数字身份，证书和物联网
大网区块链

崔建军博士 和 Wolfgang Blumental

cui@inasset.de

微信：cui8161188

摘要

大网区块链提供了一种自我为中心身份解决方案，以推动第四次工业革命和物联网，为人，机器，算法和其他非人类实体带来安全的身份（“数字双胞胎”）。 作为智能解决方案，它可以提供信息而无需透露详细信息。身份也必须是私密的和安全的。

大网区块链自我为中心身份是一种自我主权身份解决方案，该身份由政府授权或第三方发布，然后转移给用户，由用户自我管理。

您无需登录微信，Facebook 等，而是自我为中心登录。并具有租赁酒店房间，使用社交媒体或叫车的功能。

大网区块链具有近实时确认，每秒百万交易，无许可和自我为中心公共区块链。

目录

数字身份

数字身份是纸质身份的数字形式。

身份解决方案包括个人和组织内用于识别，认证和授权某人访问该组织或其他关联组织中的服务或系统的过程和技术。数字身份是对纸质身份的替代，包括例如出生证明，身份证，护照或驾驶执照。数字身份需要随时随地可移植且可验证，也必须是私密的和安全的。

当前身份系统的问题：

政府：部门与政府之间缺乏互操作性。增加流程的时间和成本。

医疗保健：医疗保健领域（医院，诊所，保险公司，医生，药房等）的参与者之间缺乏互操作性，导致医疗保健效率低下，患者护理延误和沮丧。

教育：据估计，仅在美国，每年就售出二十万份假学术证书。难以验证这些凭证的真实性会导致雇用不合格的专业人员，对大学和雇用公司造成品牌损害。

银行业务：对登录详细信息（例如密码）的需求降低了用户银行业务的安全性。

一般业务：需要存储客户和员工的个人数据是公司的责任之一。

违反 GDPR 的行为（例如英国航空公司的案子），或者仅仅是由于客户信任损失和对组织品牌的间接损害，可能会导致个人数据泄露，从而处以巨额罚款。

大网区块链

大网 (大网)是新一代的区块链。大网 (大网)通过集成家谱与马尔可夫链蒙特卡洛(MCMC）扩展了区块链技术。因此，BITCOIN 和以太坊在大网 (大网)中是特例。

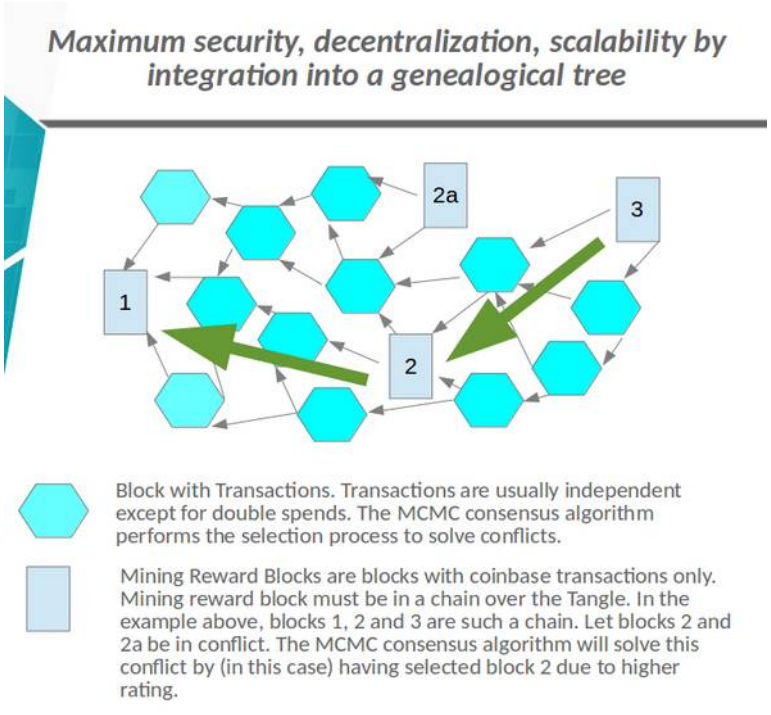
通过使用大数据技术及其可并行化架构，大网是传统区块链的后续产品，可以满足具有重要经济意义的关键应用。

大网 (大网)是一个去中心化的加密货币，支付，交易，供应链和电子商务平台，具有以下优势：

- 近实时确认，分布式工作证明,
- 无限的可扩展性,
- 去中心化交易所，
- 去中心化供应链和电子商务
- 智能合约,
- 易于使用,
- 免费, 无许可，无信任，
- 量子安全。

大网是客户端和服务器体系结构。与任何基于工作证明 PoW 的系统相比，大网 所需的功耗与比特币相同。

但是，通过比较每秒交易量（TPS），例如比特币中的 10 TPS 或以太坊中的 200 TPS，大网 (大网)在集群中具有 10 个服务器节点可以在相同的功耗下达到 100 万 TPS。大数据和区块链并行化是以可承受的成本获得大量 TPS 的唯一解决方案。



政府作为身份颁发者

1.政府在大网区块链中创建一个域，例如 id.gov
2.政府为身份证创建通证，通证名称必须是用户的公钥。 数据将用政府的公钥保存为通证的加密数据。
3.政府将通证转移到用户帐户，并使用用户公共密钥对身份数据进行加密。
4.政府可以撤销通证，应用程序可以验证数字身份。
5.用户可以为新的公钥请求新的数字身份。

服务提供商的用例

1.创建一个域 id.idnow.de
2.检查纸质身份证，然后为身份证创建通证，通证名称应为用户的公钥。 数据将保存为使用公钥加密的数据。
3.将通证传输到用户帐户，使用用户公共密钥加密数据。
4.可以撤销通证，应用程序可以验证数字标识。
5.用户可以为新的公钥请求新的数字身份。

创建域名

大网区块链具有类似于互联网域名的分布式域名服务。 系统可创建顶级域名 gov，com 等。顶级域名的所有者可以创建具有多重签名的子域名。 域名是唯一的，并受多重签名保护。所有通证都属于一个域名。

打开创建审核机构并发布

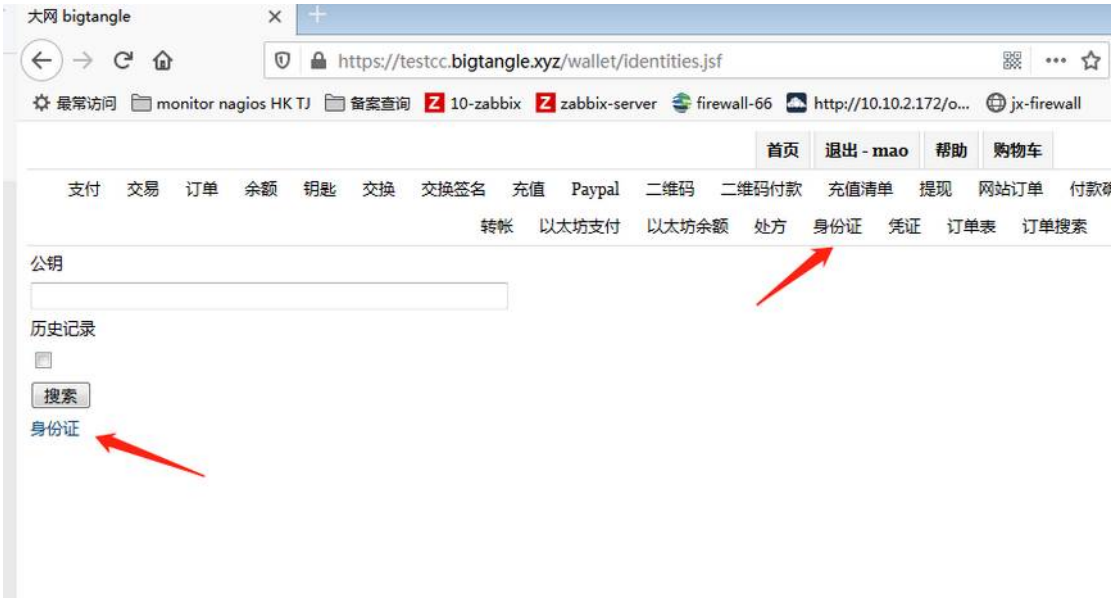

通证签名 转帐 以太坊支付 以太坊余额 处方 身份证 凭证
通证名称
身份审核
通证
02a7bc4142fd131310839218ce492377b659dcf15d5c07724d1d8a433d4a61a1a1
公钥地址
1D5MymgyrtE1z8VaDpYD2bUmLydRt64ncU
数量
1
域名
com
描述
身份审核
发布


支付 交易 订单 余额 钥匙 交换 交换签名 充值 Paypal 二维码 二维码付款 充值清单 提现 网站订单 付款确认 产品 媒体 商店 银行 位置信息 被邀请人查询
通证签名 转帐 以太坊支付 以太坊余额 处方 身份证 凭证 订单表 订单搜索 通证搜索 公共查询 区块
用户组名称
搜索
编号 用户组名称 群体类型
20191112010000007 sell 商店 02bd4202c7ba28471f81b0663ffd2512faf73f782855a19ff1bc7f7038116dca9a 修改添加用户 发布
20191218010000001 蔬菜店 商店 0303cf18783fdf7ea9b794ed79af4838773d011f3c6eb89890884d518d8605887b 修改添加用户 发布
20200304010000001 店 商店 02bc8f09cc7e86cb5d9908e6a5be4cbab27ac5da99c6fc5743d610f8a669a6f677 修改添加用户 发布
20200416010000001 prescription a8b77fdd-4193-4fa1-9cc8-b541d8cb631f 商店 0280f493d556f3febb125f65ab5fe52c236f2ac54d39e6ce7319bc6e54a9150c6b 修改添加用户 发布
20200418010000001 health authority germany a8b77fdd-4193-4fa1-9cc8-b541d8cb631f 商店 0373a50841e4addee5c45e361955bdc73ffd47e902609d4176b2587e3be2a4d412 修改添加用户 发布
20200509010000002 土豆店 商店 0202ba223dbc2196092d9e8f90be0ec6715c295eae27c6e2069ccd3397df3cae1f 修改添加用户 发布
20200513010000001 处方审核 商店 03bd9392c96b183a5253230cd5f32f1b991f00ddcc20493211b0b473cd55749bb1 修改添加用户 发布
20200515010000001 身份审核 商店 03c50d78d6b9a6ae903abd8b2216510c5fcab7ab3665431d142c5c4fe2f19e6899 修改添加用户 发布
20200515010000004 房产证明所审核 商店 03e1caaf7b49588fe50a3179a732f096f6c40ae3973f7fbc711708e155df1ebcca 修改添加用户 发布
全选 删除
新建

创建数字身份证

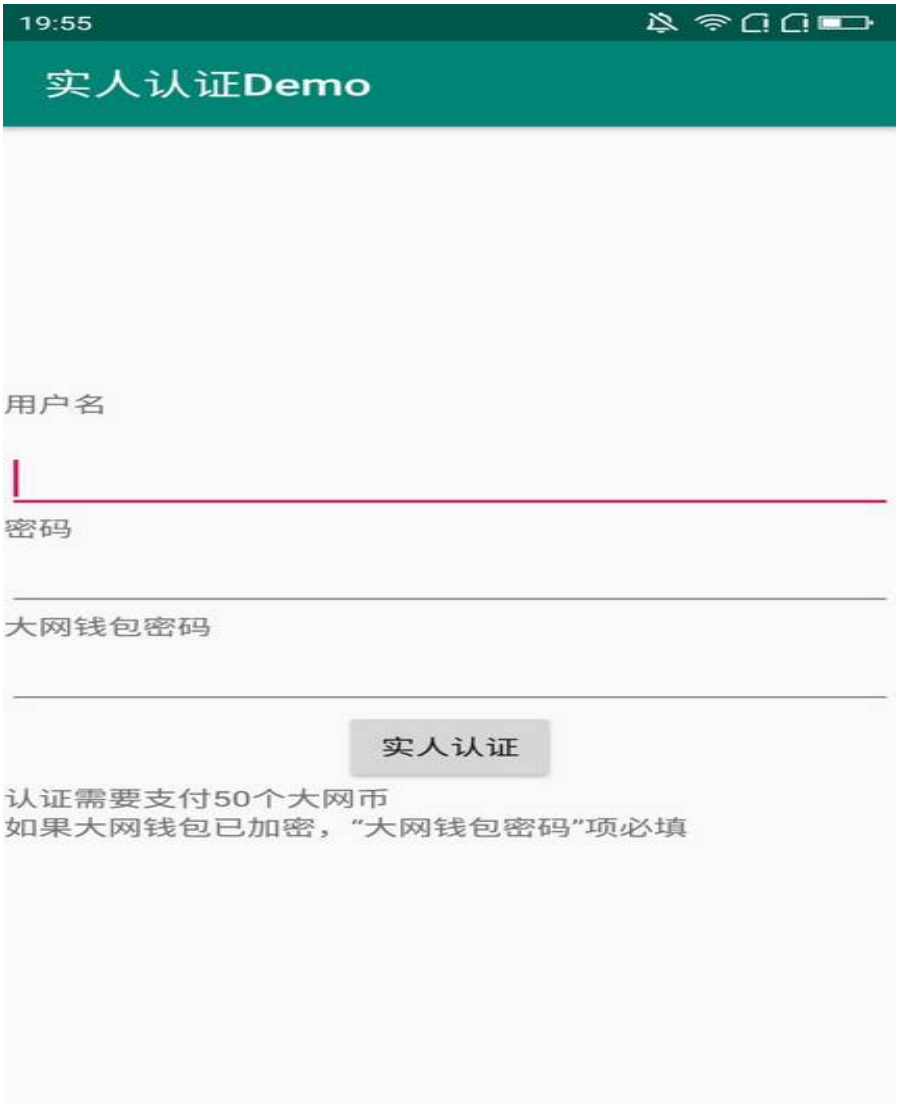
身份将由域所有者组创建。 身份是在给定的公钥上颁发的，并且仅对此公钥有效。 身份数据由用户公共密钥加密，并具有颁发者的签名以验证身份。 除到期日期外，所有身份数据均已加密。将数字身份证转移给用户。
身份通证可以通过加密转移到用户的公共密钥地址。 可以使用公共余额检查此地址是否具有全名为 publickey@id.gov 的通证。

数字身份证流程



添加公钥接收人并发布

从 https://bigtangle.oss-cn-beijing.aliyuncs.com/app/identity_verify.apk 下载实人认证 APP，并安装后运行该实人认证 APP。



输入用户名、密码及大网钱包的密码（如果已加密钱包）后，点击“实人认证”按钮开始进入实人认证流程。


19:57
实人认证
欢迎体验实人认证!
本过程需要 您本人 亲自完成，仅需要1分钟！
您提交的资料将只会用于实人认证审核。
开始认证

点击“同意”按钮后，进入人脸认证和身份证照片上传操作页面。

张下嘴


21:57
确认证件
人脸验证
确认证件
请拍摄以下证件照片，注意避免证件反光：
身份证人像面
身份证国徽面
示例
姓名 吴潭
性别 男 民族 汉
出生 1992 年 12 月 1 日
住址 浙江省泉山县龙港镇宫后路535号
公民身份号码 327323199212010208
示例
中华人民共和
居民身份证
签发机关 泉山县公安局
有效期限 2009.08.17-2019.08.17
立即拍照


21:58
实人认证
认证成功
感谢您的信任与支持
返 回

点击“返回”按钮完成签名。

无密码验认证服务

大网区块链钱包支持身份验证服务标准 FIDO2。 这将启用无密码验证服务。

FIDO2 的核心是身份验证标准和 FIDO 客户端身份验证器协议。客户端到身份验证器协议使一致的密码身份验证器可以与客户端进行互操作。

使用大网区块链 应用程序为应用程序创建单一签名服务。

这些应用程序使用公共密钥向服务器发送请求，并获取由应用程序的公共密钥签名的安全访问通证。 钱包可以解密安全访问通证并签名安全访问通证，然后将已签名的消息作为请求中的标头发送到服务器。 如果验证过程成功，则服务器将验证安全访问通证并可以创建会话。

对于身份验证服务，计算机使用多重签名将签名的安全访问通证传输到大网区块链区块链，用户获得签名的通证并将其解密以在计算机上登录。 可以将大网区块链钱包安装在设备上以进行本地和直接身份验证。