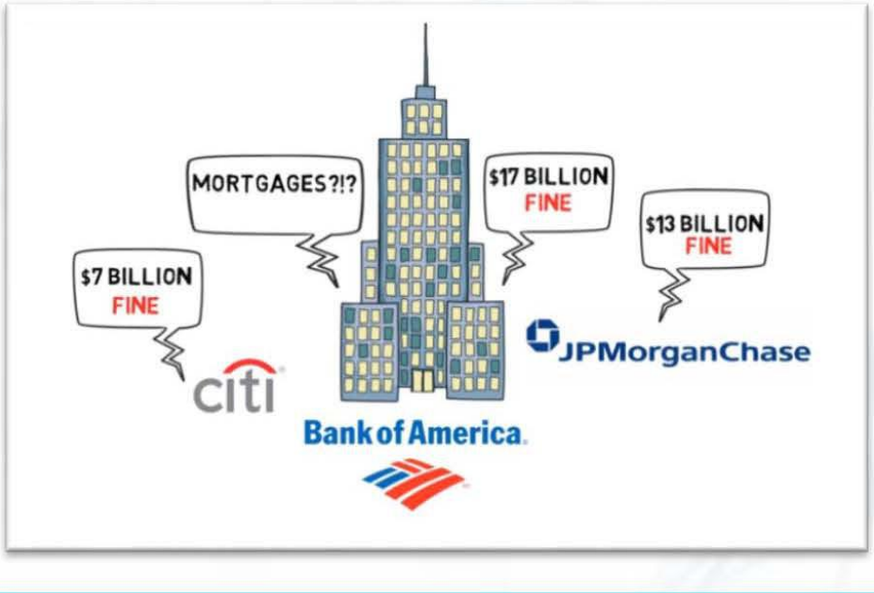
检查性证明

核查最近的项目文档的更新情况

(C) DavidKuoChuenLee

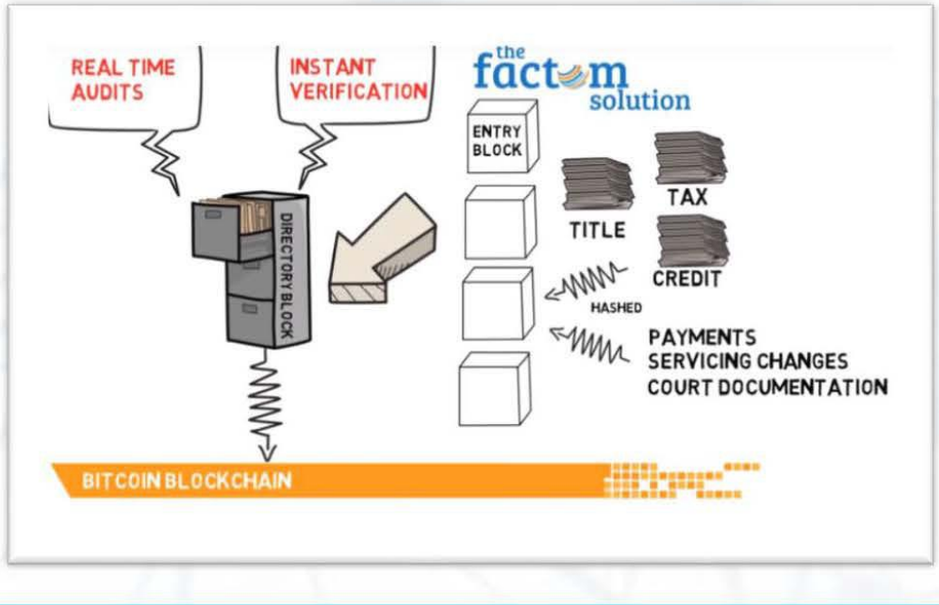
来源：http://factom.org/

具体应用分析1：帮助美国银行节约170亿美金成本



背　景

房屋贷款背后通常是非常繁琐、复杂的文件。2008年次贷危机发生后，美国银行收购了Countrywide，数十亿份文件必须转移。而因为美银的子公司Countrywide和美林证券的欺诈行为，美国银行被罚款170亿美元。



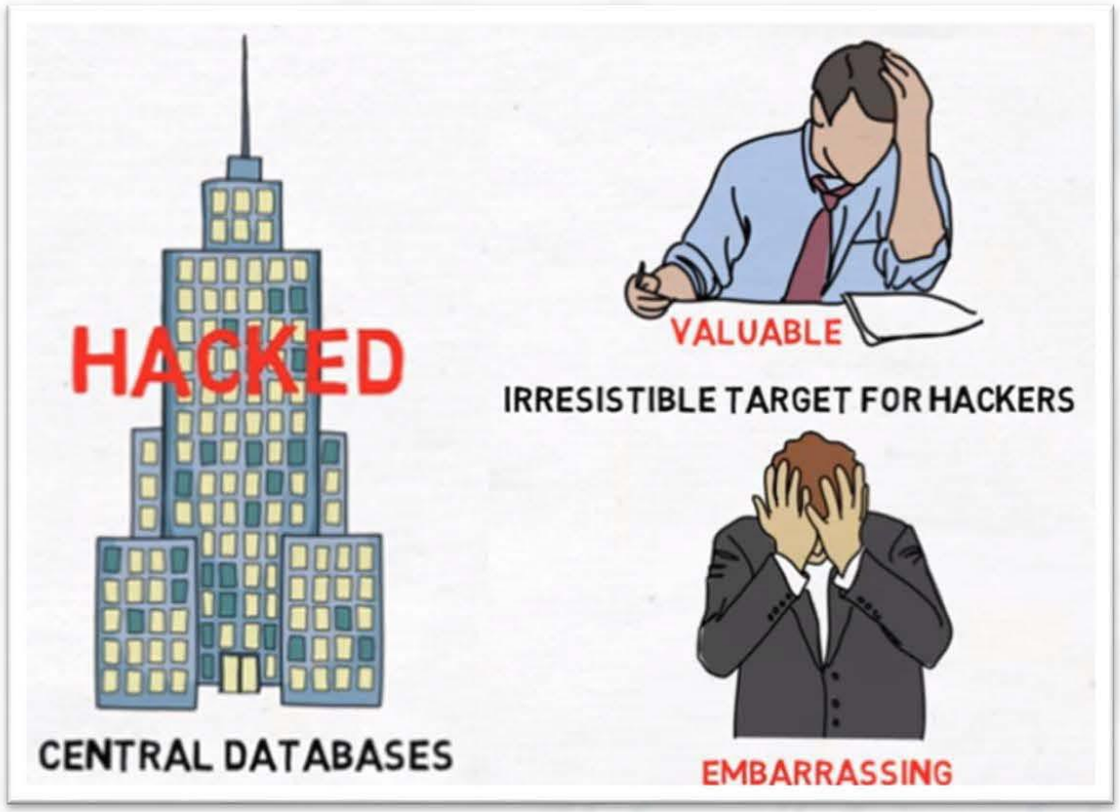
方　案

Factom把所有文件分散化储存在区块链中。每一笔交易、付款和法庭文件都被实时记录、跟踪和审计。现在，相关的工作人员可以获取其权限的文件，二次审查，避免再次发生欺诈事件。

(C) DavidKuoChuenLee

来源：http://factom.org/

具体应用分析2：防止索尼公司的图片泄露丑闻的发生



背　景

2014年11月索尼公司的数据库被黑客入侵，部分未发行的电影、员工的工资与社保号码甚至名为“snapchat”的商业策划被泄露，导致公司损失惨重。

方　案

Factom建立了一个防破解的身份分类账，把所有关键的文件储存于去中心化的“尾对尾”加密储存。不同的文件散列放置，实时被监控。多重数字签名技术防止信息被黑客入侵盗取数据。

(C) DavidKuoChuenLee

来源：http://factom.org/

具体应用分析3：打开9万亿美金的土地交易市场

背　景

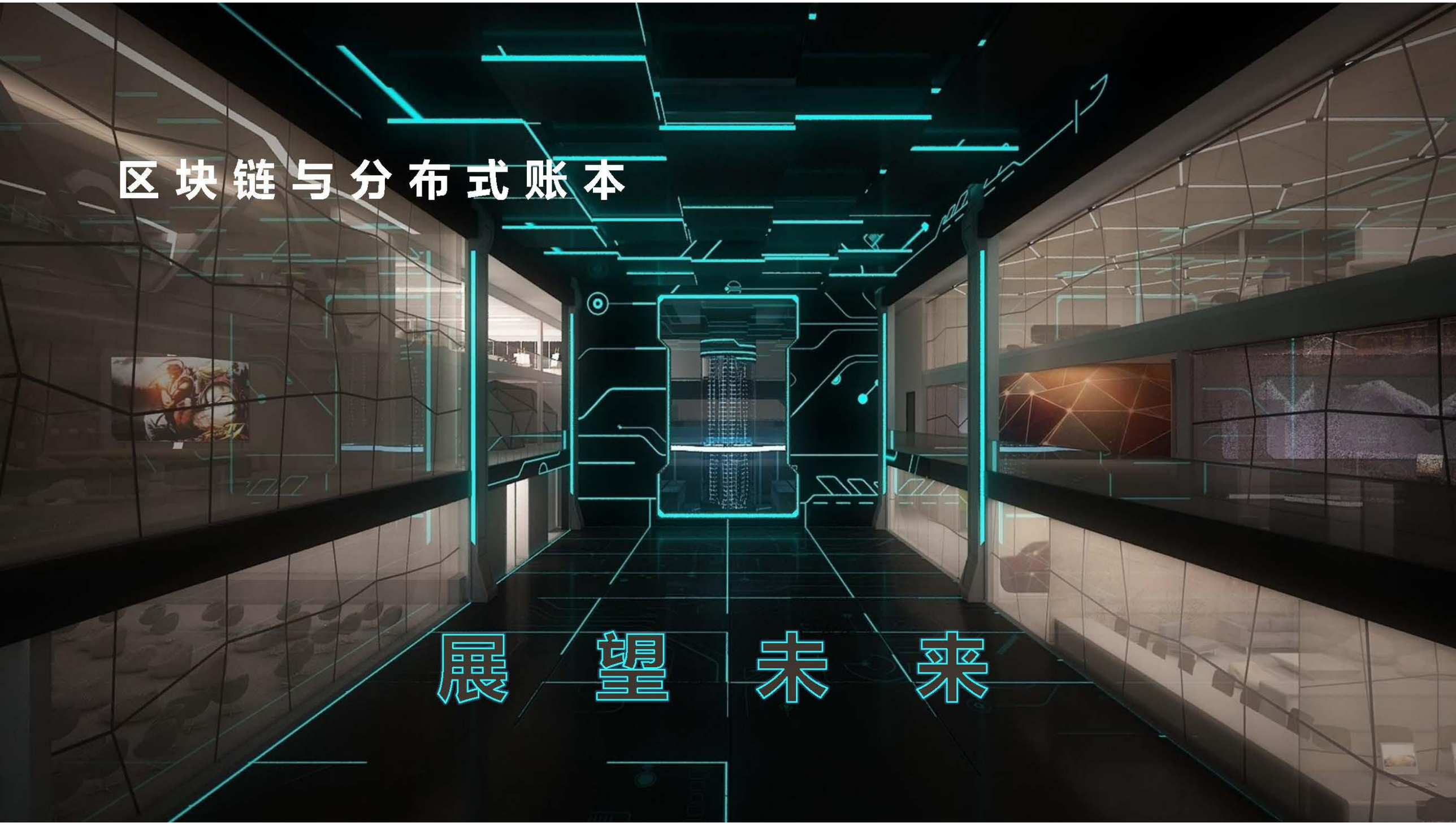
在许多发展中国家，绝大多数土地是没有文件证明的。Hernando De Soto估计，这些土地的价值数额庞大。如何有效证明土地、房产的所有权，是一个巨大空间的市场。然而，现有的系统多少回牵涉产生腐败、政治丑闻和黑客入侵等因素。

方　案

Factom把所有土地产权文件数字化，存储在去中心化的区块链中。Factom可以跟踪每一笔土地所有权的变更、租赁协议甚至是矿产权归属。所有非法的修改都可以被识别并被更正。

来源：http://factom.org/

(C) DavidKuoChuenLee


区块链与分布式账本
展 望 未 来

难找应用场景

- 区块链是否优于现有的方案？如何设定衡量标准？
  *是否节省人力资源成本，提升服务质量或用户体验？
- 不能篡改的共享账本、统一标准的合同、记账、交易等概念不太现实
  *不同的记账规则和不同的企业业务分类（很难建立一个统一标准）
- 区块链应用必须能够为用户创造有切实价值的应用场景，才会成功

资源整合的难题

- 资源整合的难题：
- 如何分配研发资源？是否能把相关的资源整合起来？
- 资源应该导向哪些技术方案？哪些领域？

(C) DavidKuoChuenLee

来源：“区块链落地还有多远”《财新周刊》 2016年第7期 出版日期 2016年02月22日

降低成本的可能？

- 表面上区块链的交易成本低，但要维护其安全性和不可篡改性的成本可能很高
- 篡改成本虽大（要篡改，就必须更改区块链系统中51%的副本），但也意味着巨大的存储成本。
- 区块链存储效率不高：1.大量副本 2.区块链不能瘦身（失效的垃圾信息也会被保留。）
- 更新数据耗时：更新内容乘以副本的数量，再加上副本间的传输距离和带宽，会耗时。影响对高频应用的响应，例如诸多的交易场景。

监管和市场的疑虑

- 预防非法使用，例如洗钱、恐怖组织融资、欺诈、身份盗用等。
- 去中心化性质难符合传统监管模式
- 过早的监管可能限制区块链潜能的最大化，因而使研发却步扼杀区块链用途的发展

(C) DavidKuoChuenLee

来源：“区块链落地还有多远”《财新周刊》 2016年第7期 出版日期 2016年02月22日

千万别生于互联网死于区块链。。。

-姚余栋（央行金融研究所所长）

一些互联网公司可能对于区块链的功能不在乎，不以为然，但要是错过这样的机会，可能会颠覆整个顶层技术的变革

(C) DavidKuoChuenLee

RESEARCH PLAN

- Bitcoin and Blockchain
  - Understand Bitcoin & Blockchain
  - Try bitcoin client and read documents
  - Bitcoins the hard way: Using the raw Bitcoin protocol
  - http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html

- Ethereum and Smart Contract
  - Understand Ethereum and Smart Contract
  - Try Ethereum client and write some smart contracts

- Decentralized applications
  - Slock and DAO
  - Arcade City

THANK YOU!

Q&A