通付盾
Pay Egis

基于区块链的身份认证系统研究与实践

汪德嘉 博士

通付盾创始人

密级：可对外发布

通付盾 Pay Egis

目录

CONTENT

01 第一篇：HUE多因子身份认证

02 第二篇：区块链身份认证研究

03 第三篇：数字货币安全研究

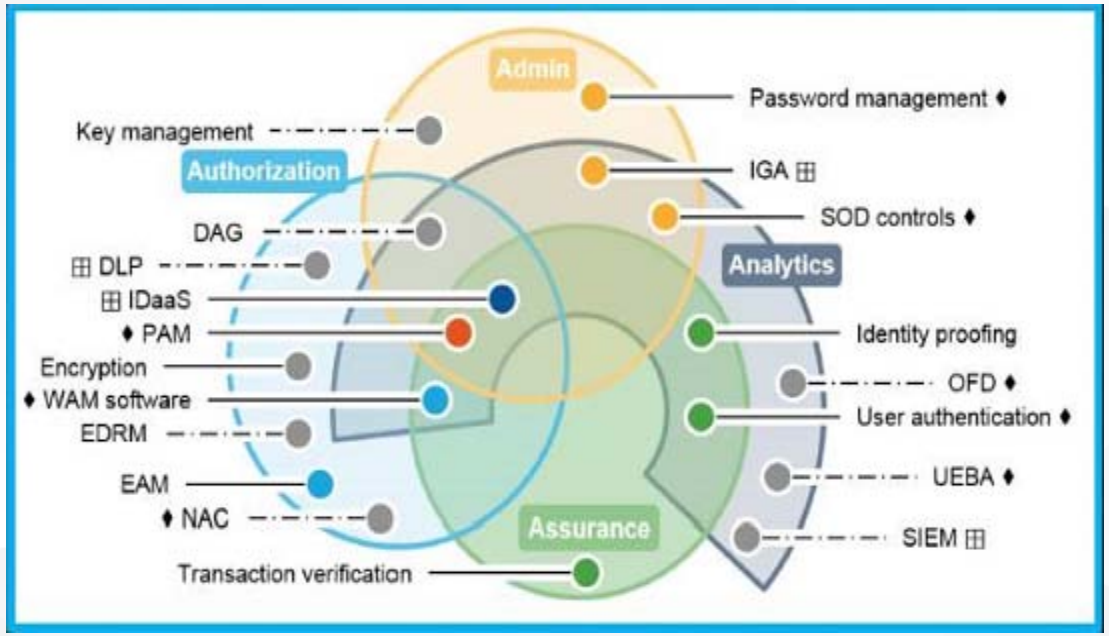
Part

01

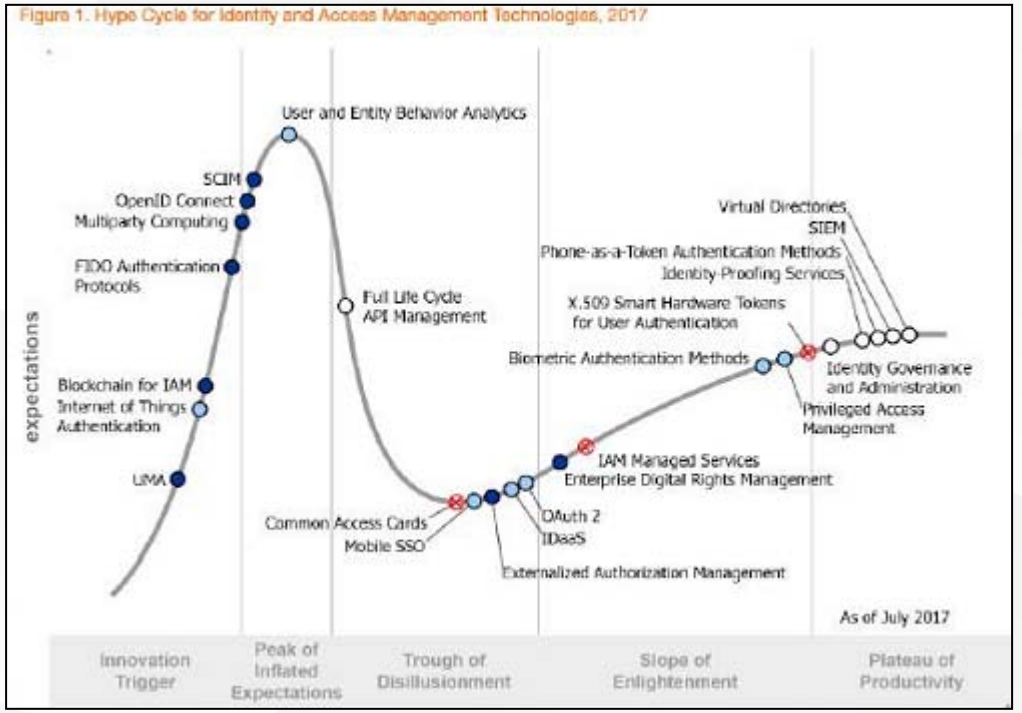
第一篇：HUE多因子身份认证

身份认证技术的发展

身份认证领域，由最初的口令管理、密钥管理，发展到网络访问控制、数据访问控制，再到最新的IDaaS。管理范围已经从简单的信息管理扩展到身份相关全生命周期管理。IDaaS、 User and Entity Behavior Analytics（UEBA）、 IoT Authentication、 Biometric Authentication 、 FIDO等技术的兴起和成熟给解决开放环境下身份认证难题带来了思路。



Gartner 2016《What You Must Know About Identity and Access Mangement in 100 Tweets》



Gartner《Hype Cycle for Identity and Access Management Technologies 2017》

移动互联网时代：身份认证危机重重

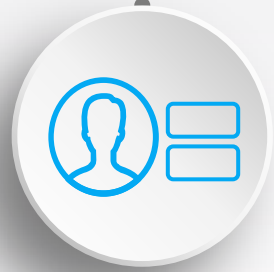
身份计算概念的兴起

如何找到安全与便捷的“平衡木”？

通付盾 Pay Egis

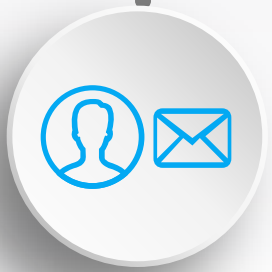
账号密码

- ✓ 安全性：安全级别非常低
- ✓ 易用性：普适性
- ✓ 成本：无成本



账密+短信验证码

- ✓ 安全性：安全级别低
- ✓ 易用性：简单方案，使用广泛
- ✓ 成本：短信收发

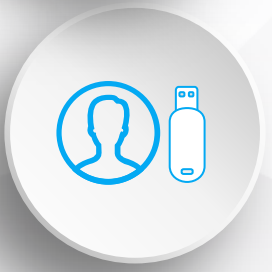


便捷性 VS 安全性

低成本

- ✓ 安全性：中等安全级别
- ✓ 易用性：需携带额外硬件
- ✓ 成本：令牌+服务器+维护

账密+动态令牌

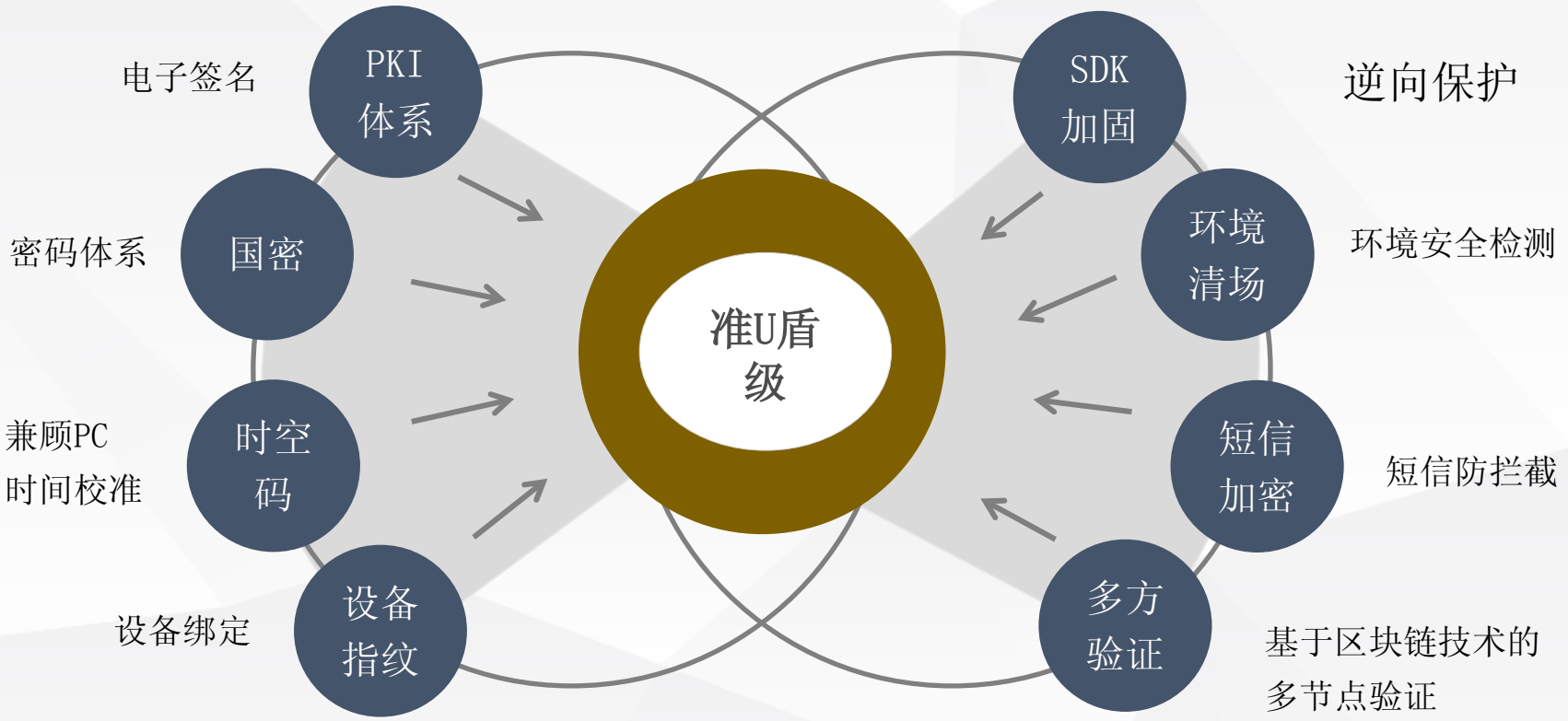


- ✓ 安全性：安全级别高
- ✓ 易用性：携带额外硬件，连接移动端
- ✓ 成本：U盾+证书+认证服务器+维护

账密+U盾

HUE多因子身份认证产品

Host USB Key Emulation Identity Authentication Component



HUE多因子身份认证产品

Host USB Key Emulation Identity Authentication Component

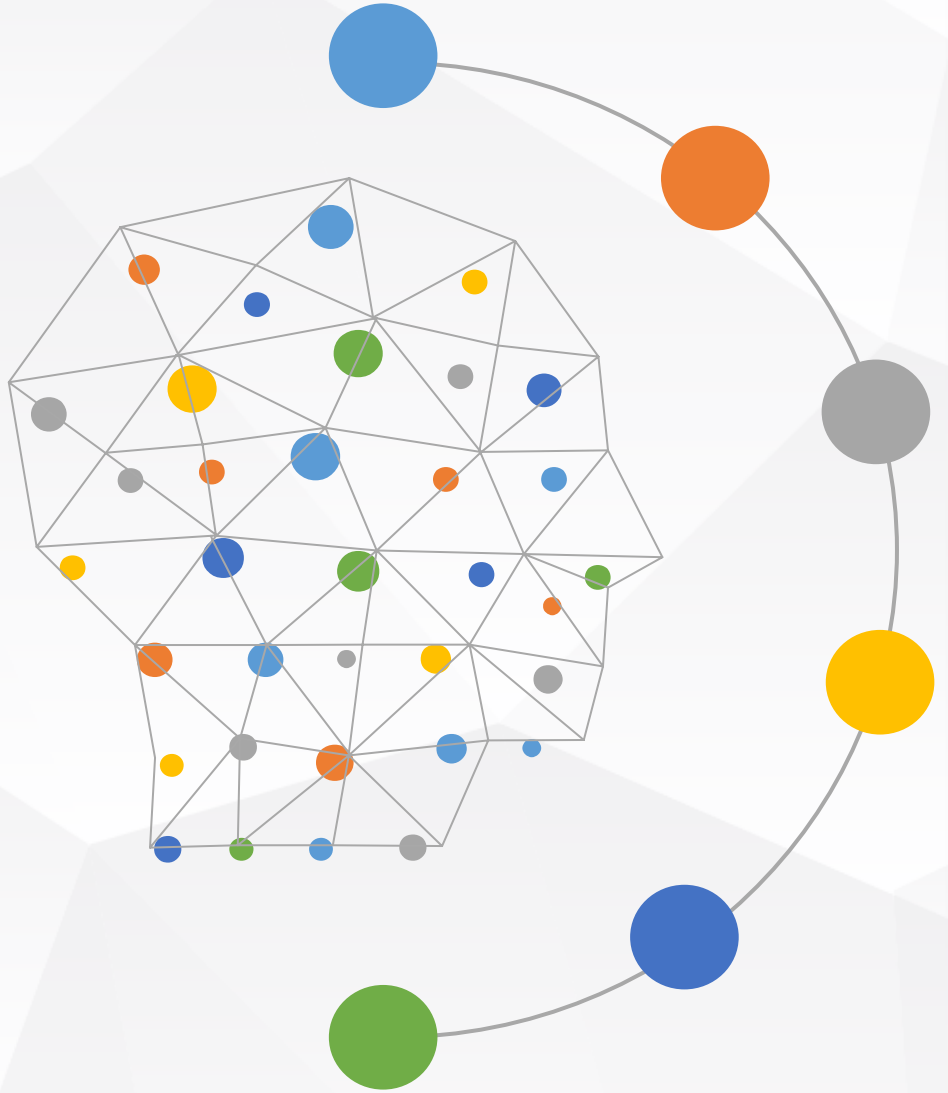
通付盾 Pay Egis

前沿的密码学理论

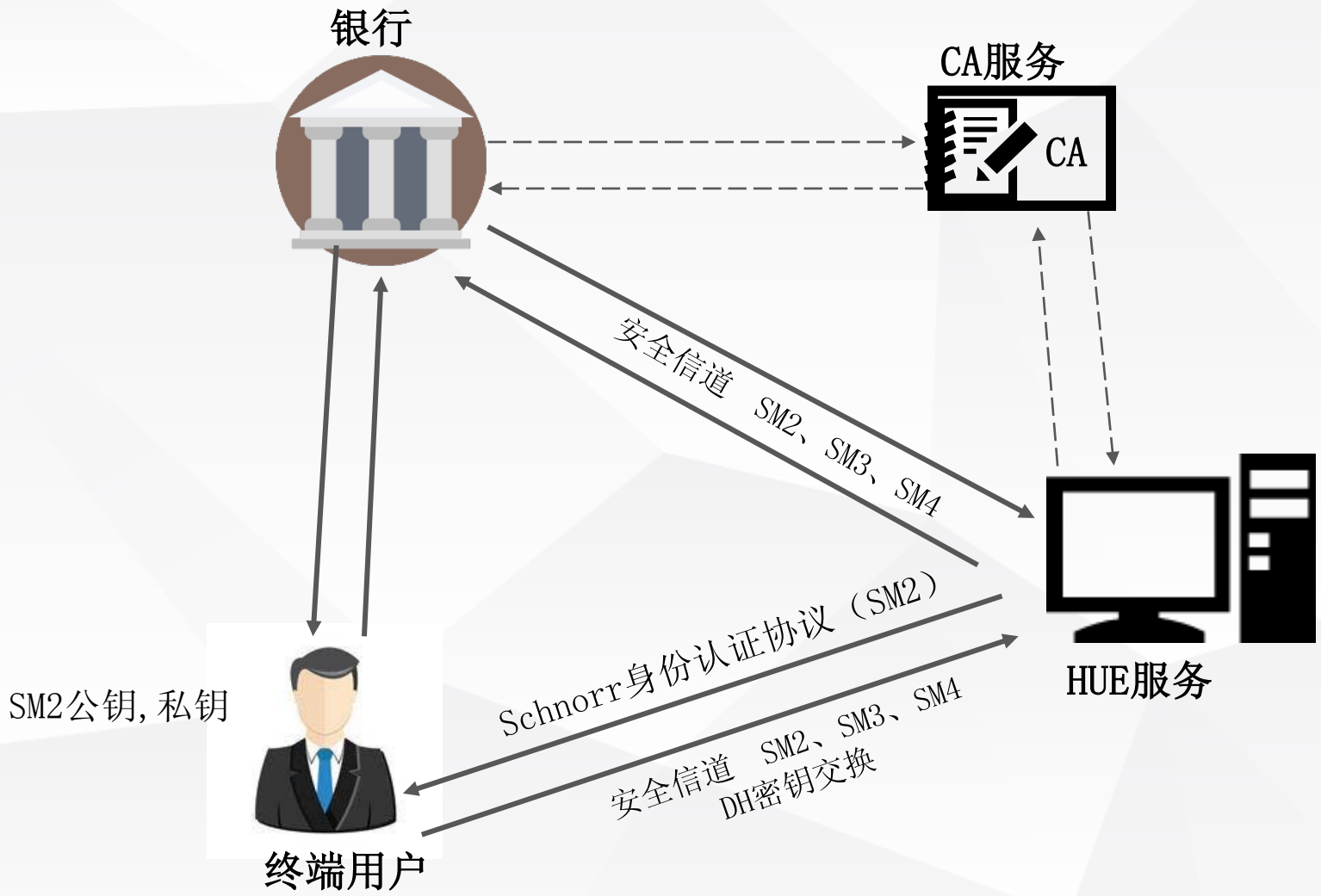
- 抗量子计算的密码学理论
- IBS公钥签名与加密体系 [Dan Boneh, Stanford]
- 基于椭圆曲线双线性配对的同态隐藏技术 [Andrew MIiller, UIUC]
- 非交互式零知识证明技术 (Eli Ben-sasson, Technion)
- 基于格的同态加密技术 (Craig Gentry, IBM)

自主知识产权的区块链技术 (40+项专利申请)

- 基于区块链的大规模数据存储
- 基于移动设备的轻节点技术
- 基于移动设备的共识协议
- 区块链网络性能优化技术



HUE融入市场：银行业客户案例



多因子身份认证——广东农信

项目的目标是综合运用电子签名、数字证书及手机终端设备认证技术，实现手机银行免外设（如蓝牙盾）完成大额资金交易的目标。

通过本项目的建设：

一、可以**满足监管**部门发布的如电子签名法、261号文、170号文及金融电子认证规范等系列监管文件要求。

二、通过手机设备认证将手机作为安全载体通过用户密钥及证书安全技术实现手机银行大额资金交易的**安全认证**。

三、通过手机银行软加密产品技术将手机作为安全载体，无需额外硬件设备满足客户资金交易要求，用户**体验便捷**，同时银行无需采购硬件Ukey**降低成本**。

HUE多因子身份认证帮助行方提升手机银行安全性和便捷性、满足国密改造要求、满足监管部门的要求。

部分需求说明

序号	需求概述及说明
1	认证因子： ● PIN 码认证 ● 手势密码认证 ● CA 安全证书认证 ● 重要信息确认认证
2	认证方式组合： ● 重要信息确认认证+手势密码认证+ CA 安全证书认证 ● 重要信息确认认证+ PIN 码认证+ CA 安全证书认证
3	支持业务流程： ● 安装安全证书（绑定） ● 删除安全证书（解绑） ● 身份认证 ● 修改密码 以上业务流程皆由用户在 APP 端开展，其中删除安全证书（解绑）也支持用户在网银客户端开展。
4	HUE 认证组件产品名称暂定：安全证书；由通付盾位安全证书产品设计一款
5	PIN 码的安全策略 :PIN 码长度为 6-8 位 ,必须同时包含字母和数字两种字符，不需要同时包含大小写字母，但 PIN 码中的字母是区分大小写的。
6	软证书管理界面（申请界面、证书状态界面、删除证书界面等）由行方设计、开发，HUE 提供 SDK 接口供行方调用。
7	手势认证中的手势绘制需做到无感知。
8	证书安装码认证（即加密短信认证）由行方生成、校验，通付盾 HUE 负责加解密；证书安装码可使用 3 次，证书安装码的有效期待定。
9	安装证书时 PIN 码/手势码设置界面需增加提示文案：当前选择设置 PIN 码，则后续转账汇款中将始终校验 PIN 码，不可更改为手势密码；当前选择设置手势密码，则后续转账汇款中将始终校验手势密码，不可更改为 PIN 码。
10	CA 安全证书认证使用行方自建 CA
11	CA 证书有效期为 2 年，证书过期的两种处理方式： 当证书尚未过期时，用户可在 APP 端通过软证书管理界面的“更新证书”功能完成证书更新（即重新绑定）（需先前往柜面/网银客户端获取证书安装码）； 当证书已经过期后，用户可在 APP 端点击软证书管理界面的“安装证书”走初次绑定流程生成新的证书（需先前往柜面/网银客户端获取证书安装码）；

安装证书并绑定--开启“安心付”

安全便捷转账--使用“安心付”

其他安全性保障


手指轻触 登录如此简单
指纹登录 正式上线
我的账户
转账汇款
定活互转
个人贷款
预约提现
当面清
软证书服务
当前设备与安全证书安装设备不一致
客服热线
消息中心

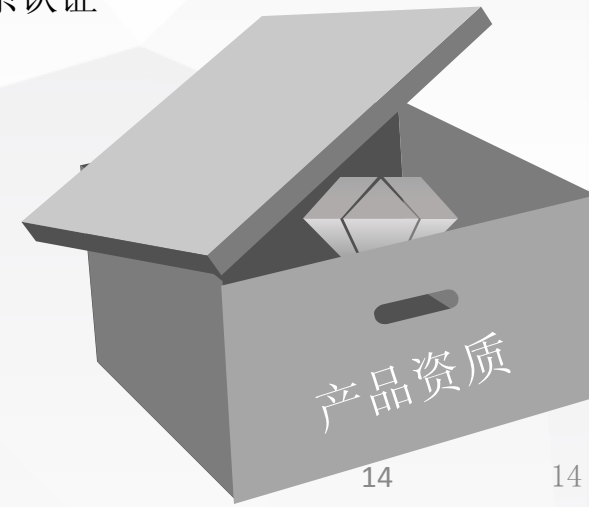

美人玉甜瓜
美人似玉瓜如蜜
温馨提示
您的账号已锁定，请前往柜面或登录网银系统更新证书！
确定
客服热线
消息中心


软证书管理
安装证书
修改密码
温馨提示
删除数字证书后，将无法XXXXXX，若想再次安装数字证书，需再次前往网点或者登录UKEY版网银申请。
取消


想一起
绽放普惠理想
账户管理
转账汇款
定活互转
个人贷款
广东农信安全键盘
完成
1
2
3
4
5
6
7
8
9
abc
0

HUE产品资质

- 公安部计算机信息系统安全专用产品销售许可证
- 中国国家信息安全漏洞库（CNNVD）技术支撑单位
- 商用密码产品型号证书
- 商用密码产品销售许可证
- 信息安全风险评估一级服务资质认证
- 信息安全应急处理三级服务资质认证
- EAL3信息安全产品分级评估
- … …
- CMMI3软件能力成熟度集成模型
- ISO27001信息安全管理体系认证
- ISO9001质量管理体系认证



14

HUE产品优势

合规性

- ✓ 符合电子签名法
- ✓ 符合银发11号文
- ✓ 符合银发170号文
- ✓ 符合银发261号文

安全性

- ✓ 账号安全保护
- ✓ 交易安全保护
- ✓ 环境安全检测
- ✓ 大额交易认证
- ✓ 认证记录追溯
- ✓ 防交易抵赖

便捷性

- ✓ 无需附加硬件
- ✓ 兼容PC端
- ✓ 认证方式快捷
- ✓ 用户体验良好

低成本

- ✓ 无需硬件成本
- ✓ 无需证书成本
- ✓ 云部署方式
  - 节约服务器成本
  - 节约维护成本
- ✓ 前置机+云部署方式
- ✓ 本地部署方式

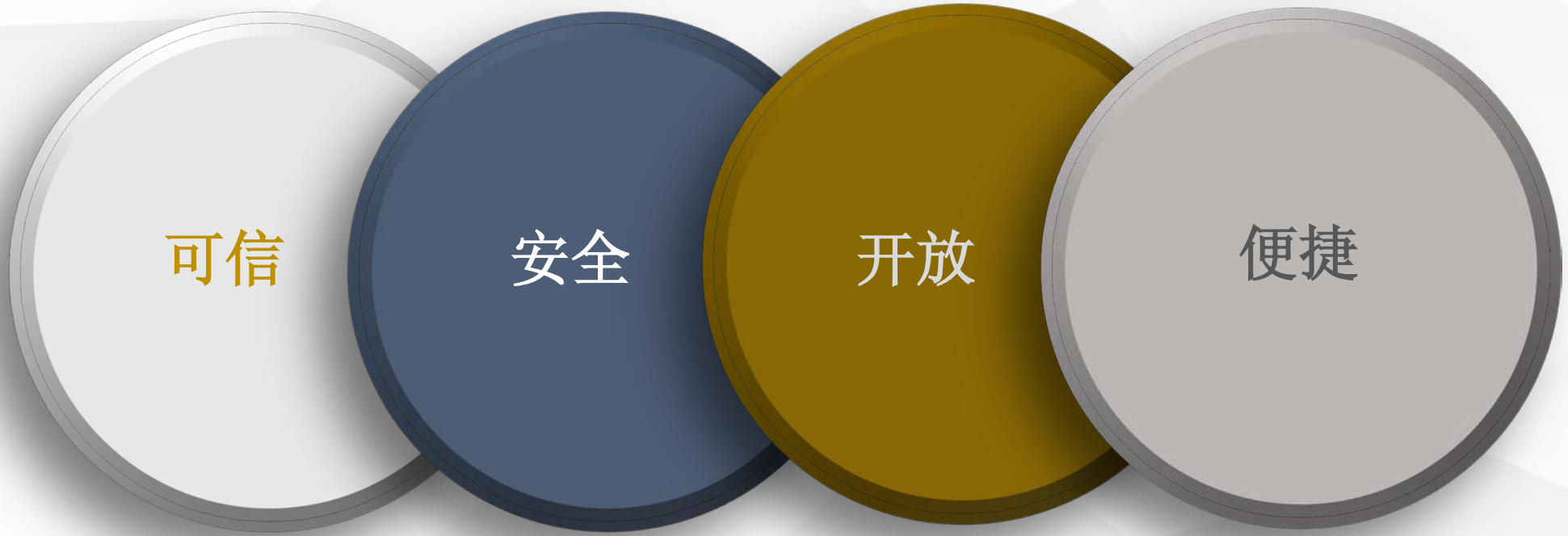
Part
02

第二篇：区块链身份认证研究

基于区块链的PKI认证体系

基于区块链的IBS数字签名与身份认证体系

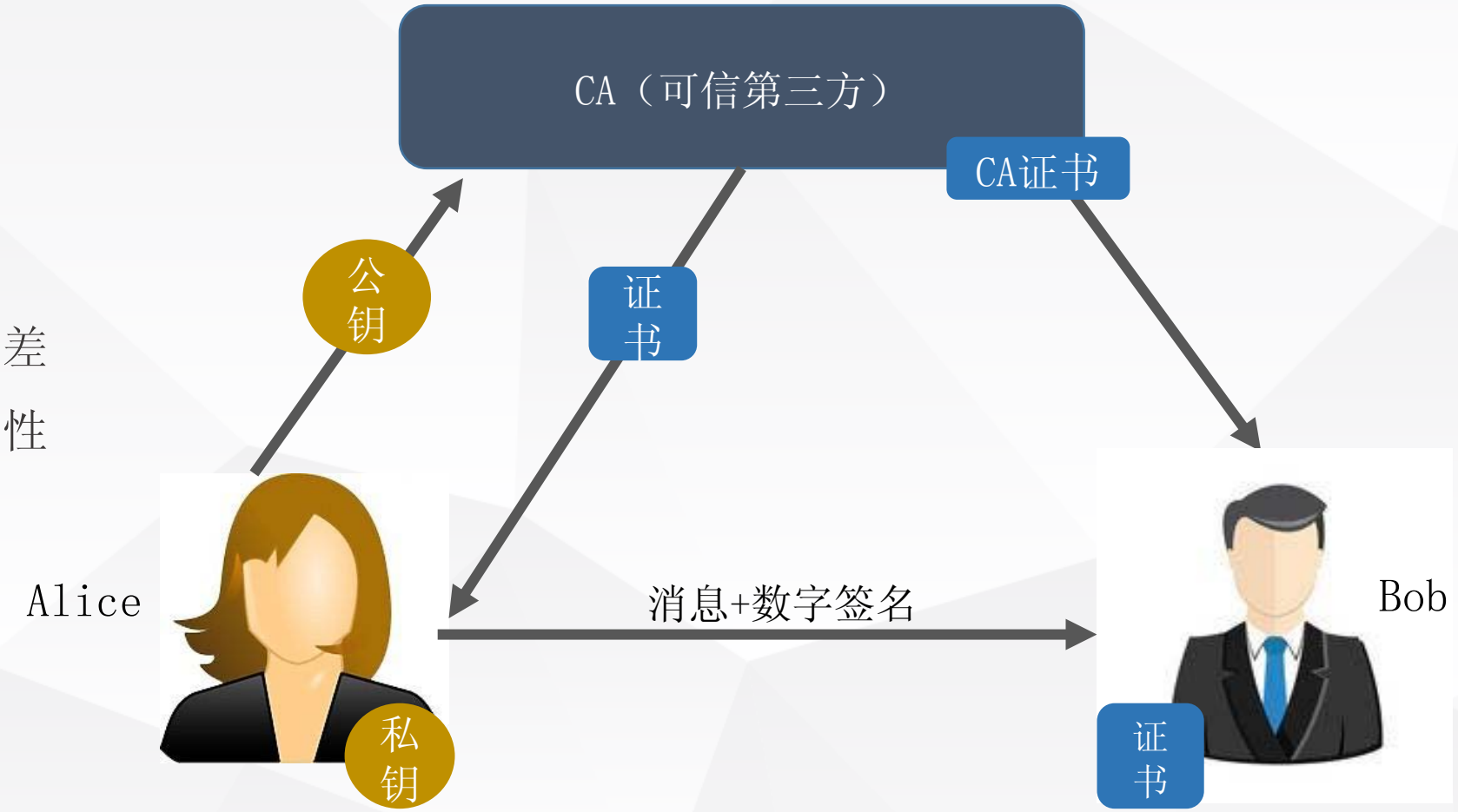
基于区块链的身份认证系统



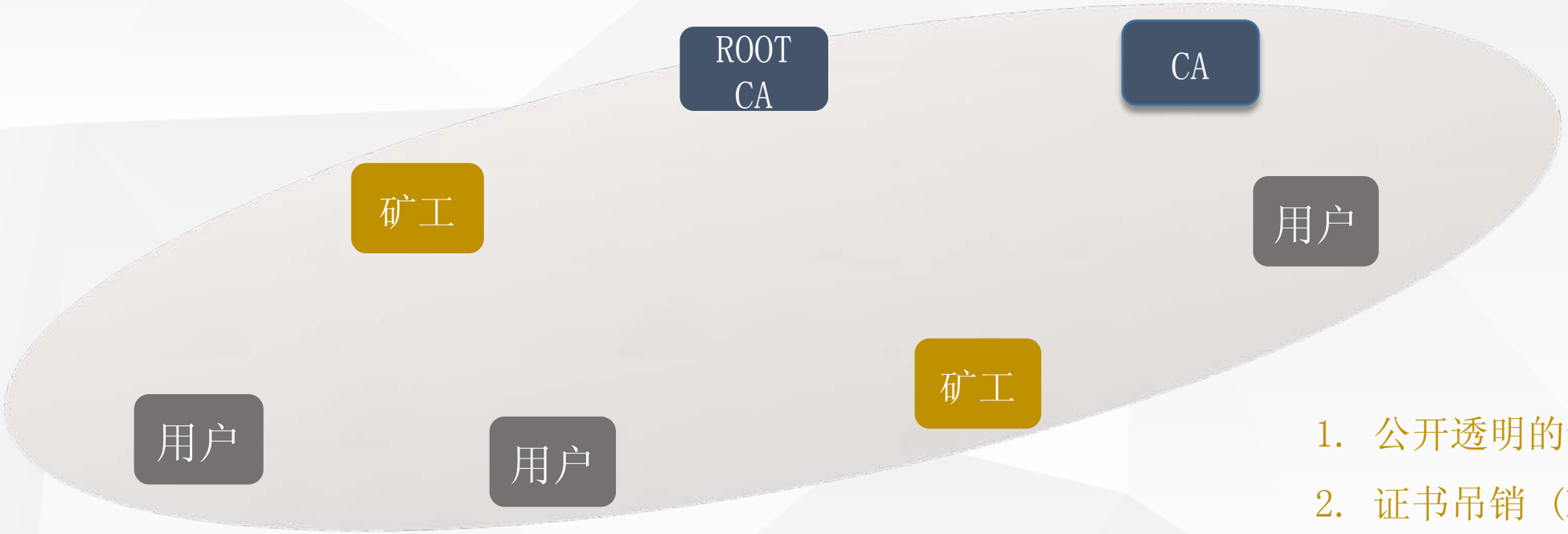
传统的PKI公钥认证体系

Weakness

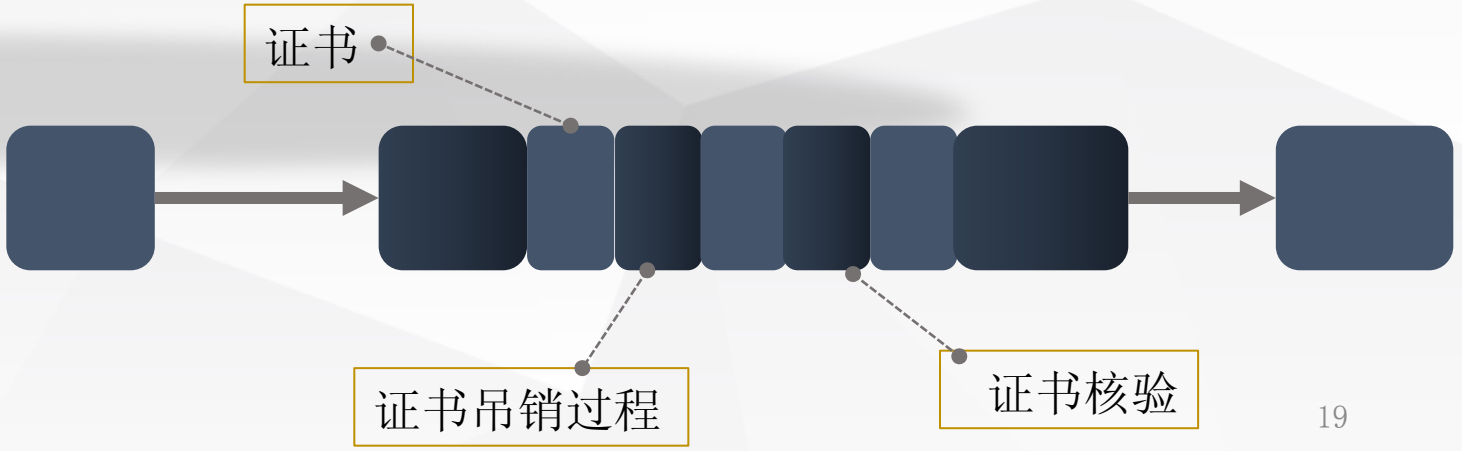
1. 依赖绝对安全可信的第三方
2. 证书被盗与吊销之间有时间差
3. 证书存在被破解伪造的可能性



基于区块链的PKI体系



1. 公开透明的证书管理
2. 证书吊销（Revoking）的广播与存证

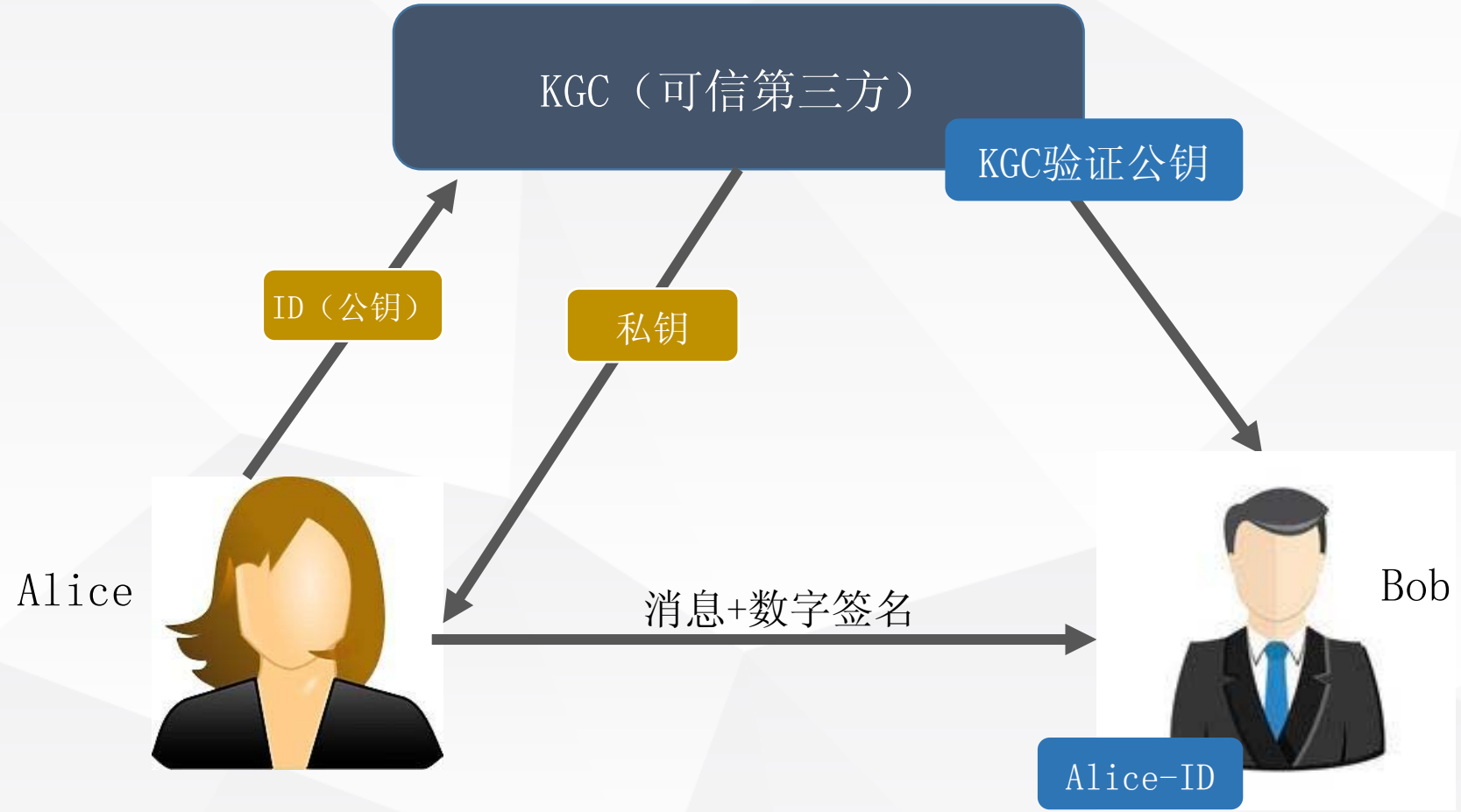


传统的IBS公钥认证体系（Boneh-Franklin 方案）

IBS：基于身份ID的公钥体系

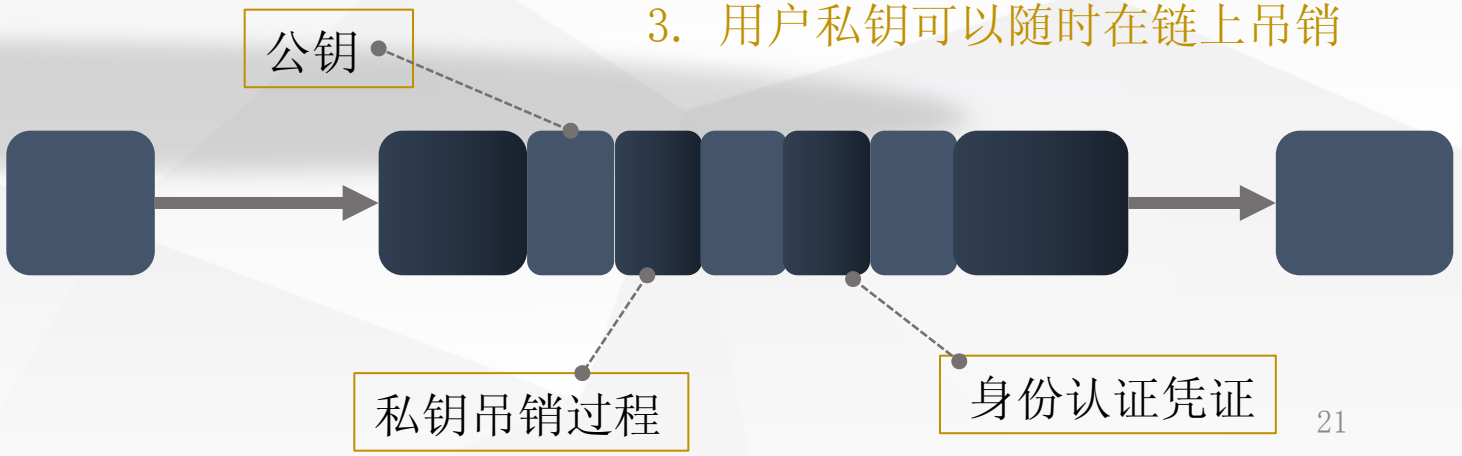
Weakness

1. 依赖绝对安全的第三方KGC
2. KGC可以伪造Alice身份
3. 私钥难以吊销



基于区块链的IBS数字签名与身份认证体系

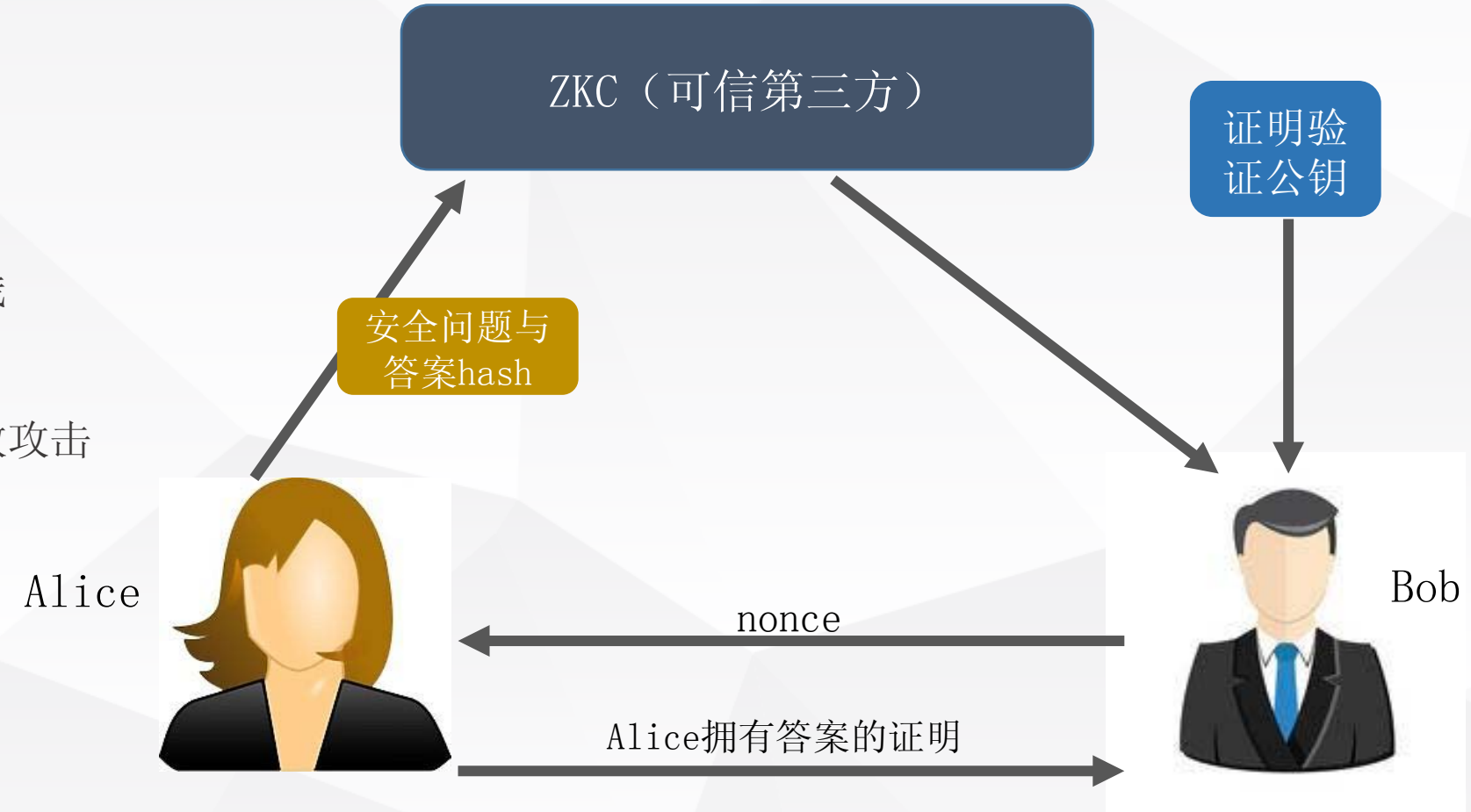
1. 去中心化的KGC，安全可靠
2. 用户可以采用多个KGC进行身份认证，避免KGC伪造身份
3. 用户私钥可以随时在链上吊销



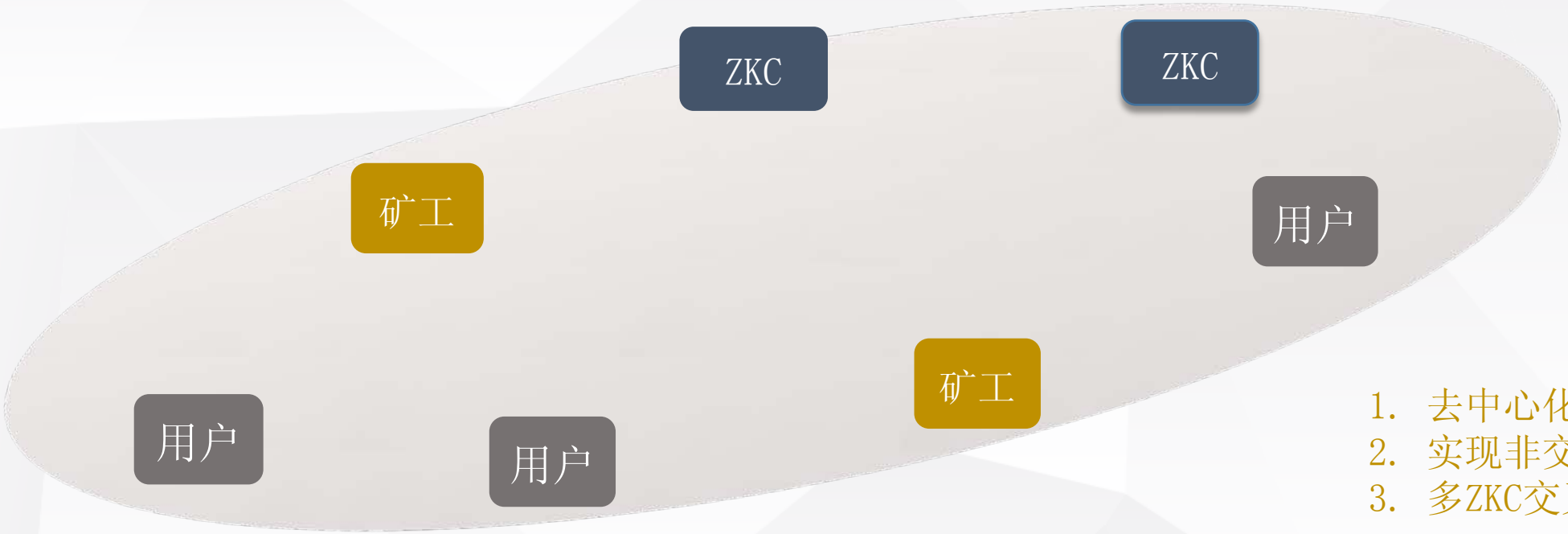
零知识证明ZKP认证协议（zkSNARK方案）

Weakness

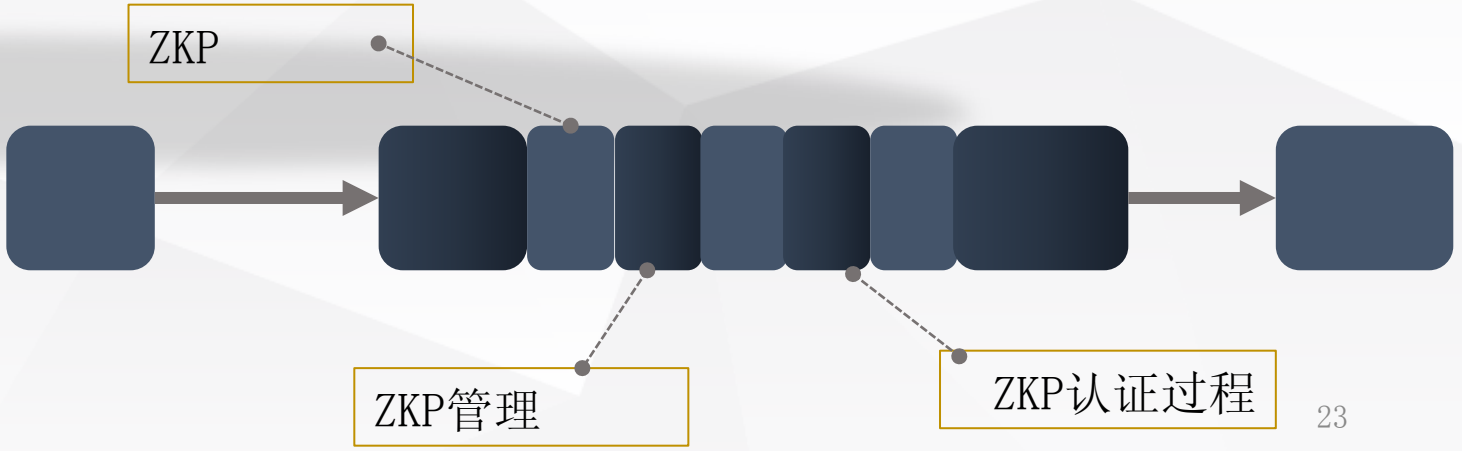
1. 依赖第三方ZKC，要求其在线
2. ZKC自身的身份认证；
3. 非交互式的ZKP难以防止重放攻击



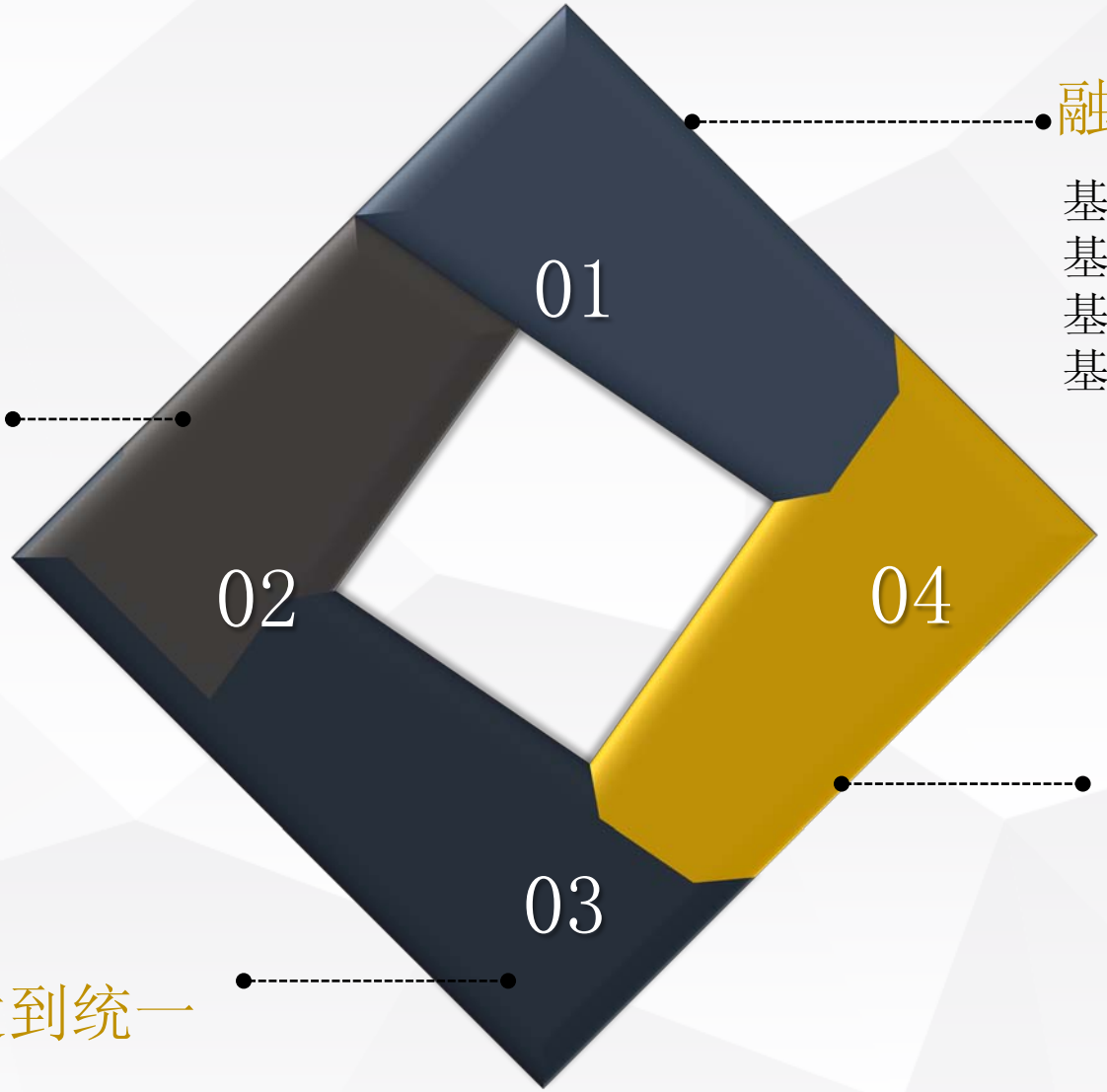
基于区块链的零知识证明(ZKP)身份认证系统



1. 去中心化的ZKC
2. 实现非交互式ZKP的防重放攻击
3. 多ZKC交叉互相认证



基于区块链的身份认证系统——BA



融合多种公钥体系

基于椭圆曲线签名的底层公钥体系
基于PKI的证书公钥体系
基于IBS的身份交互认证体系
基于ZKP的身份认证体系

适用于多种场景与架构

基于生物特征的认证的扩展

安全与便捷性达到统一

Part

03

第三篇：数字货币安全研究

央行发行数字货币的必然性

通付盾 Pay Egis

实物货币

货币形式发展的第一阶段，其作为货币用途的价值，与其作为非货币用途的价值相等。

金属货币

以金属作为货币材料，充当一般等价物的货币。

信用货币

由国家法律规定的，强制流通不以任何贵金属为基础的独立发挥货币职能的货币。

电子货币

指用一定金额的现金或存款从发行者处兑换并获得代表相同金额的数据或者通过银行及第三方推出的快捷支付服务。

数字货币

网络社会经济和科技发展到一定阶段的必然产物，是满足货币流通的安全性与便捷性需求的存在，代表着未来货币存在形式的发展方向。

1、以国家信用为保证发行数字货币，可最大范围地实现线上与线下同步应用，最大限度提升交易便利性与安全性。

2、发行和推广法定数字货币无疑具有巨大政策效益与社会效益。

货币的发展

央行的法定数字货币的特点

通付盾 Pay Egis

央行发行

作为本位币的新形态，央行发行的数字货币是真正意义的货币

二元模式

兼容现有货币二元体系，逐步替换

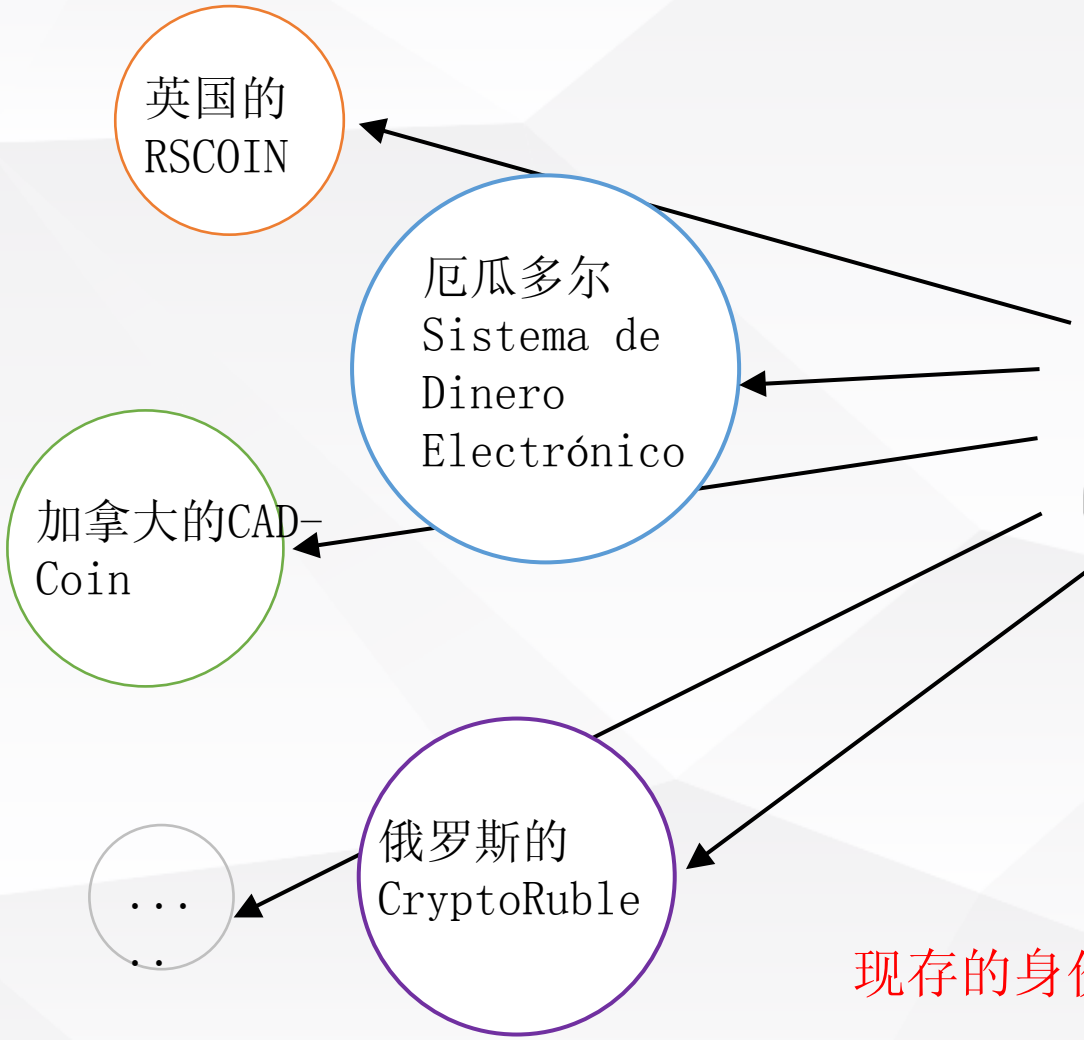
金融安全

更加有效的宏观经济调节工具，更加灵活的管控与监管

行业变革

传统的支付、结算、票据等金融行业将面临重大变革

央行发行数字货币的安全挑战



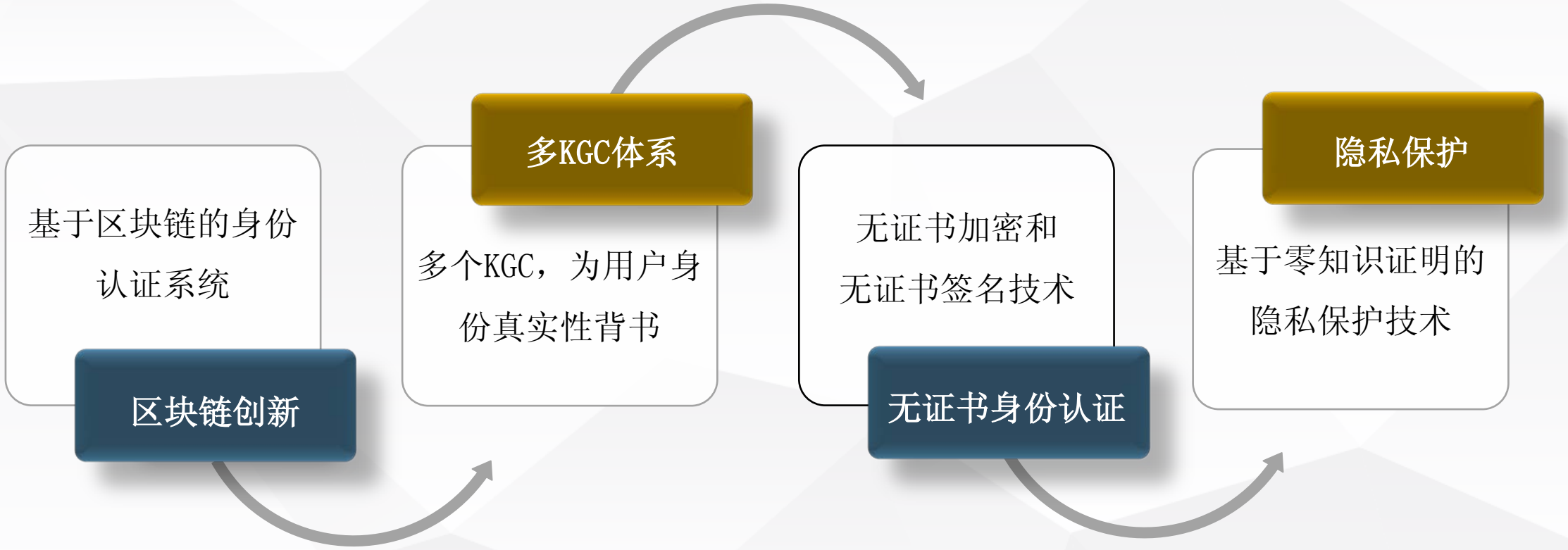
2014年2月7日，黑客对世界最大规模的比特币交易所Mt.Gox发起交易延展性攻击成功骗取了数十万个比特币。

Bitfinex数字货币交易平台曾被爆遭黑客攻击，导致近12万个比特币（总价逾6000万美元）被盗。

.....

现存的身份认证体系如何应对数字货币时代身份认证安全的挑战？

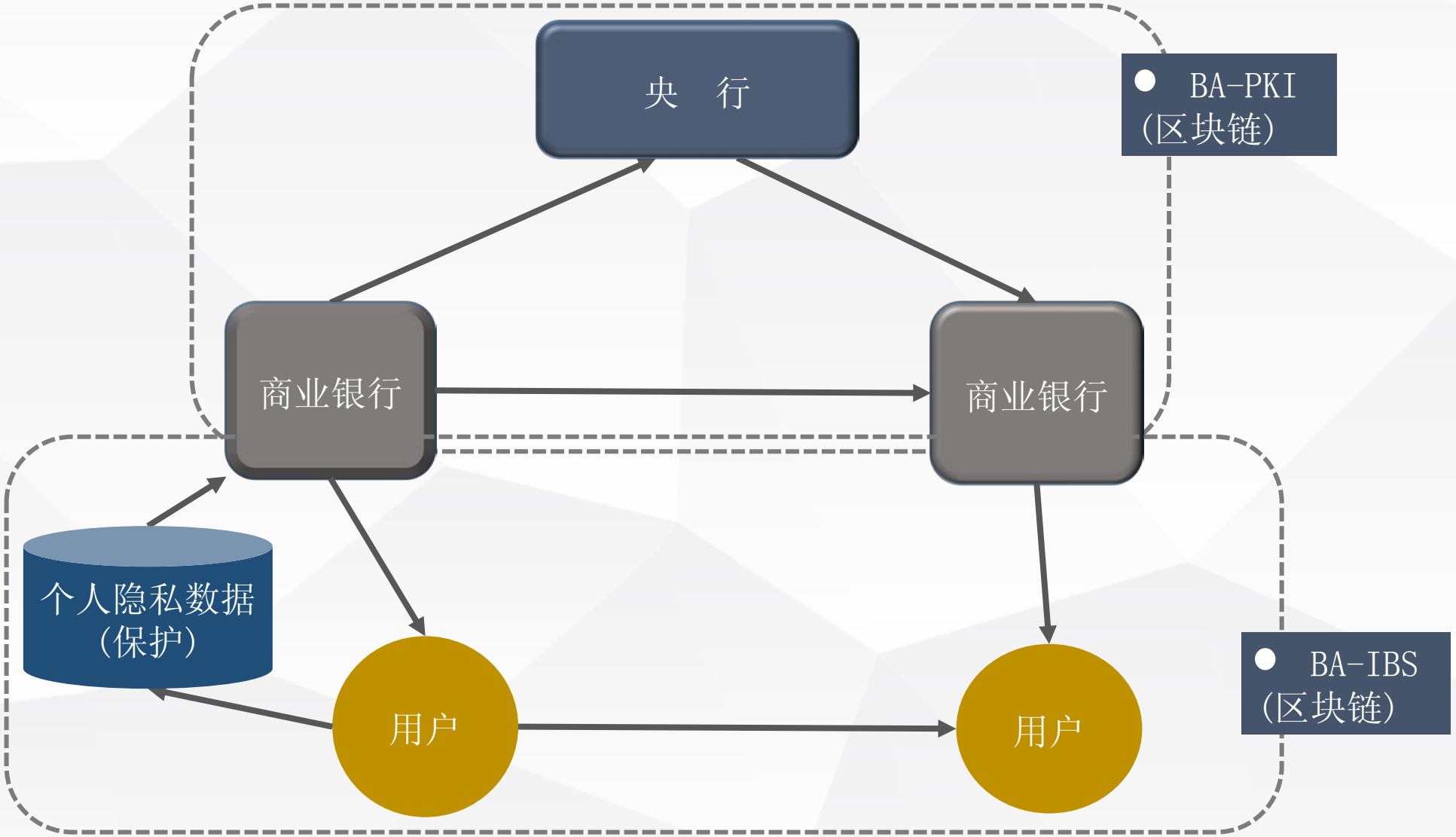
通付盾数字货币研究组研究重点



通付盾数字货币项目组深入研究数字货币发行、流通、支付、回笼各个环节的风险点，提出了基于PKI区块链与IBS区块链技术结合的无证书身份认证和隐私保护技术。

数字货币发行流通整体解决方案

从发行和流通两方面切入，着重于数字货币体系中**身份认证**进行了研究，提出了发行端PKI**区块链技术和流通端IBS区块链技术相结合**的安全体系构成。



研究成果-基于区块链的身份认证系统(BA)

宗旨：建立一个开放、可信、安全、便捷的身份认证系统，为数字货币的发行与流通提供高安全、高便捷的确权认证与身份校验服务。

BA系统相关概念

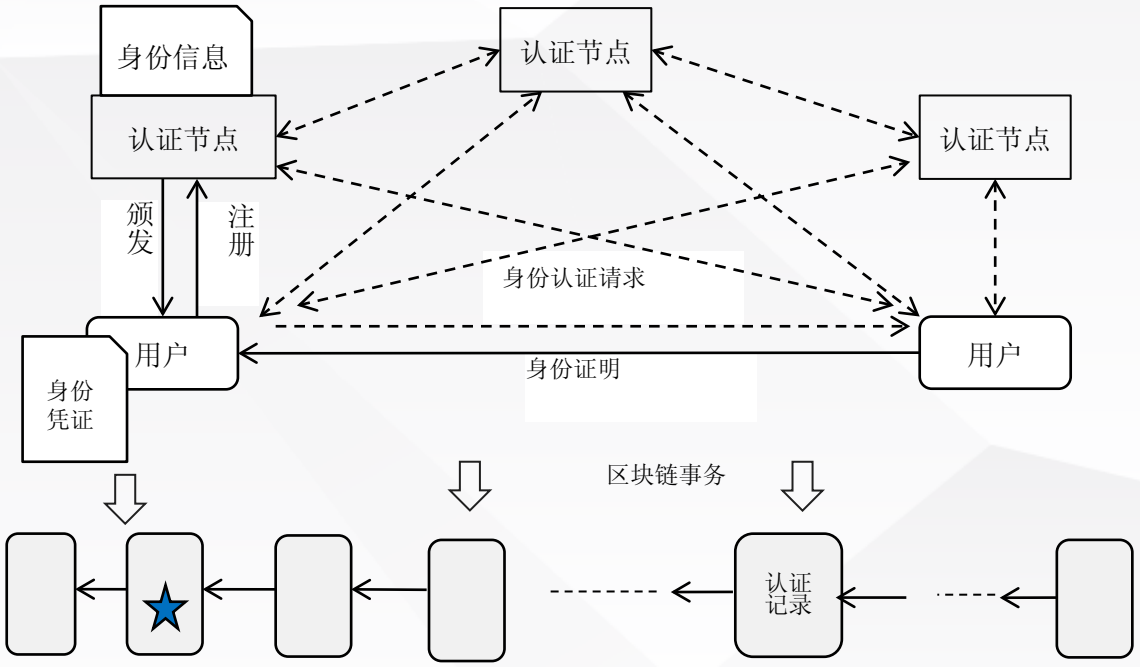


图1. 基于区块链的身份认证系统（BA系统）示意图

区块链节点(Node)：
接入区块链网络的任意一个客户端都是一个节点，所有节点通过共识协议来产生区块，区块链节点主要包括认证节点与用户节点。

区块(Block)：
区块是区块链的组成部分，用于存储有价值的信息。

区块链事务（Transaction）：
区块链节点之间的交互所产生的消息或事件，携带相关的事务内容、数字签名、智能合约与带外数据。

区块链地址(address)：
任何区块链节点加入区块链之前，需要产生一对公私钥，其中公钥经过处理之后产生一个字符串，作为区块链地址，该地址作为认证事务的接受者标识。

BA-PKI身份认证子系统

用于数字货币发行端，解决银行等金融机构的身份安全问题！

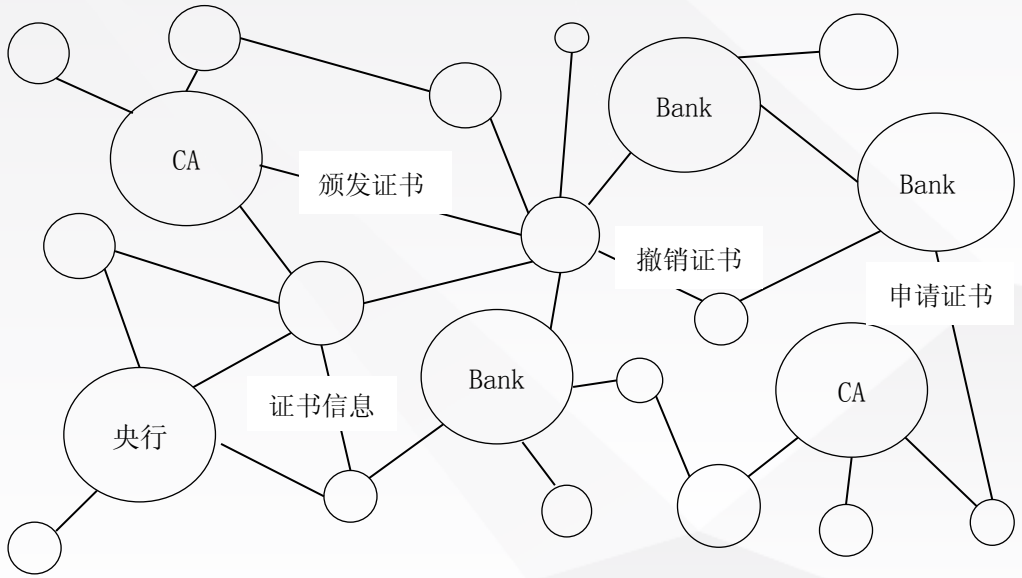


图2. BA-PKI子系统基本构成示意图

预防被伪造

通过UTXO关联技术将用户数字证书申请、颁发与撤销的全过程相互关联地存储在区块链上，实现用户数字证书在区块链上的可追溯，弥补了传统PKI体系中数字证书存在被伪造可能的缺陷。

及时撤销证书

使用UTXO管理技术管理所有被有效颁发的证书，CA撤销的证书可被及时地从BA-PKI子系统的证书管理池（存放在区块链上）中销毁，弥补了传统PKI体系中证书撤销不及时的缺陷。

降低CA私钥泄露危害

使用分布式CA管理模式，即用户证书的颁发与撤销需多个CA提供数字签名，使得即使单个CA私钥泄漏，攻击者也无法伪造用户数字证书，极大降低了单个CA私钥泄漏带来的危害，弥补了传统PKI体系中过度依赖单个CA的缺陷

BA-IBS身份认证子系统

优点1

（1）采用了IBS无证书公钥认证技术，使得用户的身份信息被包含在用户公钥中，相比难以辨识的PKI公钥，该系统中包含身份信息的公钥使用更便捷。

优点2

（2）采用了区块链技术，使得认证节点为用户节点颁发公私钥对的过程与用户身份认证的过程都公开透明，易于监管。认证节点为用户节点颁发公私钥时，BA-IBS子系统使用了与BA-PKI子系统中相同的UTXO关联技术，将认证节点为用户节点颁发公私钥对的全过程相互关联地记录在区块链中。

优点3

（3）基于区块链技术实现了BA系统中的认证节点（KGC）去中心化，采用多个（KGC）进行认证，降低了单点安全风险。

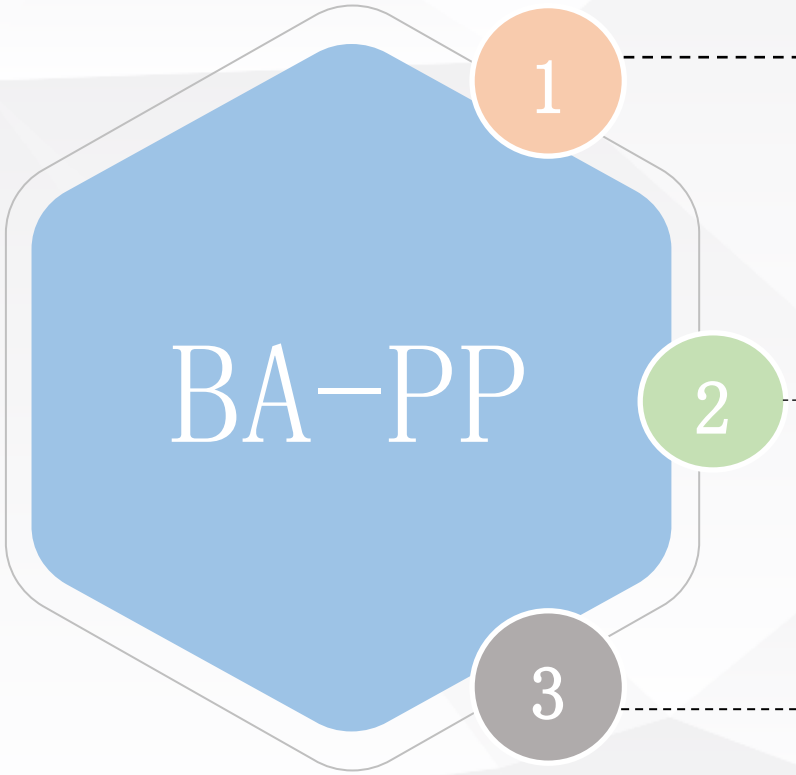
目的

解决数字货币体系中大量普通用户的身份认证需求

银行或其它被央行授权的金融机构能够作为认证节点（KGC），为普通用户提供身份担保，担保方式为由认证节点向普通用户颁发公私钥对。普通用户能够作为用户节点进行身份认证以证明自身身份，身份认证的方式为使用认证节点颁发的私钥进行数字签名

BA-IBS

BA-PP隐私保护子系统



1 用户在丢失密钥时可通过向商业银行等认证节点提供有效身份信息（如安全问题答案等）更换密钥。

2 BA-PP子系统使用了零知识证明技术，使得能够在对用户隐私身份信息做认证的同时保障用户隐私身份信息不暴露在网络中，实现了用户信息的隐匿性

3 实现过程，包括密钥颁发及设置身份信息和验证身份信息撤销密钥证书

技术实现与实验测试

表1. BA系统已实现的功能列表

组件名称	基本功能点
BA-PKI子系统	银行节点申请证书
	CA节点颁发证书
	CA节点吊销证书
	任意节点查询证书及操作记录
BA-IBS子系统	普通节点申请密钥对
	KGC节点颁发密钥对
	用户进行身份认证
	KGC节点撤销密钥对
	用户查询密钥对
BA-PP子系统（主要为零知识证明模块）	keypair参数生成
	证明的生成
	证明的验证

表2. BA系统事务处理性能测试结果

事务数量（条）	平均区块产生时间（s）	平均区块包含事务数量（条）	耗时（s）	TPS均值（条/s）	本地数据库体积增长（MB）
100	5.0	100	5	20	0.34
300	5.0	300	5	60	1.11
1000	5.5	500	11	91	3.74
3000	5.3	500	32	93	11.10
10000	5.6	500	112	89	34.76
30000	5.7	491	352	85	102.24
100000	5.6	490	1142	87	331.05

BA系统坚持选择成熟、稳定、先进的技术。整个测试过程中BA系统表现出良好的可靠性、吞吐率、扩展性。

技术实现与实验测试

表3. 单节点区块链信息查询性能

场景名称	并发数	最小响应时间	平均响应时间	最大响应时间	90%响应时间	TPS	CPU消耗
节点查询证书及操作记录	20	0.036	0.036	0.061	0.081	320	60%
	50	0.032	0.032	0.136	0.159	360	65%
	100	0.035	0.035	0.148	0.299	363	70%
用户查询密钥对	20	0.032	0.032	0.060	0.080	328	60%
	50	0.035	0.035	0.135	0.162	362	70%
	100	0.032	0.032	0.211	0.304	368	72%

表4. 密码学模块-IBS无证书签名验签性能

操作名称	参数大小（byte）	耗时（ms）
KGC参数生成	生成s: 20, P: 128, P0: 128	6.26
KGC生成部分密钥	生成Da: 128	7.86
用户生成完整密钥	生成XA: 128, YA: 128, pri: 128	8.47
IBS签名	传入msg: 26	7.13
IBS验签	传入msg: 26	9.20

表5. 零知识证明模块耗时典型数据

操作名称	参数大小 (byte)	耗时 (s)
零知识证明keypair参数生成	生成vk: 522, pk: 10791216	7.78
零知识证明proof生成	生成proof: 312	8.78
零知识证明proof验证	传入proof: 312	0.0343

BA系统坚持选择成熟、稳定、先进的技术。整个测试过程中BA系统表现出良好的可靠性、吞吐率、扩展性。

（注：以上分享的是2017/12/15结项时的数据，目前又有大幅提升）

业务应用场景-发行过程中商业银行的认证

金融体系管理（证书查询和更新）

证书查询功能主要包括两种形式。一是央行主动查询商业银行的证书，二是商业银行向央行申请并查询证书状态。

银行间的同业拆借（签名验签）

基于区块链的PKI发行体系，允许将商业银行之间的资金融通写入区块链中，每笔事务都会做签名验签，结合实体货币向数字货币的转化，可以确保同业拆借的安全、便捷。

数字货币发行端的证书颁发

在数字货币首次发行过程中，商业银行向央行发起证书颁发申请并提交相关材料，央行核实商业银行身份后通过区块链向各商业银行颁发CA证书。

金融风险管控（证书撤销）

央行是根证书的持有者，证书的撤销可以用于金融风险的控制，证书的撤销也分为央行主动撤销和商业银行申请撤销两种形式。

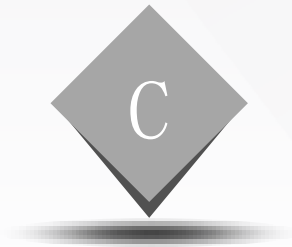
业务应用场景-数字货币流通过程中的应用

数字货币钱包的认证

身份认证节点线下对用户身份进行核实，核实通过后认证节点基于用户ID生成部分私钥并返回给用户，用户添加秘密值计算生成自己的公私钥，并将公钥公开，用户借助其私钥证明其网络中的身份。

数字货币钱包找回

当私钥丢失后，用户需要向认证节点再次申请公私钥，可以在不提供用户隐私信息细节的前提下，出示用户本人拥有隐私信息的的零知识证明，达到身份核验并且重置公私钥的目的。



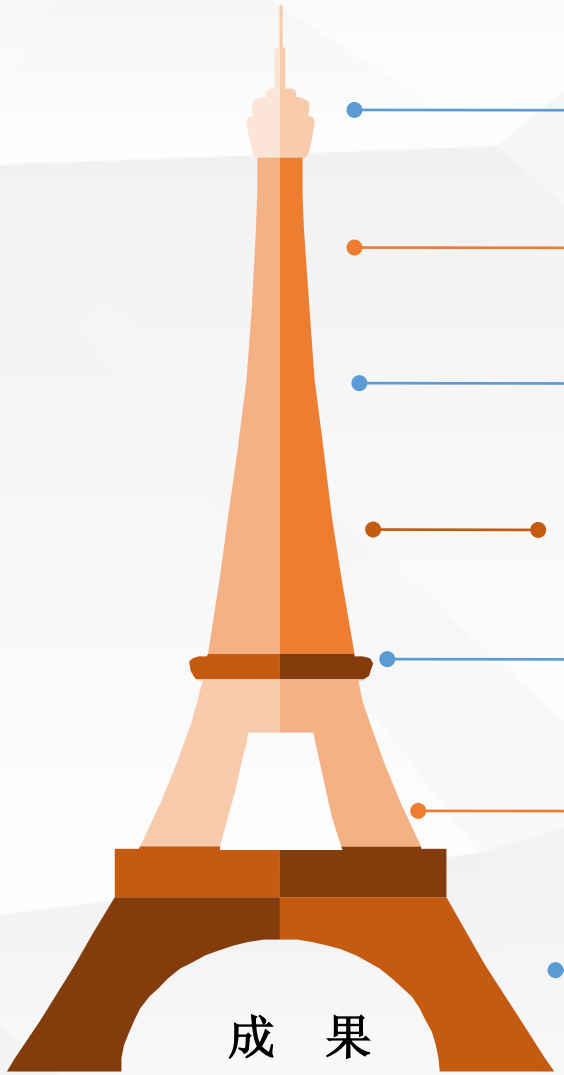
交易明细及余额查询

在进行交易明细和余额查询过程中，用户先发起查询申请通过签名验证，证明自己对私钥的所有权，进而授权查询该私钥对应钱包的交易流水和余额。

智能交易与智能合约

如证券的自动化支付，通过一段智能合约启动一个智能化支付，在特定时候向债券投资人支付利息或本金，避免手工操作和债券发行人的违约行为。

阶段性成果展示



1、基于区块链的CA认证管理方法、装置及系统

2、UTXO查询方法及装置

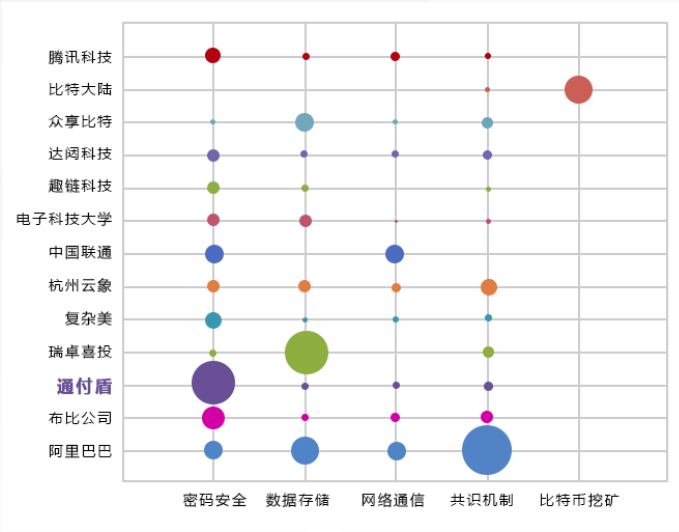
3、基于区块链的信息验证方法及装置

4、一种基于智能合约的认证权限评价方法及装置

5、区块链中区块共识建立方法及系统

6、基于公有区块链的认证记录审查方法及装置

7、简单支付验证节点交易查询方法及系统



成果形式：专利

作者：江苏通付盾科技有限公司

通付盾身份链：key-chain

通付盾 Pay Egis

愿景： 打造数字经济时代的身份安全基础设施

基于智能合约打造身份网络，实现共识参与者的身份安全

创建智能合约极速通道，提高智能合约的性能，并实现合约交互的信息安全

只支持身份认证类DAPP运行于KeyChain上

■ 官 网： kc.tongfudun.com

我们是谁？

通付盾 Pay Egis

2011-2016

2016-2021

2021+

通付盾 - 以数字身份为核心的智能网络解决方案和数据运营提供商

通付盾®
Pay Egis

客服电话：400-831-8116
官方网址：www.tongfudun.com
商务合作：info@tongfudun.com
售后服务：service@tongfudun.com

北 京 · 上 海 · 广 州 · 苏 州 · 成 都