

区块链中的智能资产

梁然



我的区块链经历

- 2006年~2013年 在美国道富银行学习和工作
- 2013年来到上海，期间比特币飞涨，第一次知道了区块链
- 2013年底，研究对比各区块链技术，思考区块链对金融的影响
- 2014年创建了RippleFox网关，主要针对Ripple和Stellar进行技术开发
- 2016年加入万向区块链实验室

大纲

- 讨论各种区块链中的资产
- 深入介绍资产发行的公链
 - Ripple
 - BitShares
 - Stellar
- 总结对比相关技术

区块链中的币——原生资产



去中心化的交易所

以Ripple为例介绍资产的发行和交易

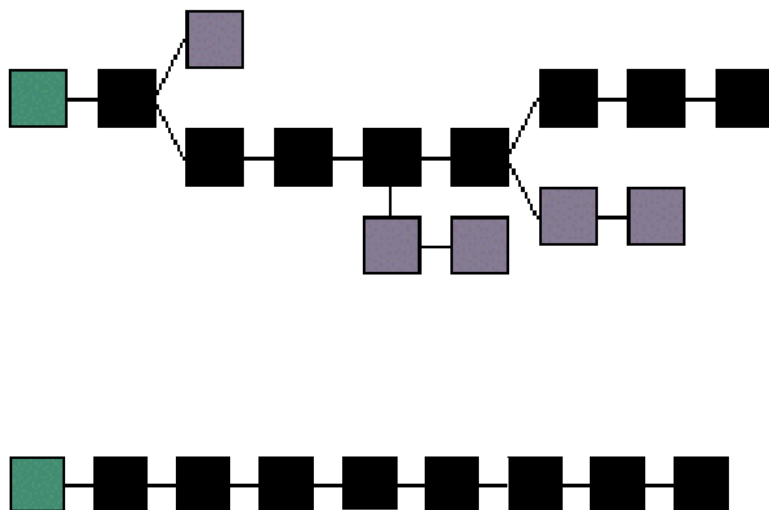


不同的共识算法

- 工作量证明机制(Proof of Work, POW)
- 股权证明机制(Proof of Stake, POS)
- 特殊节点列表达成共识的机制
 - 瑞波共识机制(Ripple Consensus)
 - 恒星共识机制(Stellar Consensus)
 - 比特股BitShares(DPOS)

不同的出错机制

- 同一个位置多于一个区块
 - 分叉
 - 节点选择最长的一条继续计算
 - 比特币、Bitshares
 - 暂停
 - 节点列表不同意，总账暂停
 - Ripple、Stellar为代表



新型区块链技术Ripple等的改进

—速度

- 比特币10分钟
- Ripple只要3到6秒

—磁盘

- 完整模式，同步全部账本
- 普通模式，同步最近的账本

—分布式的交易

- 可以发行其他资产
- 资产可交易

网关发行资产并记账

- 网关G发行CNY
 - 用户A : 200CNY
 - 用户B : 300CNY

网关G	用户A	用户B
A: -200	G: 200	
B: -300		G: 300

- A发送100CNY到B
 - A减少100
 - B增加100

网关G	用户A	用户B
A: -100	G: 100	
B: -400		G: 400

网关的运作

- 充值：
 - 用户A给网关转账100 CNY
 - 网关G在链内发行100 CNY给A
- 提现
 - 用户A在链内发送100 CNY
 - 网关给用户A转账100 CNY

充值前	网关G	用户A
银行账户	0	100
Ripple	0	0

充值后	网关G	用户A
银行账户	100	0
Ripple	-100	100

提现后	网关G	用户A
银行账户	0	100
Ripple	0	0

Ripple发行资产的特性

- 用户必须先设置对网关的信任
- 网关可以设置信任用户列表
- 网关在必要时可以冻结资产

示例1：记账

G

CNY - Chinese Yuan
-500

A

CNY - Chinese Yuan
200

B

CNY - Chinese Yuan
300

联系人姓名/钱包地址

货币类型 余额

rNLfxSFsnDvpWtdKwB1XMCMFYGiAMv7nYd

CNY

0

rwf4eDa3XhHWSSQpDhaxNxNJoeCH7TFe5X

CNY

-200

rPFen5k45s9QefN5Xg8dfSDUrkdICTgYh2

CNY

-300

联系人姓名/钱包地址

货币类型 余额

razNdEaWEjhx4dSpQJ9oYfqizRcw28oXmQ

CNY

200

联系人姓名/钱包地址

货币类型 余额

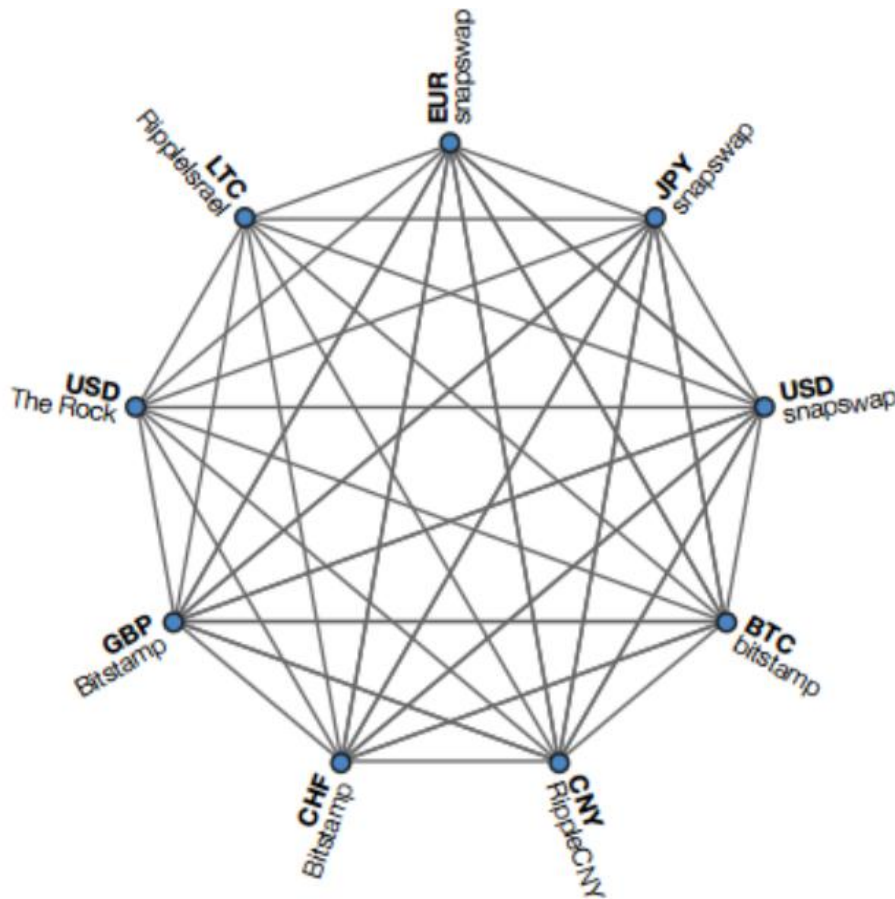
razNdEaWEjhx4dSpQJ9oYfqizRcw28oXmQ

CNY

300

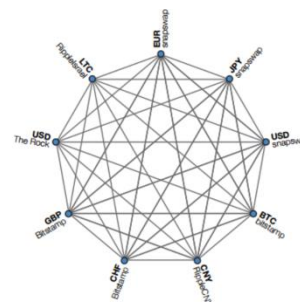
内置交易功能

- 任意资产均可交易
- 7 X 24小时，无涨跌停
- 全球统一市场



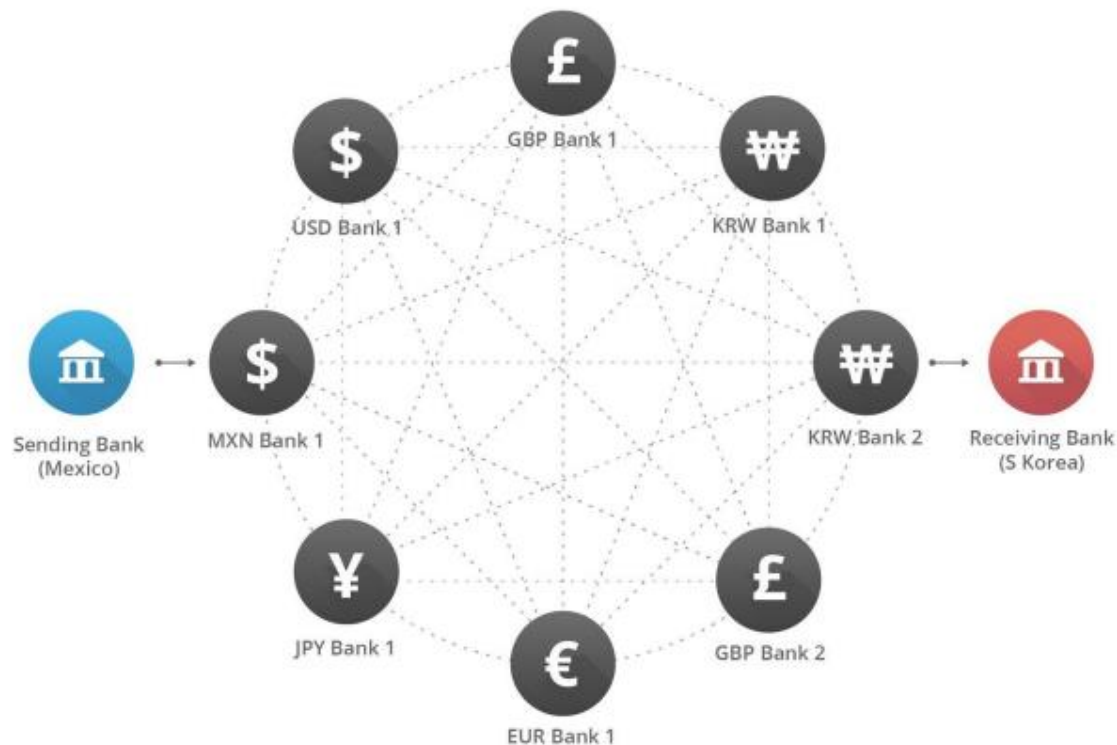
与中心化交易所的区别

- 安全强健
 - 多节点，永不停机
 - 不怕DDoS
 - 攻击只导致单个账户失效
- 公开透明
 - 撮合算法公开，无黑箱操作空间
 - 交易透明，持仓透明
- 统一市场
 - 任意的交易品种
 - 充分的市场竞争
 - 流动性最大化
- 高速但非高频
 - 理论上限10万笔/秒



跨币种支付

- 两个币种之间的直接买卖
- 通过其他币种的买卖桥接
- 自动寻找最优路径
- 例：用MXN支付KRW
 - MXN/KRW市场
 - MXN/XRP, XRP/KRW两个市场
 - MXN->CNY->USD->KRW多个市场



示例2：交易

USD/CNY	▼	Base currency USD rvYAfWj5gh67oV6fW32ZzP3Aw4Eubs59B change issuer	Counter currency CNY rKiCet8SdvWxPXnAgYarFUXMh1zCPz432Y change issuer
Bid = 6.5200000		Ask = 6.5385000	Spread = 0.0185310
Last price = n/a			

Buy rvYAfWj... USD 205,147 rKiCet8... CNY available

Amount To buy

1 USD rvYAfWj...

Price of Each

6.5 CNY rKiCet8...

Order Value (max)

6.5 CNY rKiCet8...

You are wanting to buy 1 USD for 6.5 CNY (6.5 CNY per USD)

Buy USD (rvYAfWj...)

Sell rvYAfWj... USD 1,383.5 rvYAfWj... USD available

Amount To sell

1 USD rvYAfWj...

Price of Each

6.6 CNY rKiCet8...

Order Value (max)

6.6 CNY rKiCet8...

You are wanting to sell 1 USD for 6.6 CNY (6.6 CNY per USD)

Sell USD (rvYAfWj...)

示例3：跨币种支付

Receive

100

JPY - Japanese Yen

兑换

142.97 XRP

(1.4297 JPY/XRP)

兑换 XRP

0.0019964 BTC

(0.00001996 JPY/BTC)

兑换 BTC

5.9599 CNY

(0.059599 JPY/CNY)

兑换 CNY

5.969600 FMM

(0.059696 JPY/FMM)

兑换 FMM

0.91192 USD

(0.009119 JPY/USD)

兑换 USD

510.620000 XLM

(5.106200 JPY/XLM)

兑换 XLM

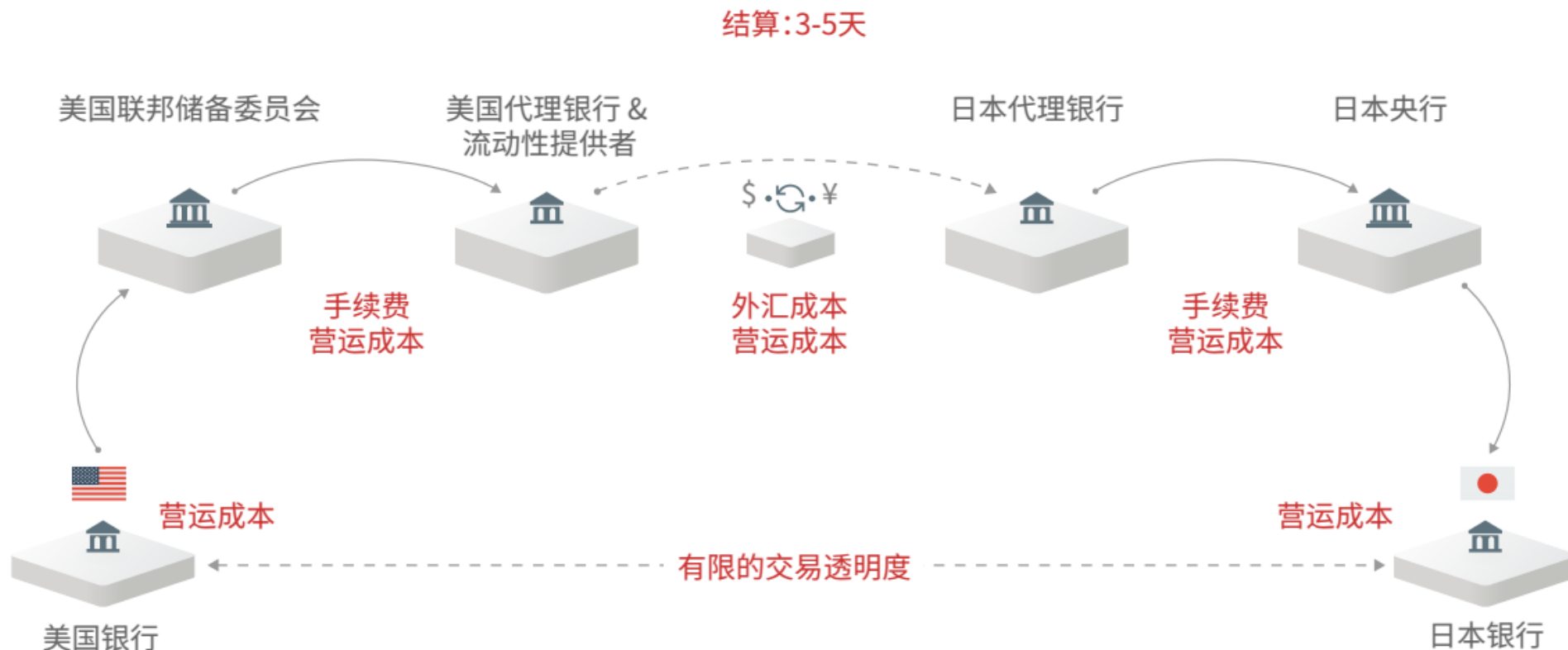
Paths last updated 3 seconds ago

对国际支付的成本改进

理解分布式交易形成的统一市场如何减少支付成本



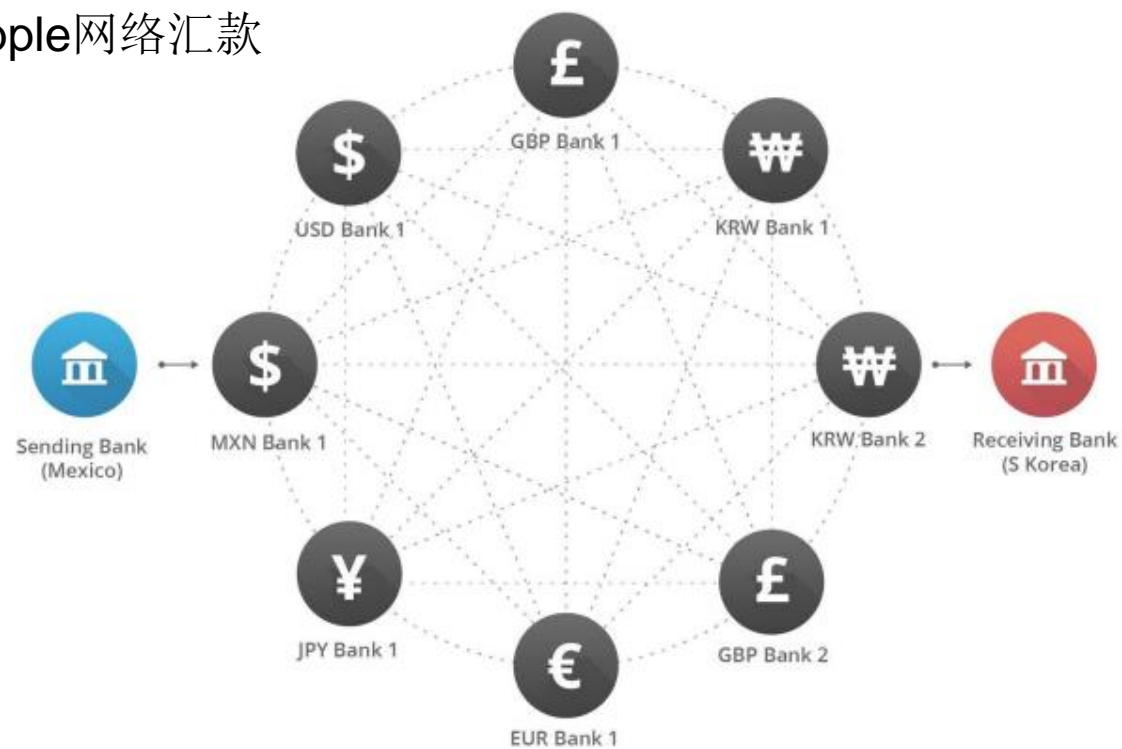
普通国际支付的成本



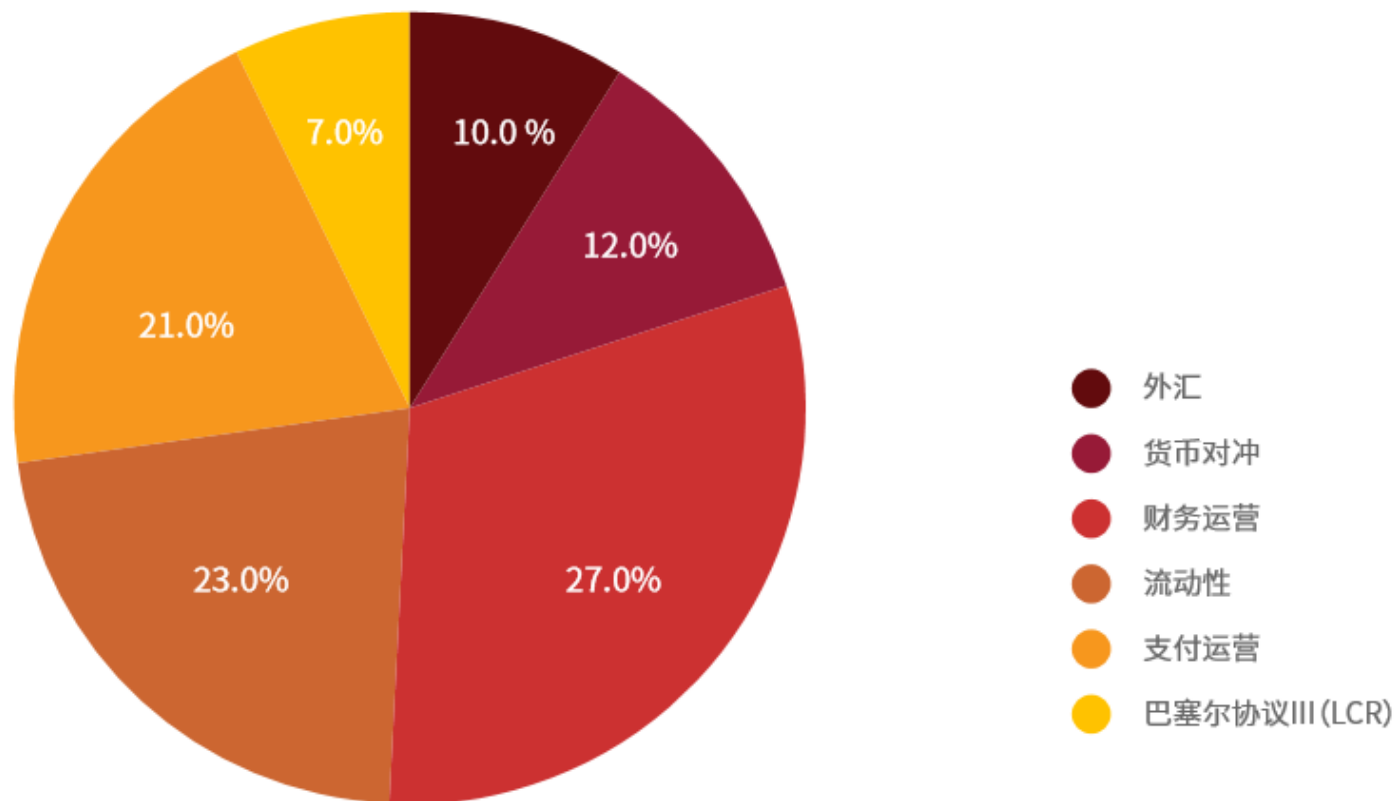
通过银行汇款



通过Ripple网络汇款

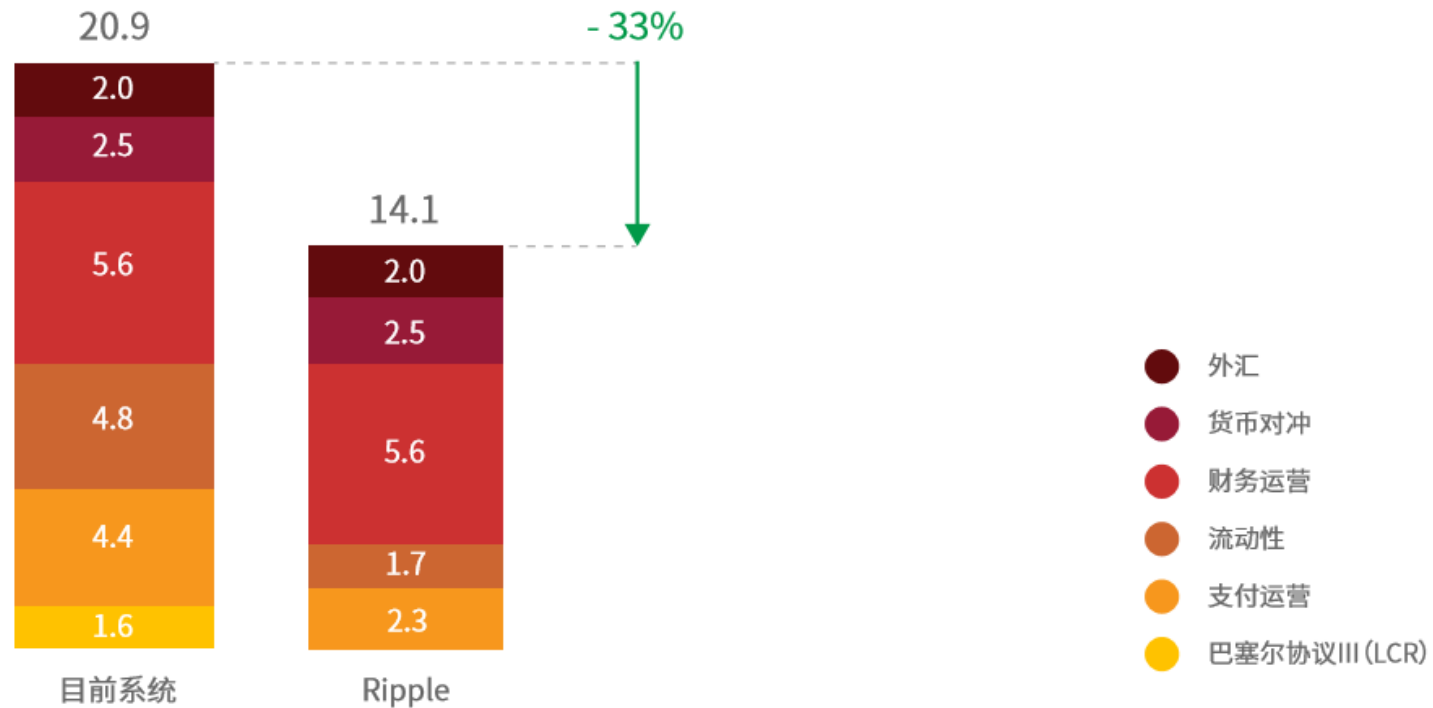


国际支付服务成本分析



成本减少预估

全球平均支出: 支付总量20.9个基点



中国与Ripple合作的案例



“利用 **Ripple** 解决方案，我们正在为零售业客户开发新的商务支付服务，以便他们能够实时将钱从中国汇到美国和其他国家。”

上海华瑞银行总经理兼创新与研究主管

讨论和问答

比特股BitShares 分布式自治公司 (DAC)和智能资产平台



DAC分布式自治公司

Decentralized Autonomous Corporation

- 众筹发起
- 历经两个版本 0.9x -> 2.0
- DPOS(股份授权证明机制)
- 比特股工作合同(worker)

DPOS(股份授权证明机制)

- 股东按其持股比例(BTS)拥有影响力
 - 股东可以将其投票权授予一名代表
 - 获票数最多的前N位代表成为验证者
 - 验证者轮流产生区块
-
- 优点：速度快，节省能源

系统角色

- 见证者Witness
 - 出块
 - 提供链外价格
- 委员会Committee
 - 网络费用
 - 块大小、间隔
 - 过期参数
 - 见证者数量
 - 见证者奖励
 - 预算项目
- 预算Worker/Budget Item
 - 起止日期
 - 每天花费BTS
 - 项目名字、URL
 - 类型:
 - 工资 Vesting
 - 销毁 Burn
 - 返回到预算池 Refund

DAC鼓励会员和发展新用户

- 终身会员
 - 一次性费用
 - 80% 手续费返还
- 推荐奖

手续费分配

网络收取	20%
终身会员推荐人 (btsabc)	30%
注册人 (bts.api)	40%
推荐人 (btsabc)	10%
会籍过期时间	N/A

手续费及现金返回

手续费总支出	0 BTS
待结费用	0 BTS
待解冻金额	0 BTS

账户权限

- 账户权限 Owner Permission
- 活跃权限 Active Permission
- 备注权限 Memo Permission

- 块签名的密钥 Block Signing Key

丰富的账户权限控制

活跃权限

账户权限

备注密钥

活跃权限用来设定拥有花费本账户资金权限的账户名或公钥。

可方便的架设多重签名机制，参见 [权限](#) 了解更新信息。

阈值



输入账户名/公钥以及权重

添加

	账户名/公钥	权重	操作
	bitcrab	1	<div>移除</div>
	bitreserve	1	<div>移除</div>
	BTS7mgt9xGypWQh4uaEnjSC6Fv2aixyghu7wfN8q4uSMHgqc8TfWF	1	<div>移除</div>

投票

代理投票 见证人 理事会 预算项目

预算项目 是BitShares系统中独有的概念。他们是一些期望通过提供服务来从区块链获得奖金的工作项目提案。一项提案包含一个指向网站或论坛帖子的链接，在其中详细解释了工作项目的介绍。在这里Bitsharestalk可以看到一些提案。

预算总额: 0 BTS
未使用预算: 0 BTS

描述	创建者	赞成票数	每日预算 (每日)	未发放预算 (循环)	注资	我的立场
----	-----	------	--------------	---------------	----	------

新增预算项目

#1	bitARS smartcoin creation Sun, 1 May 2016 - Thu, 12 May 2016	elmato bitsharestalk.org/index.p...	60,619,167 BTS	100,000 BTS	0 BTS	0.00%	中立	赞成
----	-----------------------------------------------------------------	----------------------------------------	----------------	-------------	-------	-------	----	----

活跃预算项目

#1	svk - Bitshares GUI Development and Maintenance #2 Mon, 21 Mar 2016 - Sat, 21 May 2016	dev.bitsharesblocks docs.google.com/document/...	285,326,343 BTS	25,000 BTS	203,125 BTS	100.00%	中立	赞成
#2	refund400k Wed, 21 Oct 2015 - Mon, 31 Dec 2035	init0	259,428,056 BTS	400,000 BTS	(34,188,698 BTS)	100.00%	中立	赞成
#3	Python Library and Applications Tue, 1 Mar 2016 - Thu, 30 Jun 2016	pay.xeroc github.com/xeroc/worker-p...	251,015,555 BTS	21,467 BTS	832,537 BTS	100.00%	中立	赞成
#4	refund-100k-1 Fri, 1 Jan 2016 - Sun, 1 Jan 2017	committee-account bitshares.org	250,415,841 BTS	100,000 BTS	(3,939,307 BTS)	53.53%	中立	赞成
#5	refund-100k-3 Fri, 1 Jan 2016 - Sun, 1 Jan 2017	committee-account bitshares.org	250,015,443 BTS	100,000 BTS	(2,354,297 BTS)	0.00%	中立	赞成

特性

- 资产发行
 - SmartCoin
 - MPA (Market Pegged Asset)
 - PMPA (Private MPA)
 - UIA (User Issued Asset)
- 去中心化交易所 DEX (Decentralized Exchange)

MPA 市场锚定资产

- 通过内置的合约来实现 (Contract for Difference)
- 价格稳定
- 风险在于BTS的价格波动

比特股发展中的教训

- 不平衡的规则:
 - 没有强平时: 0.85
 - 30天强平时: 0.98-1
 - 没有人抵押时: 1.05

MPA

- 锁定抵押的BTS
- 得到bitUSD
- 卖出bitUSD
- BTS价格上涨
 - 买回bitUSD
 - 平仓
 - 实现了杠杆
- BTS价格下跌
 - 补充抵押品
 - 强平

PMPA (Privatized MPA)

CNY 保证金头寸

调整和设置你的债务及抵押物(保证金).

如果调低 CNY 债务水平, 将从 boombastic 账户中扣除相应 CNY 归还。 如果调高 CNY 债务水平, 只要 boombastic 账户持有足够的 BTS 可供抵押冻结, 新借入的 CNY 将存入 boombastic 账户中。

保证金可以增加或减少, 只要抵押率超过维持保证金率。 [更多信息](#)

喂价: 39.21620112 BTS/BitCNY

强制平仓价: 43.13782123 BTS/BitCNY

你的强平触发价: 44.81851554 BTS/BitCNY

借入金额 可用余额: 2,004.6303 BitCNY

100

BitCNY

保证金 可用余额: 430,227.99609 BTS

7,843.24022

BTS

保证金比例

2.00

调整头寸

重置

UIA用户发行资产

- 管理工具:
 - 白名单: 收发和交易 (KYC)
 - 交易费
 - 冻结
 - 转账限制
 - 交易对限制
 - 停止市场交易

DEX：去中心化的交易所



DEX：去中心化的交易所

- 去中心化
- 快速非高频，无法预知下一个出块的节点是哪个
- 安全
- 随时随地交易
- 低费用
- 可交易任何资产
- 保护隐私
- 权力分散
- 自带市场锚定资产合约
- 统一的委托单

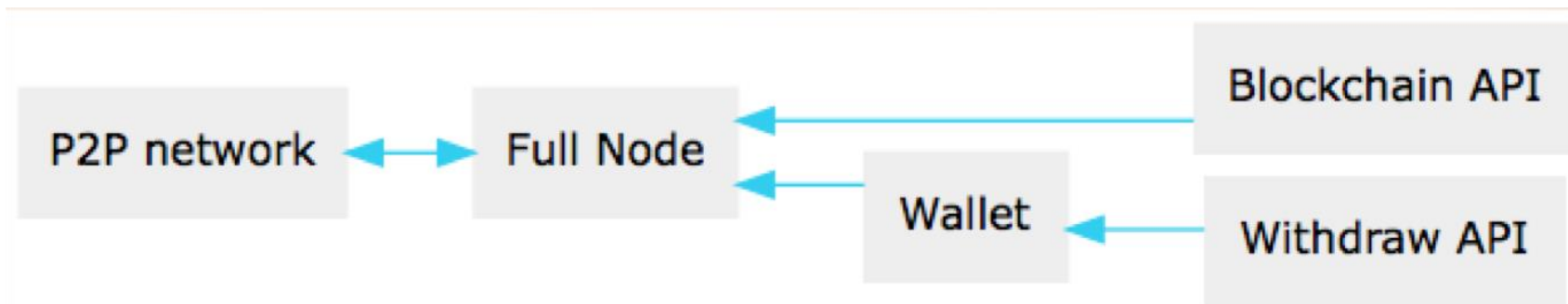
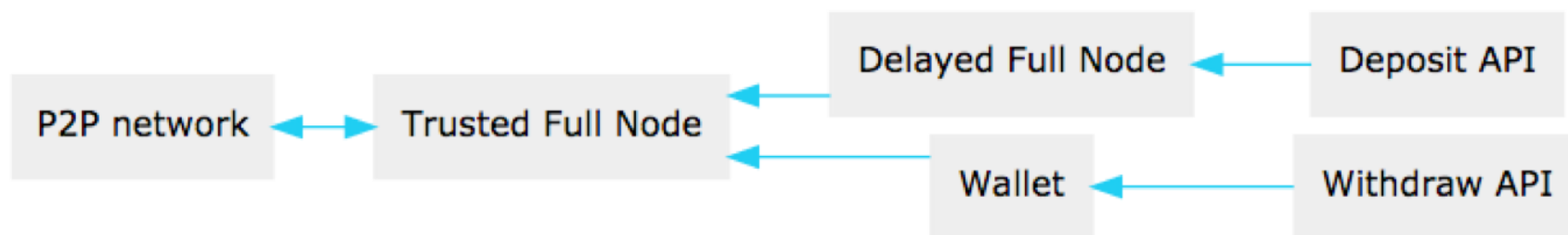
交易所VS网关

- 接收法币并发行IOU
- 撮合交易
- 处理IOU提现

- 接收法币并发行IOU
- 处理IOU提现
- 采用bitCNY可以完全避开网关风险

如何开发：Wallet API

RPC-HTTP, WebSocket API



讨论和问答

恒星Stellar：智能清算网络



背景

- 传奇人物Jed McCaleb
 - Stellar创始人兼CTO
 - Ripple创始人
 - 第一个比特币交易所Mt.Gox创始人
 - eDonkey创始人
- 恒星开发基金会SDF
 - 2014年成立
 - 非盈利组织



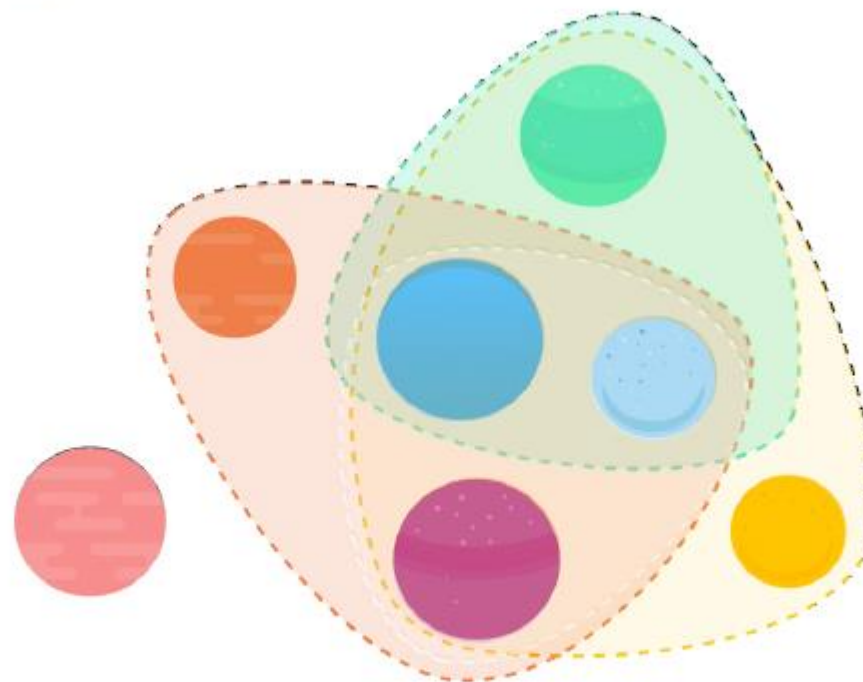
技术

- 恒星共识协议 SCP
- 保存余额状态
- 节点可以选择性同步账本
 - 完全节点
 - 普通节点，选择保存最近账本
- 无虚拟机、组合式的智能合约



灵活的共识算法SCP

- 共识与资产无关
- 拜占庭容错
 - 节点自行选择信任
 - 2-5秒
 - 无分叉、无须延迟确认
- 性能高
 - 300到1000笔每秒



Stellar Consensus Protocol (SCP)

灵活的共识算法SCP

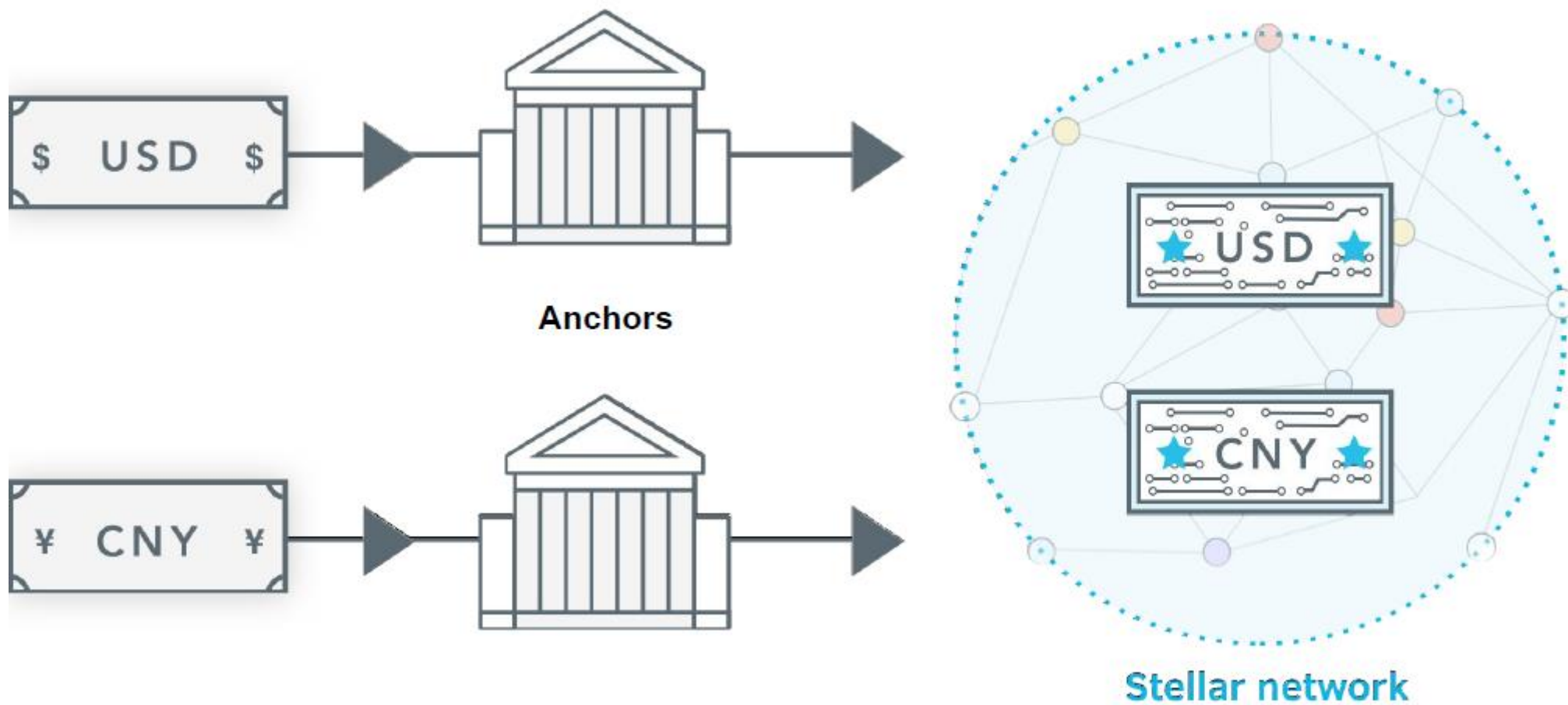
机制	去中心化 控制	低延迟	灵活信任
POW	是		
POS	是	可能	
拜占庭协议		是	是
恒星共识协议	是	是	是

技术特点

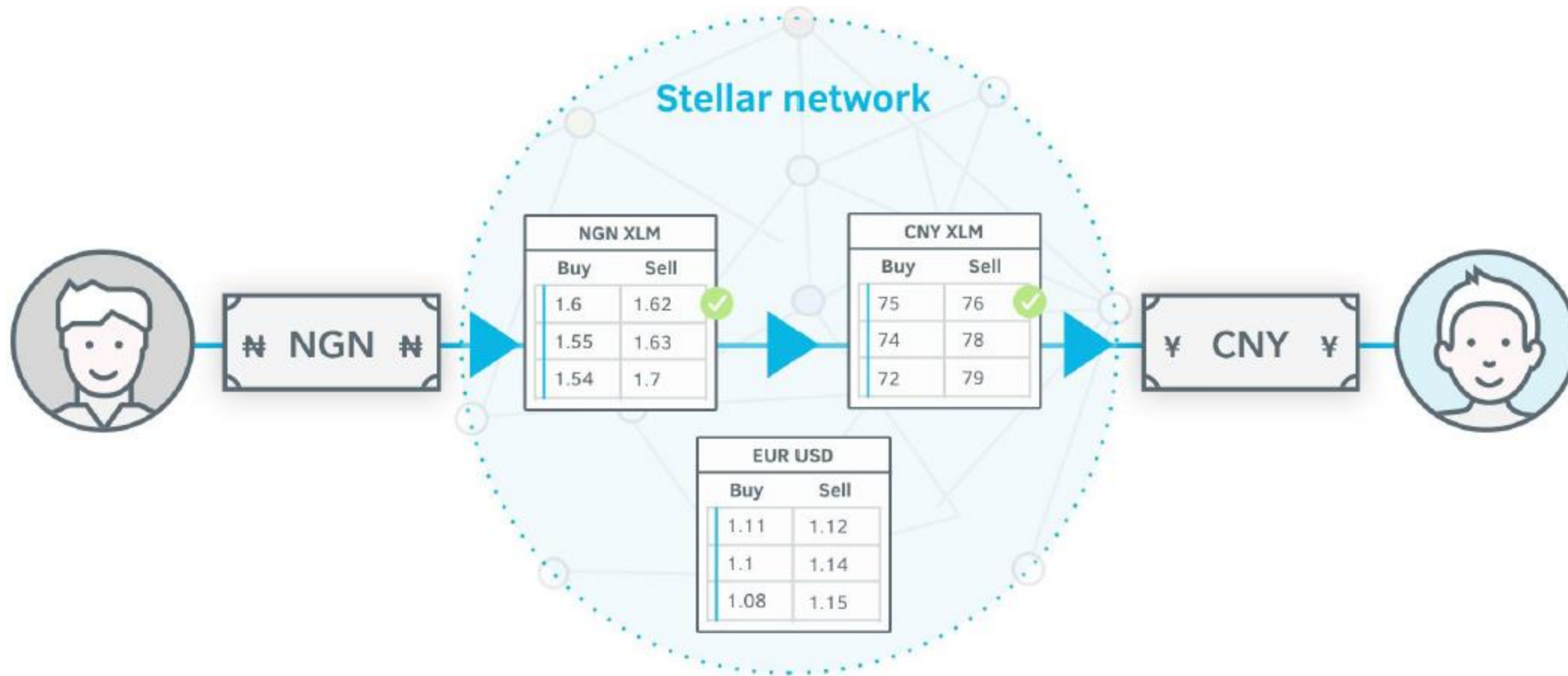
- Stellar Core : C++
- 应用层SDK : JS , Java
- 有HTTP API接口
- 组件完全开源
- 可加入公网或自建网络



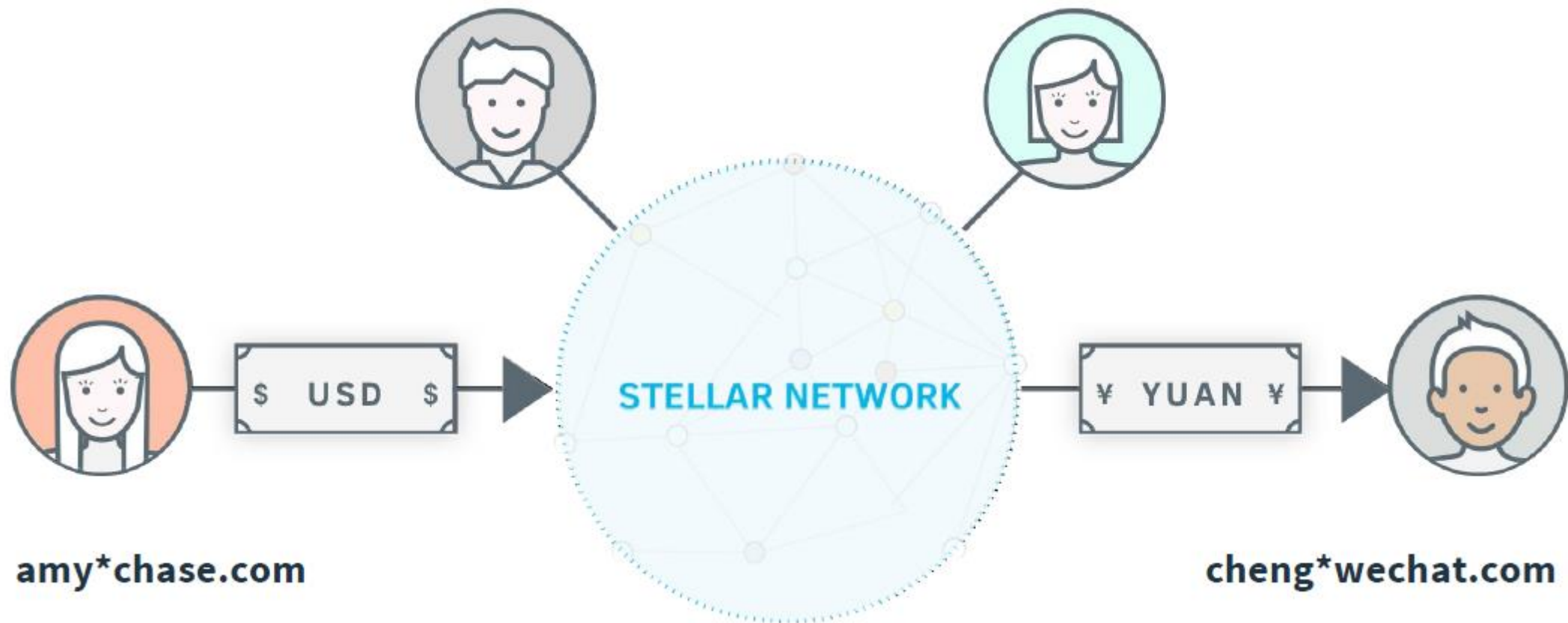
数字资产发行平台



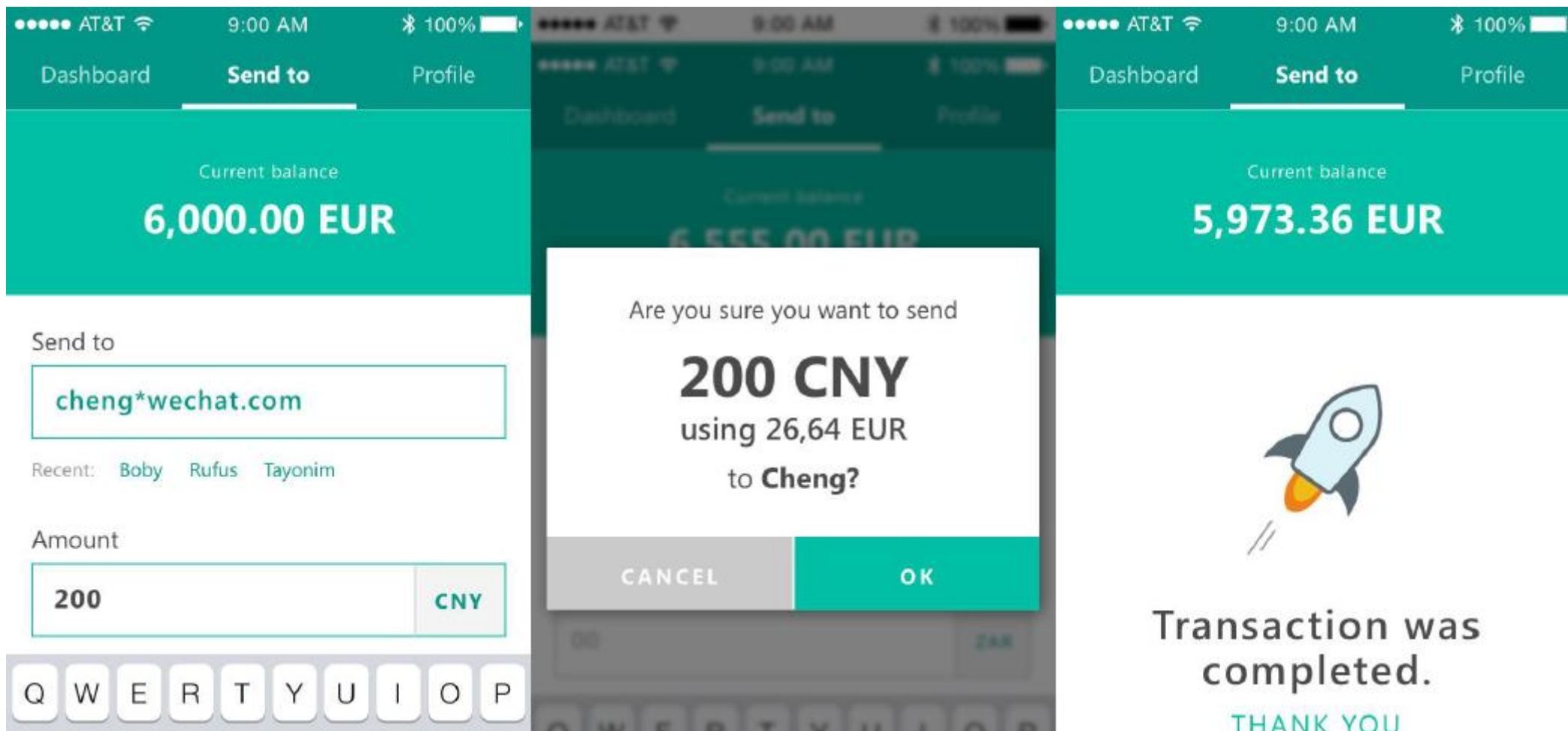
跨币种结算



联邦协议格式：信息*域名



联邦协议：支付领域的SMTP



多重签名：分级权限

- 低：授信
 - 允许账号接收某种资产
- 中：交易
 - 发送
 - 买卖
- 高：权限更改
 - 更改账号所有权
 - 更改签名者的权重
 - 更改低中高每级所需的权重

多重签名：联合签名账户

➤ 分级权重：

➤ 低 —— 0

➤ 中 —— 0

➤ 高 —— 3

➤ 持有者

➤ 老总：3

➤ 员工：1

➤ 分级权重：

➤ 低 —— 3

➤ 中 —— 3

➤ 高 —— 3

➤ 持有者

➤ 合伙人1：1

➤ 合伙人2：1

➤ 合伙人3：1

➤ 合伙人4：1

➤ 合伙人5：1

不可更改的资产

- 分级权重：
 - 低 —— 0
 - 中 —— 0
 - 高 —— 0
- 一次性发行足够数量的数字资产
- 将所有者的权重设为0

强大的交易功能

- 交易可以有多达一百个操作
 - 原子性
 - 只要有一个操作失败就整个交易无效
- 交易可以操作不同的账户
 - 所有涉及账户都必须对交易签名
- 交易有序号，按顺序执行

多重签名+操作组合+关联交易= 智能合约

交易1:

序号: N+1

操作组合:

创建一个出售100万份众筹股份的卖单, 价值1百万

签名: 政府+NGO

交易2:

序号: N+2

起效时间: 2016年12月1日

操作组合:

发送3百万资金到联合托管账户

签名: 政府+NGO

交易3:

序号: N+3

操作组合:

取消出售众筹股份的卖单

发送一百万资金到政府的账户

发送一百万资金到NGO账户

创建一个购买100万份众筹股份的买单

签名: 政府+NGO





































讨论和问答

技术对比和分析



代币

➤支付价值货币

➤比特币

➤汇兑中介

➤瑞波币

➤恒星币

➤抵押物

➤比特股

➤激励

➤POW

➤POS

➤权益证明和资源控制

➤POS

➤防攻击

➤交易费

共识机制的选择

➤与代币相关

- POS
- DPOS

➤不分叉、无延迟确认

- Ripple
- SCP
- PBFT

➤与代币无关

- POW
- Ripple
- SCP (恒星共识算法)
- PBFT

账本存储

➤ UTXO

- 比特币
- 完全账本

➤ 账本快照

- Stellar、Ripple
- 完全节点
- 轻节点

➤ 分片

➤ 状态旁路

资产发行和清算

➤以太坊

- 图灵完备
- 性能较弱
- 功能齐全

➤恒星

- 针对性解决方案
- 性能强大
- 智能合约是有限的

➤瑞波、比特股

- 针对性解决方案
- 性能强大
- 无智能合约

讨论和问答