比特元区块链项目白皮书

一．概述

1.区块链是一种几乎不可能被更改的分布式数据库，大量计算机节点维护同一个区块链，通过复杂的校验机制，区块链数据能够保持连续性和一致性，即使部分计算机作假也无法改变区块链的完整性。在私钥签名交易内容和公钥验证交易内容正确后，加密数字货币可以准确无误地在对应的帐户地址间转移。

比特币带来的区块链技术已经开始让我们能够从信息互联网向价值互联网升级，不可信的互联网升级为可信的区块链，不但会影响整个金融业，也会影响几乎所有的行业，甚至联系到每个人的吃穿住行。

2.比特元区块链开发项目：比特元开发团队致力于区块链技术的开发应用，如：安全高效的清算支付系统（代币的支付或消费）、P2P 交易所（股权、期货、外汇、票据债权资产、大宗商品）、供应链物流、个人或机构身份认证、证据保留(公证、商标、专利、合同等)、智能合约的自动执行等。

二. 比特元钱包技术概述

从中本聪发布白皮书到现在已经有 7 年的时间了，比特币的很多问题已经被发现，并且出现了不少好的解决方法，只是因为比特币的升级必须获得大多数比特币用户的同意，比特币很难有统一的意见，因而可能会失去快速发展的机会。比特元开发团队长期研究云技术和高并发低延时交易所技术，区块链技术研究也有两年多，并进行了大量的实际测试和应用，有些应用只要整合已有的技术马上就可以进入实施阶段。

分布式系统的共识机制问题，已经研究了至少 40 年，并且出现了好几位图灵奖。分布式系统共识机制的第一次工业化应用是 google 的 Chubby 系统，也就是著名的 paxos。但是，paxos 共识并不是非常适合比特币这类系统。

比特币这类系统的特点是，会存在恶意节点，故意破坏共识，这样的共识叫做拜占庭共识。比特币采用一种独辟蹊径的方法解决了这个问题，就是通过工作量证明 POW 的方法，比特币每个有算力的节点都是独立计算挖矿并提交自己的区块，最先被其他节点认可的计算机可以成功打包获得奖励。但是从第一个新区块挖出广播到被全网确认前会有很多其他的计算机提交新的区块，后面那些无效区块的传播会浪费网络和计算机的资源，并会产生负面作用，现在比特币的挖矿间隔是 10 分钟，不能太短。

目前比特币交易极限只能做到最高每秒 7 笔，比特币区块限制 1 兆据说是为了保障矿工的利益和确保弱小的计算机也能挖矿，相对于支付宝每秒 4 万笔的峰值来说几乎没有可比性，当然比特币诞生的时候无法预料到今天中国的网络支付量已经是其当年设计时的上万倍。

要符合中国的国情和用户体验，10 万/秒笔交易性能是需要的，确认时间要几乎实时，如果 10 秒一个区块，每笔交易的大小为 200 个字节，每个区块的大小为 200 兆，每天约产生 1.5T 的数据，每年可以产生至少 500T 的数据，对这 500T 数据进行校验、分析，本身就不是一个单机钱包所能满足的。

随着云技术的发展，大部分技术已经开源，我们基于现有的技术已经能够将区块链的大部分数据存储到云上。

如果区块的大小超过 200 兆，这样大的区块要在网络中快速广播也是不容易的，比特元结合目前的先进技术，经过优化可以达到每秒一个区块的级别，对外广播的每个区块的最大容量减少到 20 兆，区块链挖矿打包就很容易达成共识，系统性能就能获得大幅度提升。

目前，已经有些数字货币可以实现在区块链上进行编程，我们研究了这些系统，认为可以借鉴部分的功能，但是，在区块链上运行虚拟机会产生很多安全问题，并且会影响性能。我们会尽量在区块链上内置一些功能，比如：交易配对、发行子币、股权管理、快递跟踪，这些功能不需要通过虚拟机来实现。而虚拟机则可用来实现一些不太常见的个性化功能。

经过优化的比特元钱包配对交易可达每秒交易 15 万笔以上，并且是可编程的分布式数据库，数据库中的数据是无法更改的。

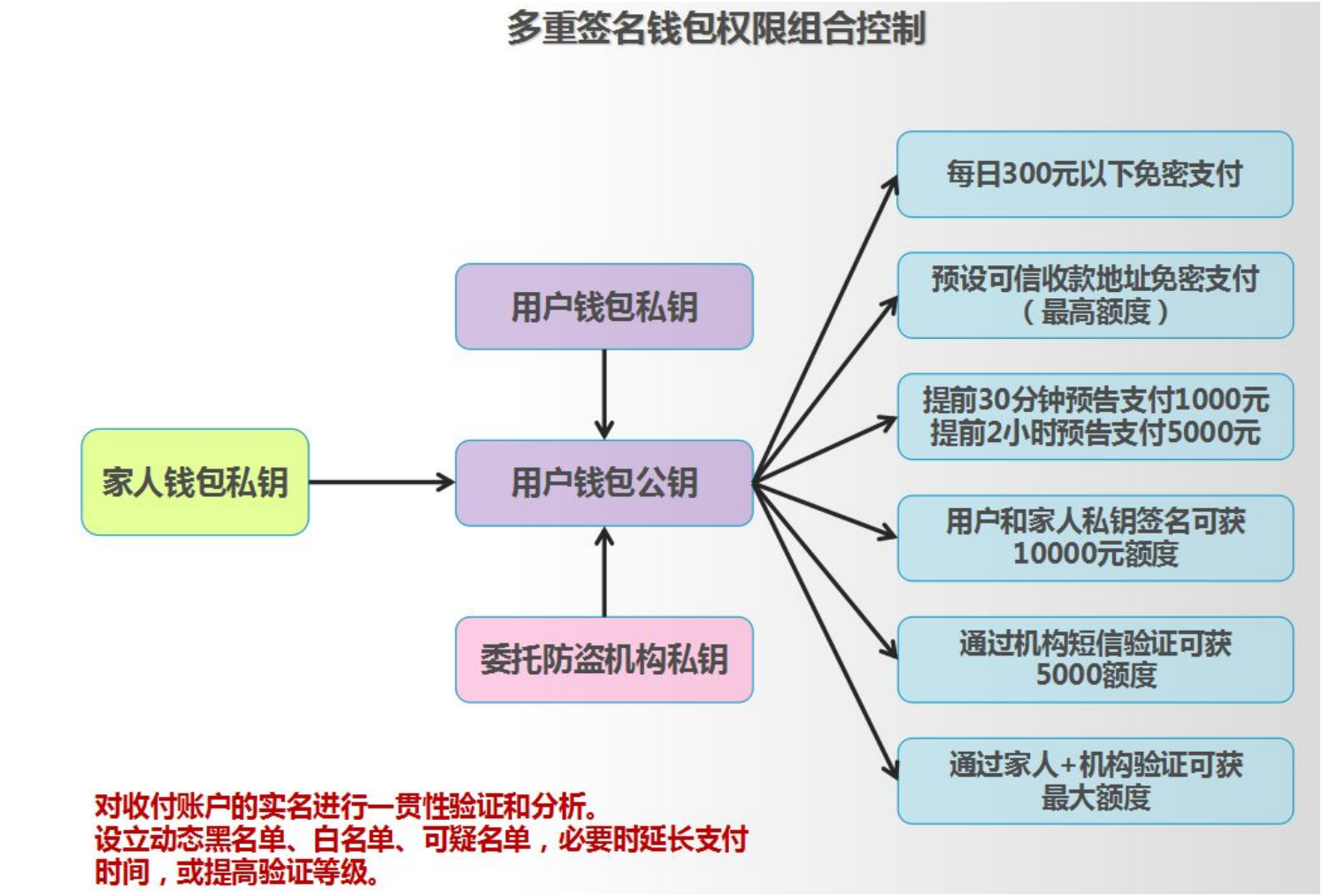
三．应用场景和先进性

（一）清算支付系统

1、分级多重签名

用多重签名的组合来控制钱包的支付权限，多重签名的一个私钥可由托管机构掌握，不同权限（大额或小额）的钱包地址都需要进行不同程度的身份认证，通过大数据或投诉举报系统可以建立黑名单或可疑名单，对可信白名单无需多重签名也可进行支付，如公交、地铁。

依据申请钱包的使用额度可以要求不同程度的身份验证，银行、非银行金融机构可面对面的对用户进行强身份验证，而通过视频语音则可以作为弱身份验证，公交、高铁、地铁、机场、高速公路收费站、商场收银台的付款时视频记录都可以作为连续身份验证。



2、提速扩容

由于中国人多交易量巨大，人人同步下载整个大钱包是不可能的，只能按投票来选举挖矿打包节点，选举打包节点（数十个或数百个）服务器必须保证一定的性能和带宽要求，各打包节点应确保在 1 秒内可以完成打包分发不少于 15 万笔交易的能力，其它节点同步节点（不需要太高的要求），不能打包，而普通用户只要手机下载区块链头部即可使用。

3、钱包找回

预设钱包找回功能，即使私钥丢失，也可以通过备用私钥（自己保存或者托管给信任的机构/人）找回自己的数字货币，同时用于找回的私钥添加了支付预告的限制，确保找回功能不会被他人冒用。

4、钱包防盗

预告支付功能可以在收到非本人的支付通知时，及时将数字货币转移到预定的安全地址；也可个性化定制支付额度，实现小额免密、大额预告的作用，兼顾了便捷性和安全性。

我们知道拥有私钥相当于拥有数字货币的控制权，所以私钥的保存方式，将影响到数字货币的安全。

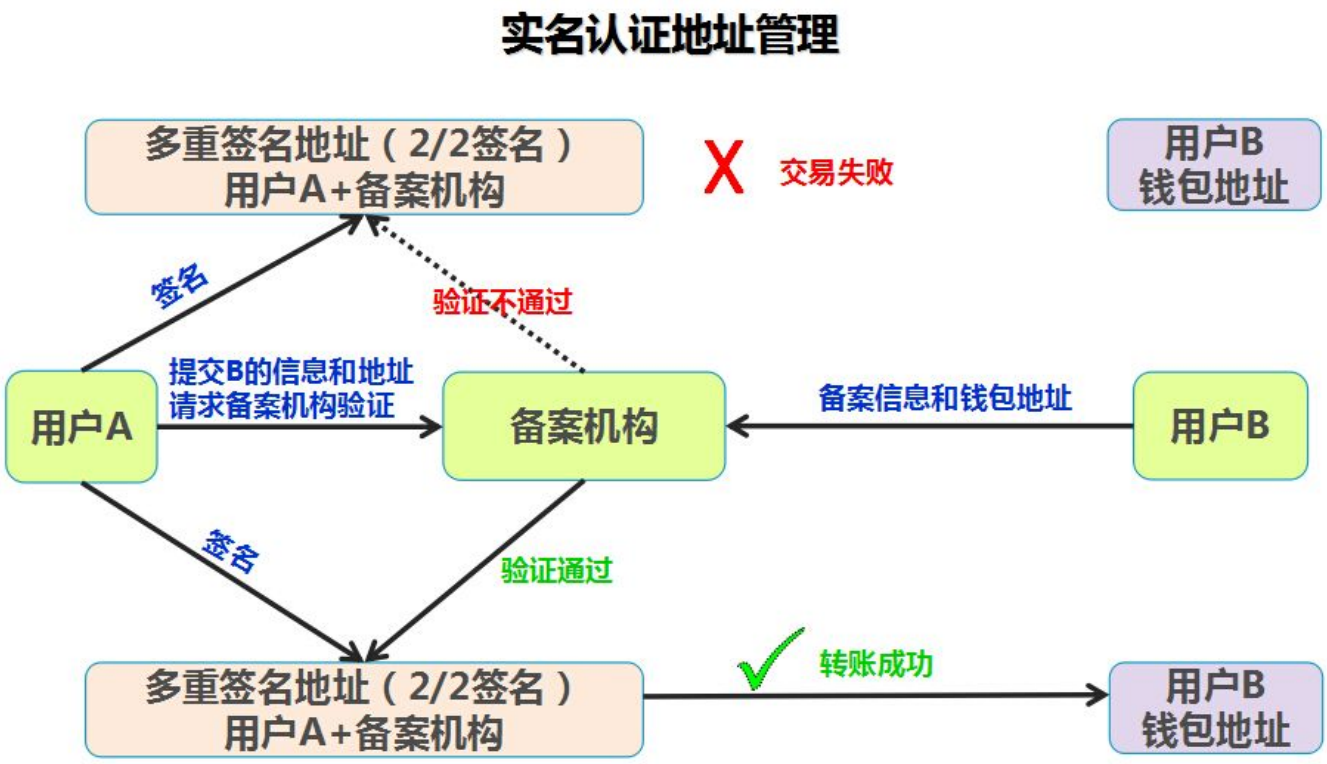
最简单的做法，私钥做为一个文件放在电脑或者手机上。这样的话，一旦电脑被入侵，那么你的币就可能被黑客偷走了。

最安全的做法：离线存储。离线存储就是用一台不上网的电脑或者手机，保存私钥，在线钱包负责创建交易，离线钱包负责关键的签名过程。离线电脑只需把签名结果告诉在线钱包，就可以进行交易。这个做法，虽然安全，但是不便捷，而且成本也比较高，要专门弄个电脑手机才行。

最佳的做法：U 盾或者金融 IC 卡。U 盾　或者　IC 卡可以认为是一个微型的计算机，外界无法从他们上面读取私钥，但是，可以方便的读取 IC 卡签名后的交易。

5、安全支付

对某些人来说，当需要向一个地址大额转账时，对安全性的需要可能远大于匿名性，这时候实名认证地址管理机制是有必要的，我们可以在转账前先确定对方地址是否属于我们要转账的人。

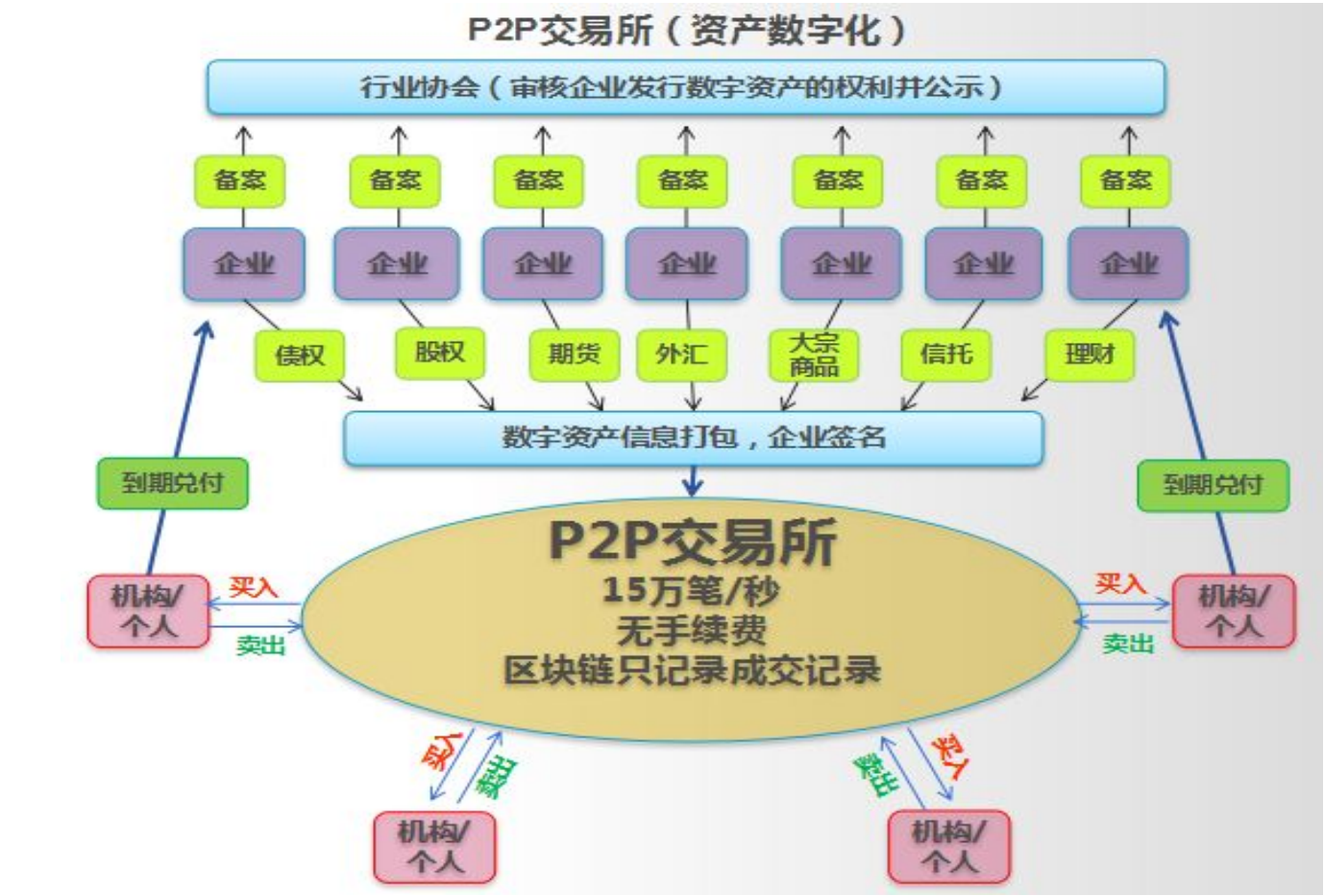


- **支付前，先验证目标钱包地址和所有人信息是否一致。**
- **备案机构收到用户签名后，验证目标地址是否实名登记。**

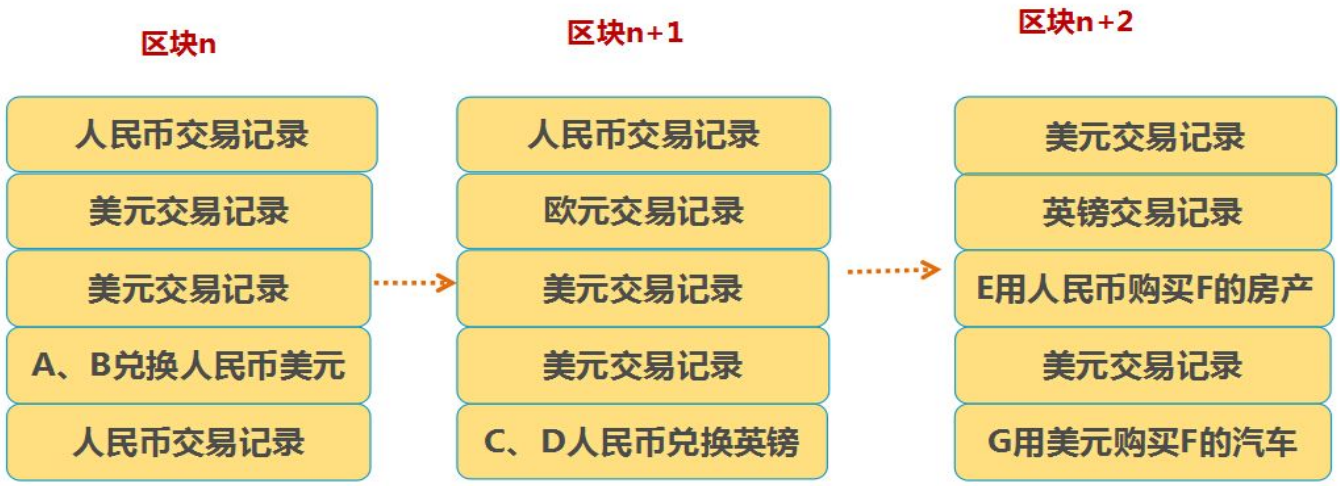
（二）P2P 交易所

1. 高速配对系统

P2P 交易所的挂单配对在内存中实现，每秒 15 万笔，交易历史数据可以保留在本地服务器硬盘，但不写入区块链，区块链只记录成交记录，成交时数字货币和数字资产同步互换，P2P 交易所不持有交易双方的数字货币或数字资产的。



多种数字资产混合P2P交易

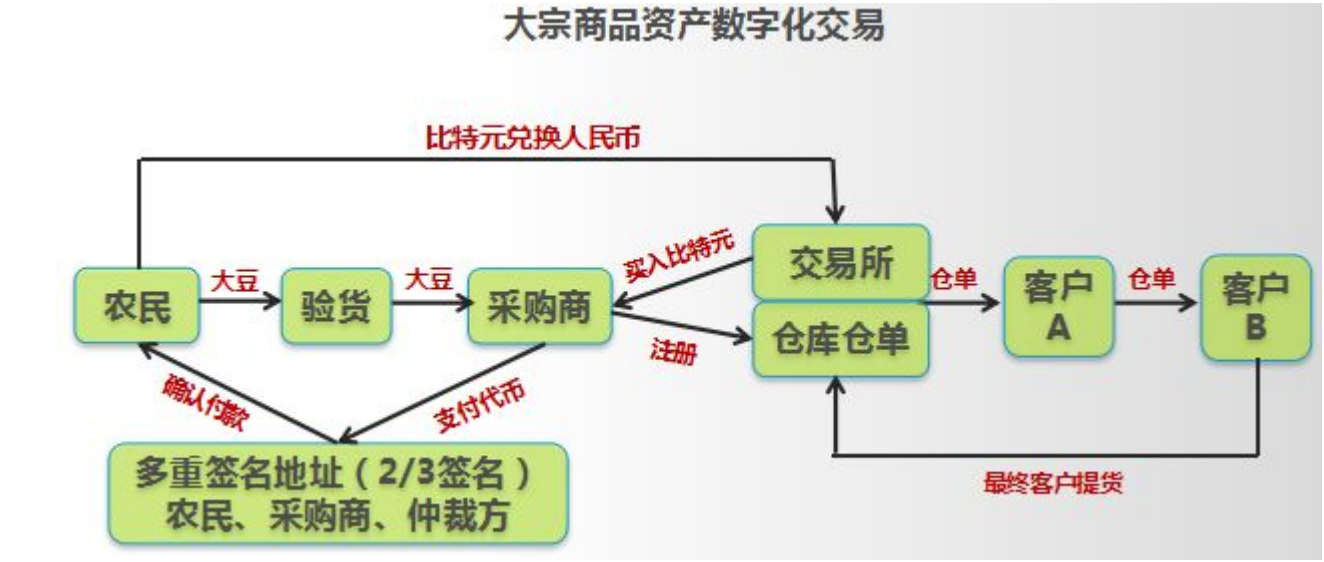


人民币地址A--->人民币地址B
美元地址B--->-美元地址A

交易所不持有用户的数字货币或资产，无风险

2. 资产数字化

在区块链上发行股权、期货、外汇、票据债权资产、大宗商品等数字资产的企业应具备相应的资质并予以公示，若有行业协会或组织的认可则更好。区块链将数字资产的发行、流通、权力人和兑付人都能够清楚的记录下来，不需要复杂的法律文书，也无法作假，有效的降低了交易成本，提高了资源配置效率。



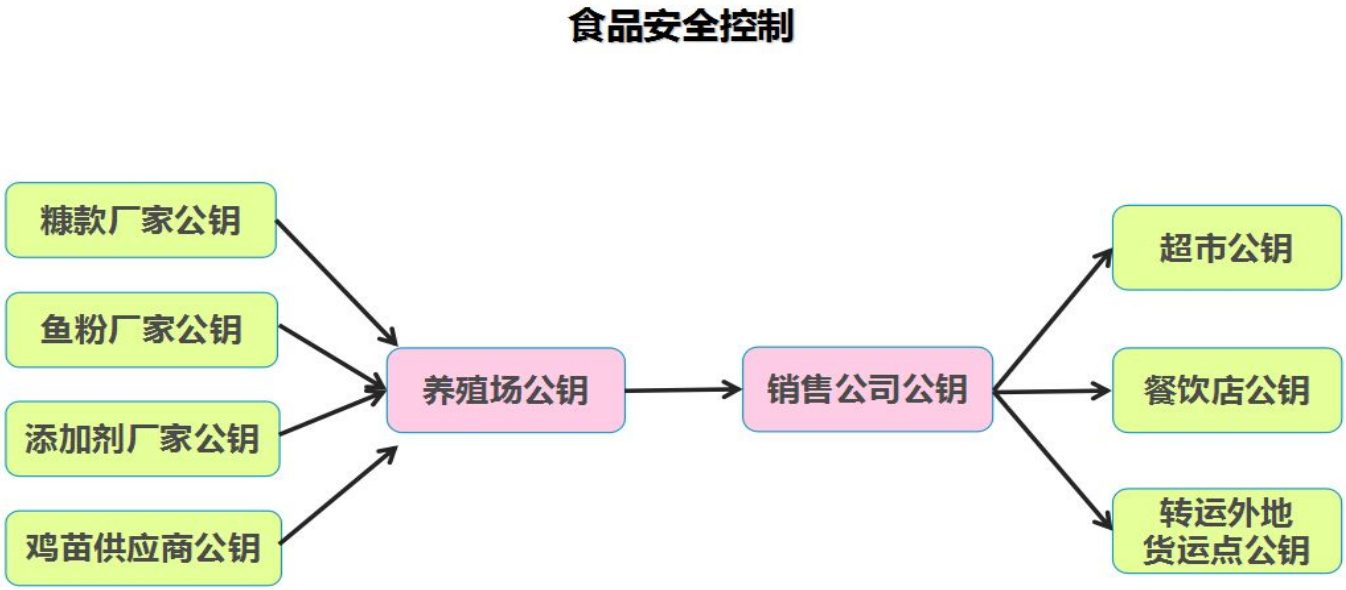
例如：交易所可以发行与人民币等价的代币，采购商购买代币后可向农民购买大豆，作为货款的代币可以打入 3 选 2 多重签名地址，农民、采购商、仲裁方只要有 2 个私钥就可以同意支付或退款，这里仲裁方是不能单独移动代币的，避免了挪用的风险。

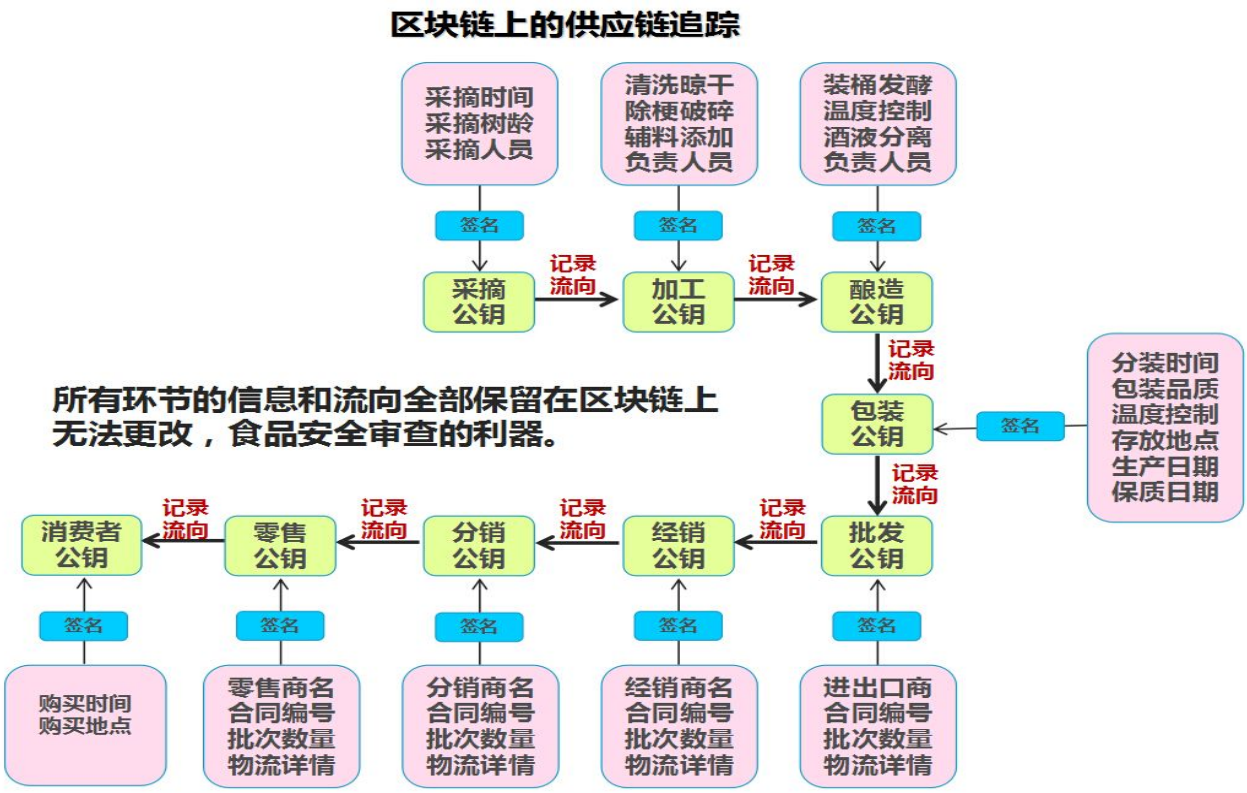
交易完成后农民收到代币可向交易所兑换成人民币。收购商将大豆检验后，交易所认可的仓库将其注册为标准仓单，并发放现货数字仓单，投机客和用户都可以用代币买卖数字仓单，也无须将货物反复运送，最终用户最后提货即可。

（三）行业管理应用

1、企业供应链追踪——记录原材料-加工-包装-销售的详细流程。

如一瓶红酒，查看区块链，可以知道是在哪个葡萄庄园、什么时候采摘的葡萄，用的是什么品质的种子，酿造存储的详细时间表，生产日期和保质期，经销代理零售的线路。饮食行业加入区块链技术，有助于食品安全的监督管理。



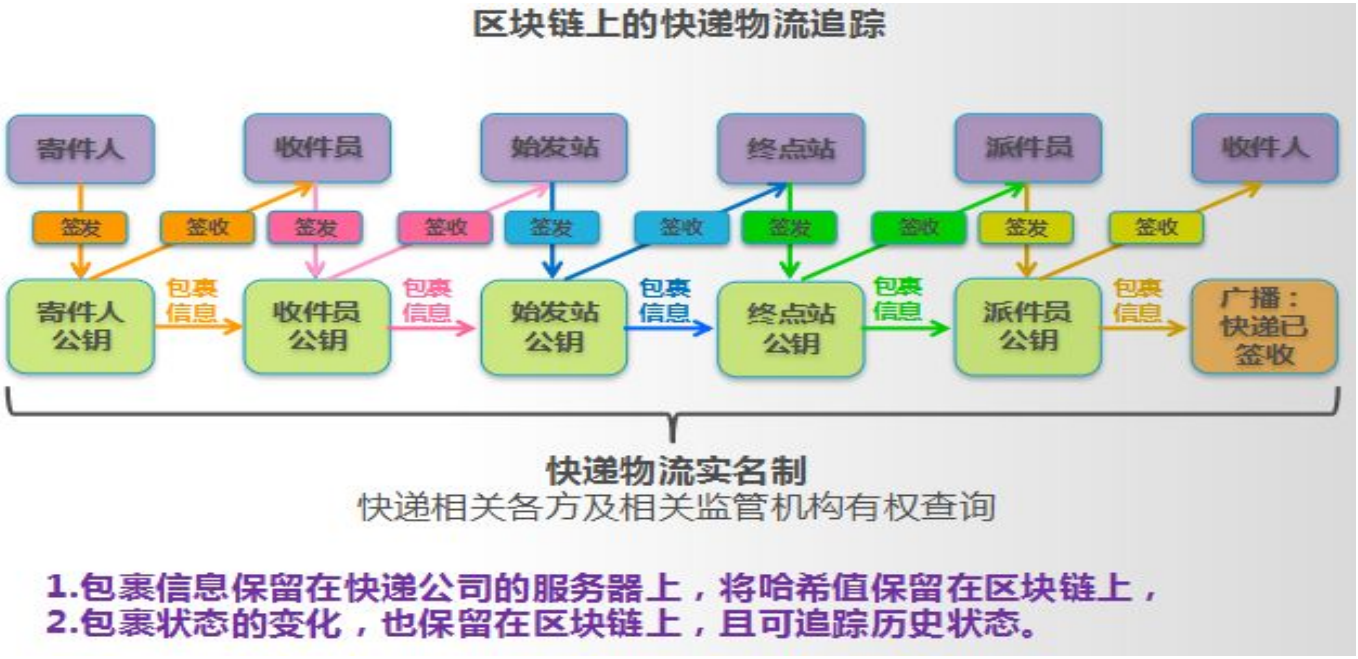


如一架战斗机，查看区块链，可以知道每个零件的原材料产地，生产厂家、采购记录，拼装记录，测试记录等。制造行业加入区块链技术，有助于提高产品的质量，维护消费者的利益。

如一座房子，查看区块链，可以知道材料是谁采购的，材料质量的标准，材料使用的实际数量等，建筑行业加入区块链技术，豆腐渣工程将无处遁形。

2. **物流追踪和交接确认**——记录货物从发送到接收过程中所有步骤。

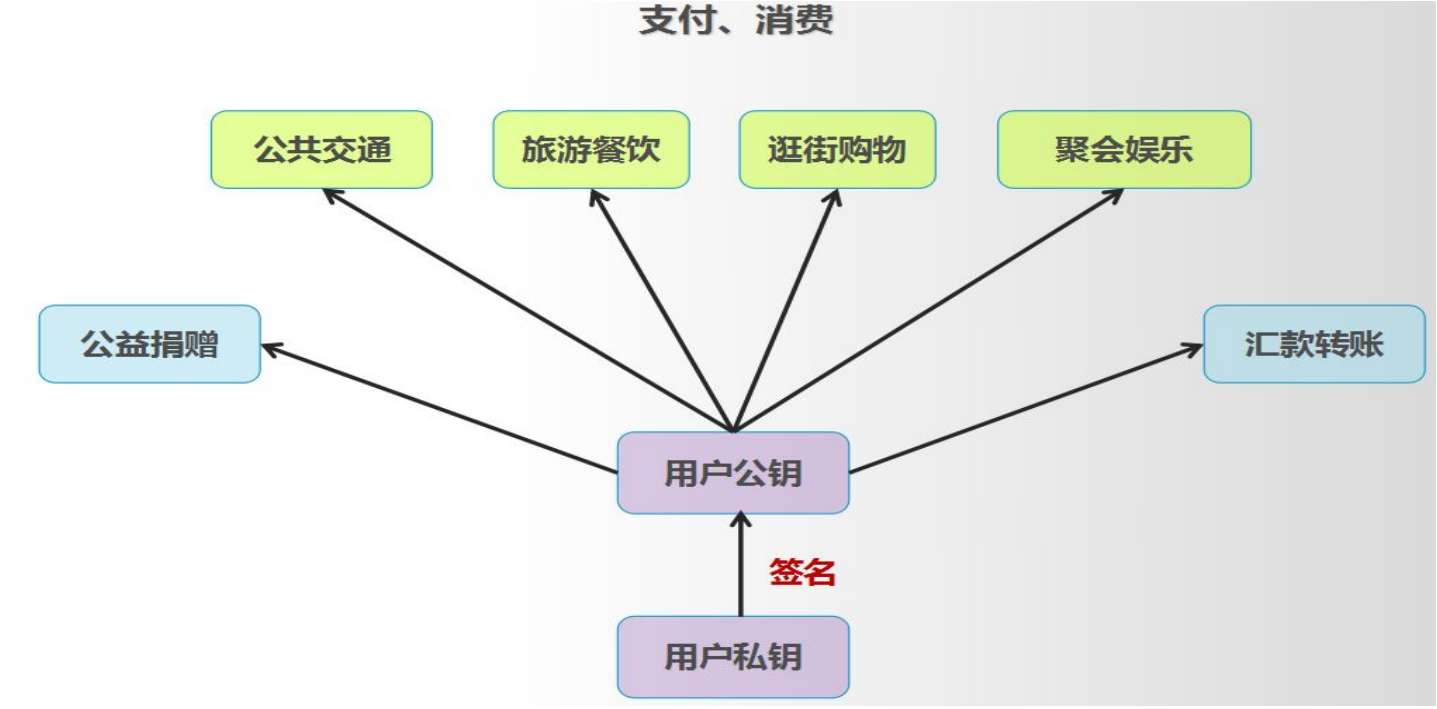
快递交接需要双方私钥签名，每个快递员或快递点都有自己的私钥，是否签收或交付只需要查下区块链即可，最终用户没有收到快递就没有签收，快递员无法伪造签名，杜绝快递员通过伪造签名来逃避考核，减少用户的投诉。



同时，企业也可以通过区块链掌握产品的物流方向，防止窜货或打假，保证线下各级经销商的利益。

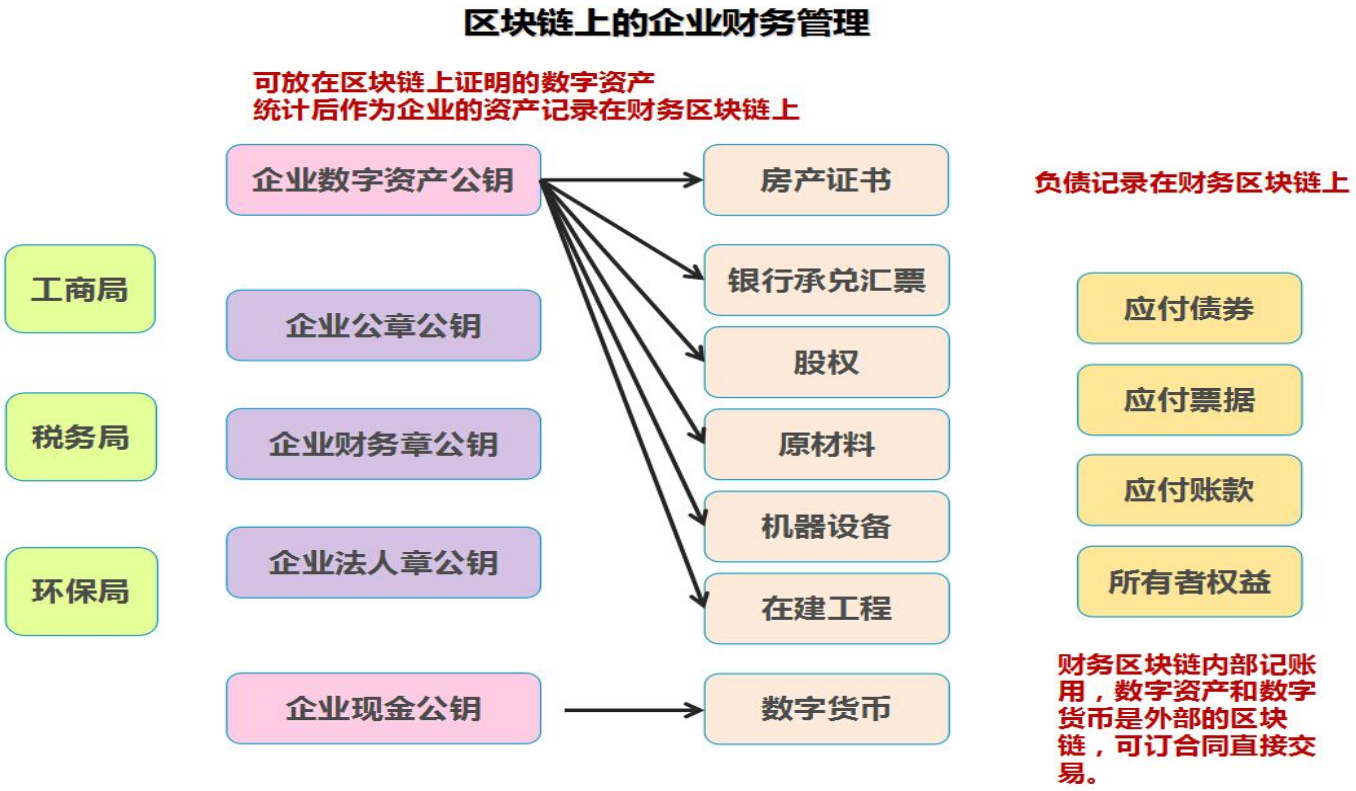
3. 用户可直接向厂家购物

有特色或品牌的商家，通过区块链来销售商品，可使厂家减少对中心化电子商务平台的依赖，可减少销售费用，提高利润。

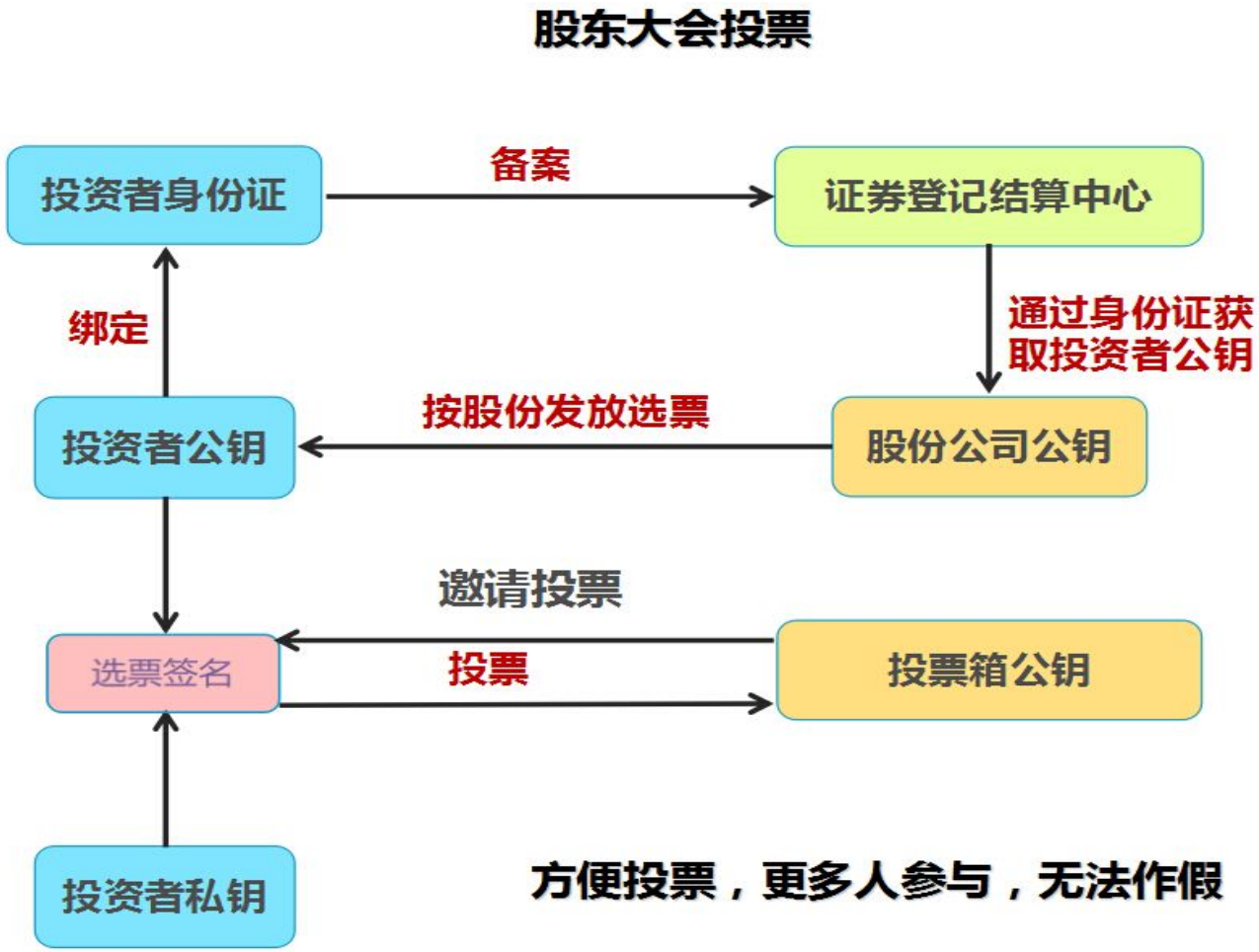


4. 企业财务记录功能

单位员工使用区块链钱包，无需填写发票去报销，只要有相应的统计接口即可直接把数据导入公司的财务系统中，企业私钥签名的合同和资金流水全部可以导入公司的财务系统中，财税部门通过区块链也可以实时掌握企业的状况，银行也可以查看企业发放贷款的流向，控制贷款的风险。

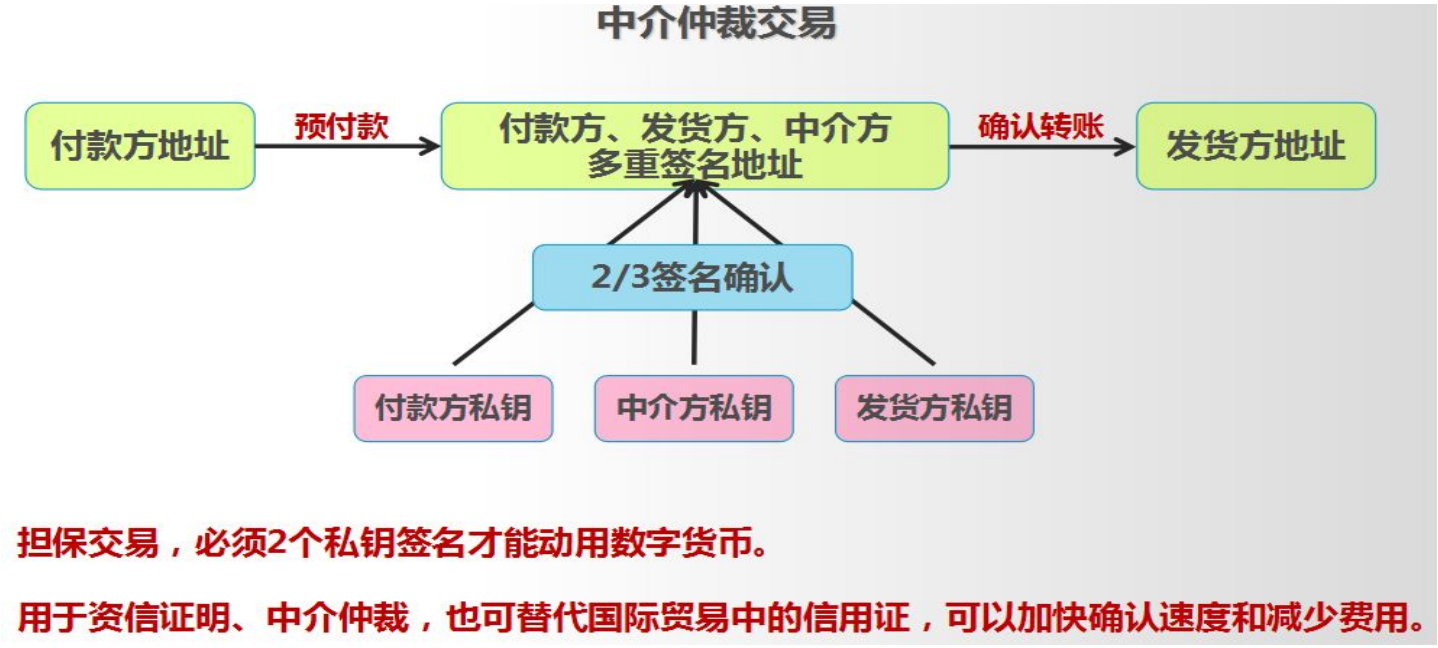


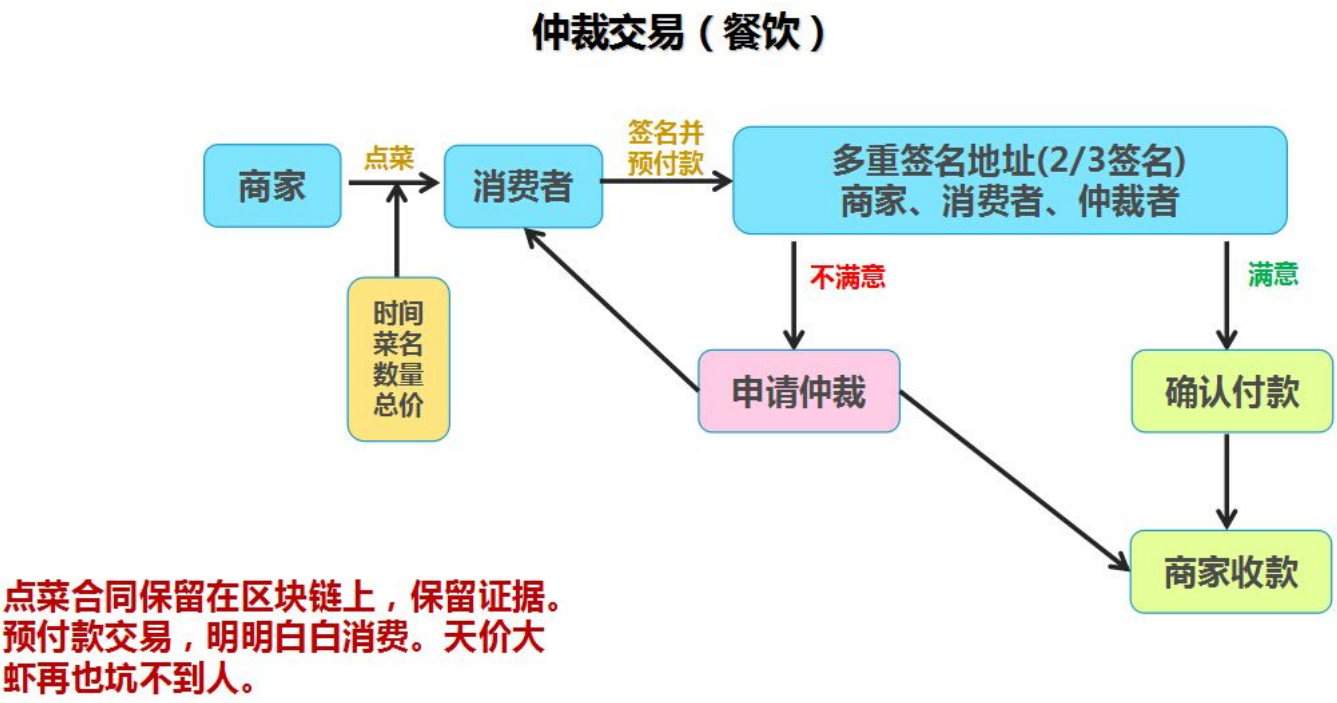
5、股东大会投票



（四）第三方担保交易

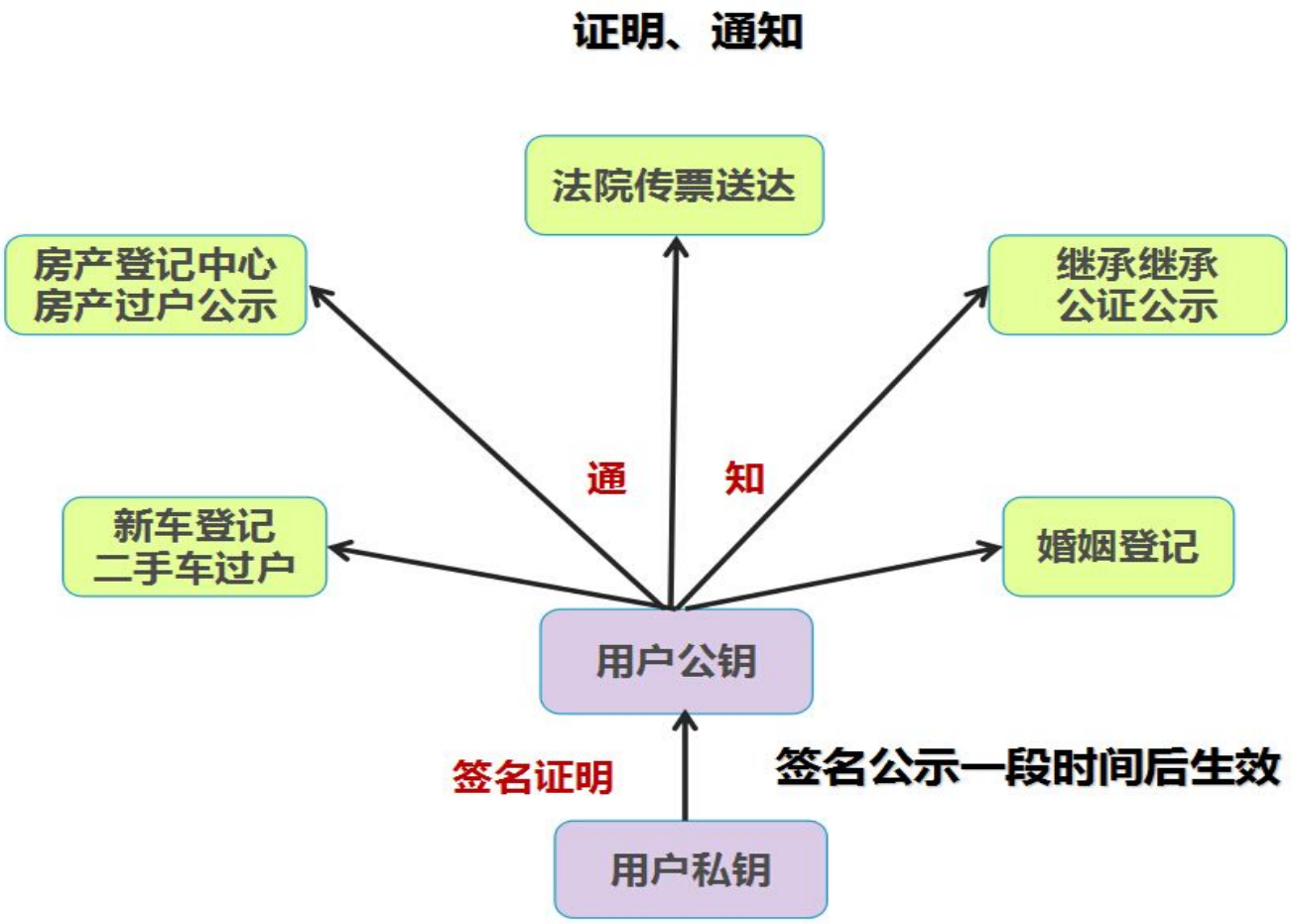
酒店预订、餐饮、网上购物、买车、购房可以事先确定交易内容，将数字货币打入三个私钥控制的地址中，第三方为大家信任的中介或仲裁者，若发生纠纷只要第三方仲裁就可以了，但是第三方是无法单独挪用数字货币的，从而避免了因持有用户资金所具有的风险。





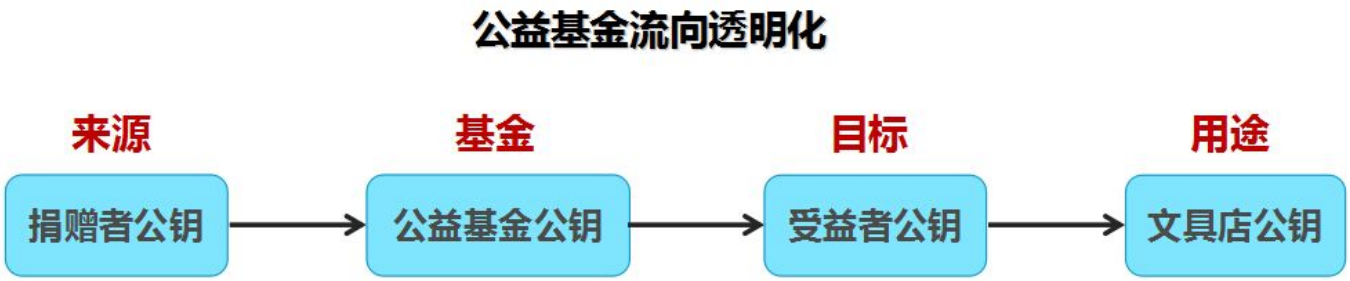
（五）社会公示和证据保全

1. 遗产分配、受益基金等可以通过区块链自动执行。



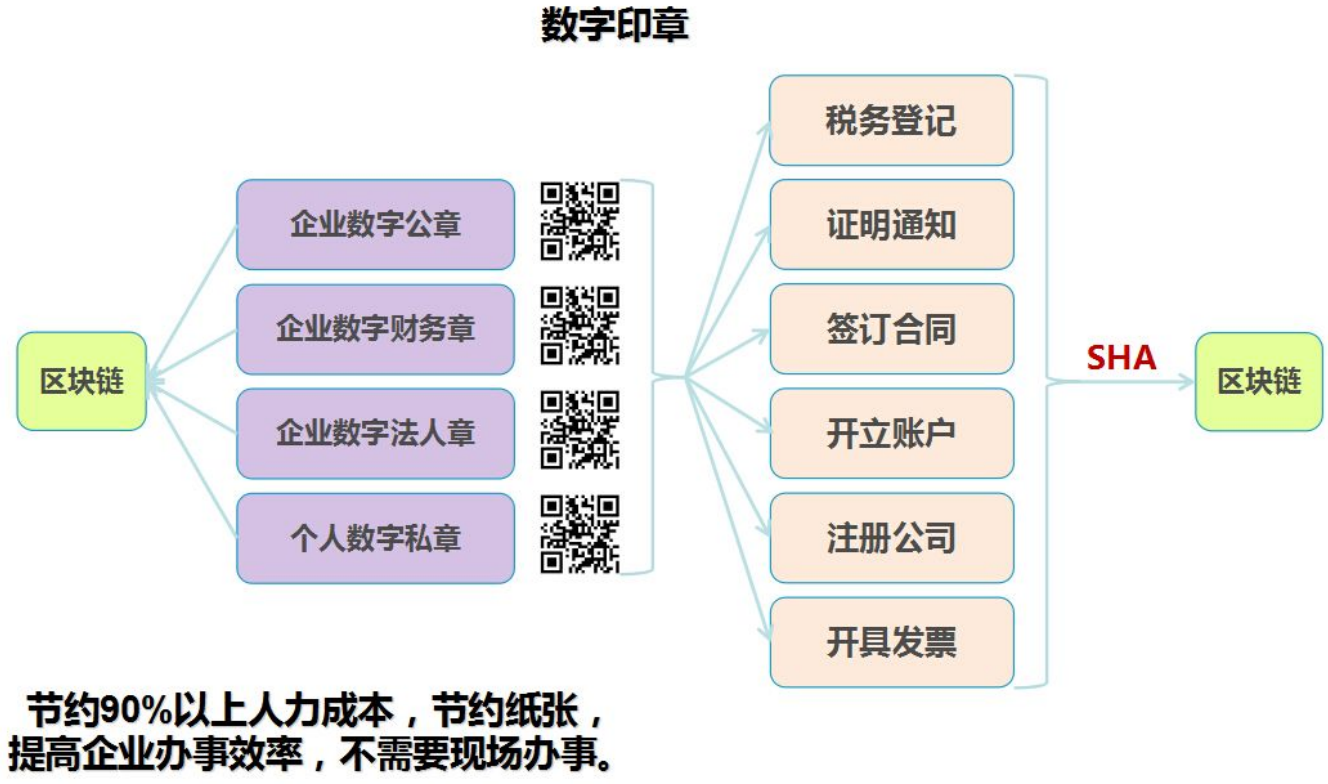
2. 社会事务的公开功能

公益事业的捐款资金流向可以直接查到受益者是否接收，甚至可以知道受益者的消费情况，如购买文具或缴纳学费。数据无法修改，公正性得到保障。

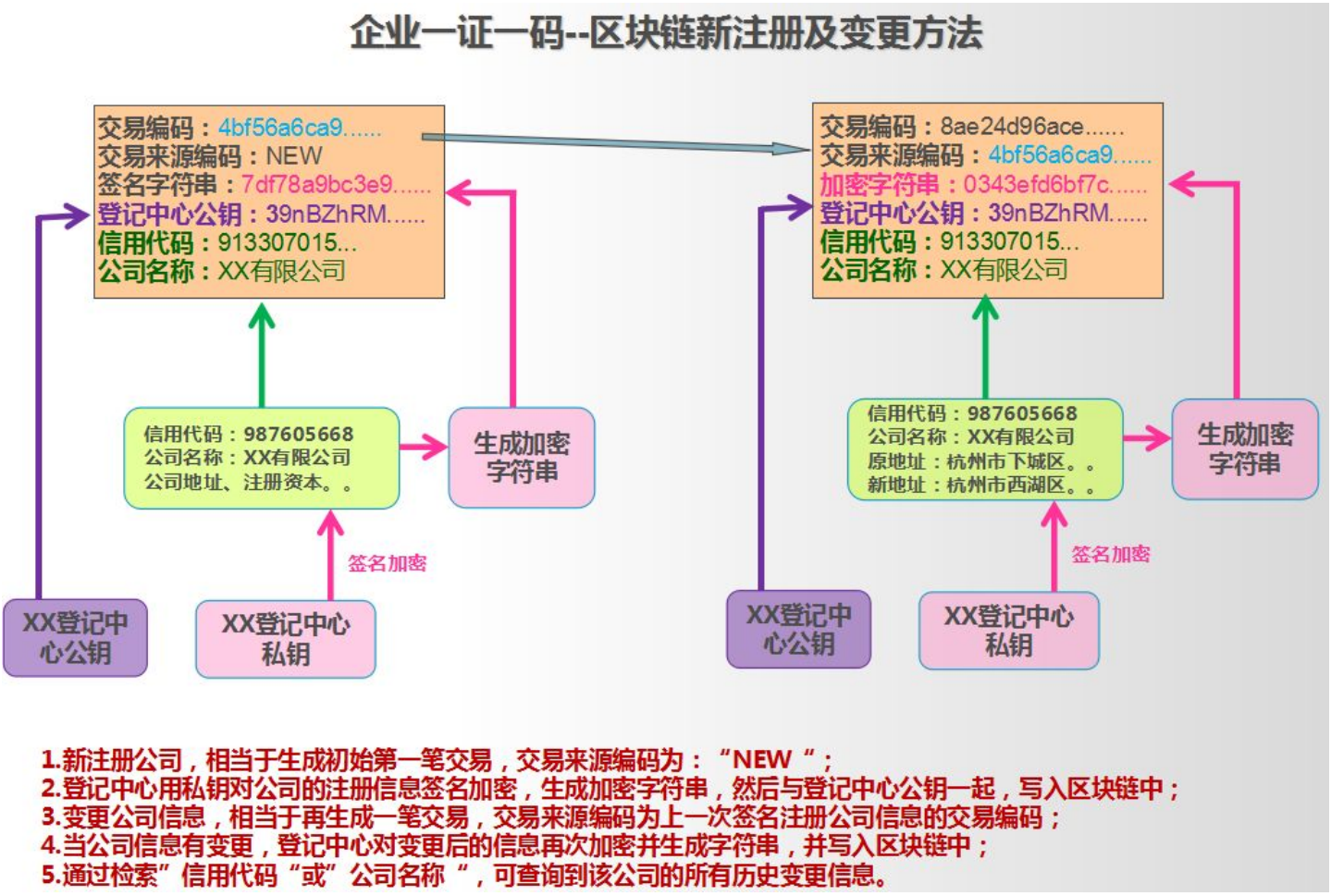


（六）智能合约的实现以及互联网技术的革命

1. 企业合同可全部通过区块链签约，企业、财务、法人全部用私钥签名即可，无需高昂的验章成本，甚至营业执照、税务登记证、组织机构代码证也都可以不用复印了。



2.在区块链上完成企业注册的“三证合一”，并实现“一证一码”模式，提高市场准入效率。这样可以保证写入区块链的数据都是通过登记中心签名，并且验证无误后写入区块链，通过交易编码的关联，保证信息的连续性和一致性，社会统一信用代码和公司名称作为检索关键字便于检索。



四．总结

比特元开发团队已经基本上完成了区块链安全支付系统的建设，多种数字资产的 P2P 高速配对交易所也即将开始测试，目前已经开始为一些合作方搭建区块链交易所或其他区块链项目。如果您对我们的区块链应用项目有合作或投资意向，可与我们联系；如果您是有意向参与区块链技术开发的程序员，也可与我们联系。

微信：yfx0323　全国电话：95105528　QQ：800032133　网站：bityuan.com

比特元开发团队
2015 年 11 月 10 日