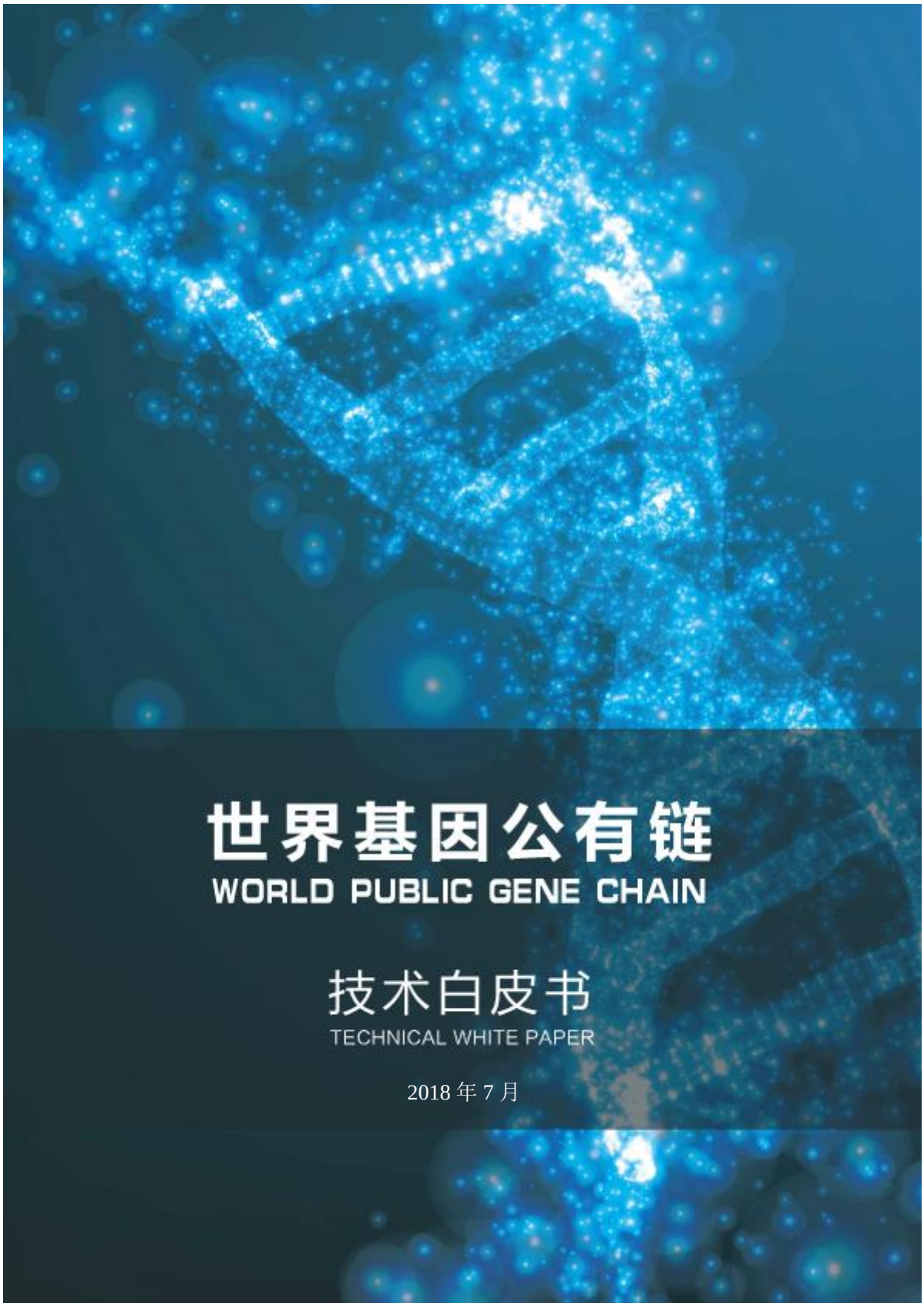

世界基因公有链
WORLD PUBLIC GENE CHAIN
技术白皮书
TECHNICAL WHITE PAPER
2018 年 7 月

1. 摘要

当今的区块链的发展势头远远不亚于 20 年前的互联网的发展。回想起三年前刚接触区块链技术，当向身边的同事提到笔者正在从事区块链技术，一般都是一头雾水。他们通常会问，什么是区块链？而如今的区块链，几乎是人尽皆知，即使很多人不是真正理解和认识区块链，但是也有个一知半解或者参与者到区块链行业中来，因为相比于三年前单一的区块链技术产业的发展，如今的区块链相关的各个产业都蓬勃发展，包括各种类型的区块链项目，区块链自媒体，区块链培训，区块链数字交易所，区块链钱包，矿场，区块链资讯和社交媒体等。

区块链的发展逐步从单一的比特币应发展到各行各业全生态的应用，而基因行业被认为是区块链很好的应用场景，基因技术关系到人类的健康甚至生命的延续，所以基因被认为是未来人们拥有的最大财富。 然而由于基因检测成本高，人们对基因技术的认识普遍不足，基因在生活中的应用相对不够普及，区块链的出现为解决这些问题提供了可能。

2. 背景介绍

现代生命科学技术，由于 DNA 双螺旋结构的发现和人类基因组计划的实施，在 20 世纪得到了空前的发展。进入 21 世纪，生命科学延续了自上个世纪中叶以来的迅猛发展势头，仅仅一个世纪的发展，基因科学技术就已成为可动摇人类生存基础的一场革命， 其巨大的创造力和破坏力使人们深切感受到其两面性。不论基因科学的研究将朝哪个方向发展，我们都正处在基因技术的爆发期，人类历史都将因基因科学而走向新的转折点，如何驾驭基因科学技术，使之安全有效地为我们每个人服务，是我们需要探索的重要课题。

区块链是一个点对点的、去中心化的、安全的共享架构，让原先不可能被共享出来的数据和资源可以被共享。区块链所能打开的数据资源将比互联网更广、更多。基因技术的基础是建立在数据分析技术之上，将基因技术与区块链融合，海量数据和资源才能被有效地分析和利用。

3. 基因技术应用场景

3.1. 精准治疗

随着时代的发展，科技的进步，医学必定朝着精准治疗方向发展，个性化治疗也会成为刚需，毕竟每个人都是一个个体，与生俱来的不一样。

在世界基因链基因护照的帮助下，基因治疗将会得到更好的发展，用户可通过世界基因链完成个体化用药的基因分析、肿瘤的诊断与筛查、出生缺陷遗传病的诊断与筛查等。

目前临床研究发现，很多类型的单基因遗传疾病和一些急性或慢性代谢性疾病，大多数都可以通过精准化的营养干预达到有效的治疗，从而改善治疗效果。

通过 WDNA 世界基因链为每个用户赋予的基因护照，用户可以共享基因数据，WDNA 平台通过大数据技术分析，获得基因对人体各个性状的影响，从而达到有效的诊断和治疗。

通过健康体检包括免疫细胞功能检测构建个人健康档案，通过 WDNA 平台，结合大数据分析动态检测人体的健康变化，通过大数据分析和基因数据解读，可对用户提供精准健康评估，干预，督导和健康教育管理服务。

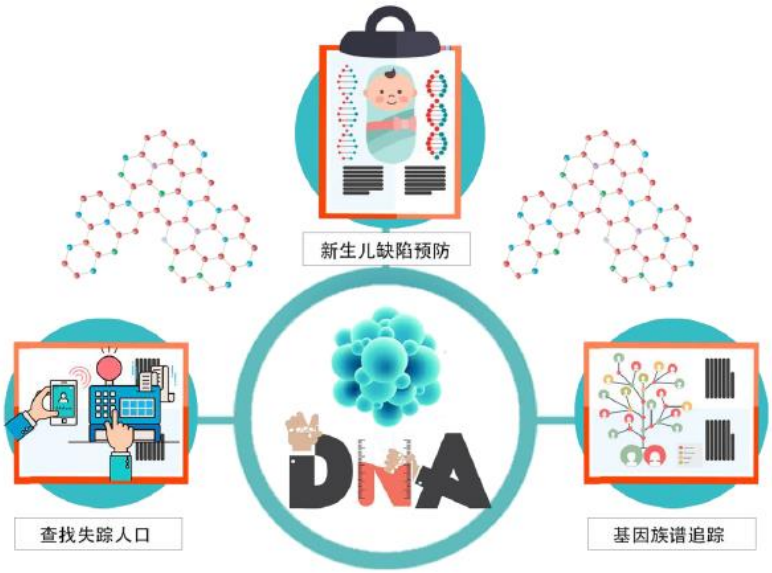
人们可以在身体没有患病的情况下，及时了解自己的基因缺陷，知道自身患病风险，对自己的疾病做到早知道、早预防、早治疗，采取一系列有针对性的预防、治疗措施，使自己的生活环境、生活习惯等适应于基因的要求，做到自己主宰自己的生命。

3.2. 基因关联查询

通过基因大数据分析，用户可以了解自己的血统，建立个体之间的关系以及不同家族之间的遗传距离。这样通过 WDNA 平台，用户就可以追溯家谱，族谱，以及父系母系祖先，同时随着越来越多的用户通过 WDNA 共享基因数据，可进一步追溯人类迁徙路线。

面对目前新生儿缺陷高发的现象，更好的办法是预防罕见病患儿的出生，基于基因护照，借助医学方法，结合遗传咨询，可快速、全面、准确地帮助育龄人群了解自身是否是隐性遗传病致病基因的携带者，让所有夫妇拥有健康的宝宝和幸福的家庭。

WDNA 将建立失踪人口基因数据库，用户将自己的基因护照信息录入数据库后，WDNA 还能网络会将信息自动检索“碰撞”，可用于寻找失踪人口、被拐儿童。



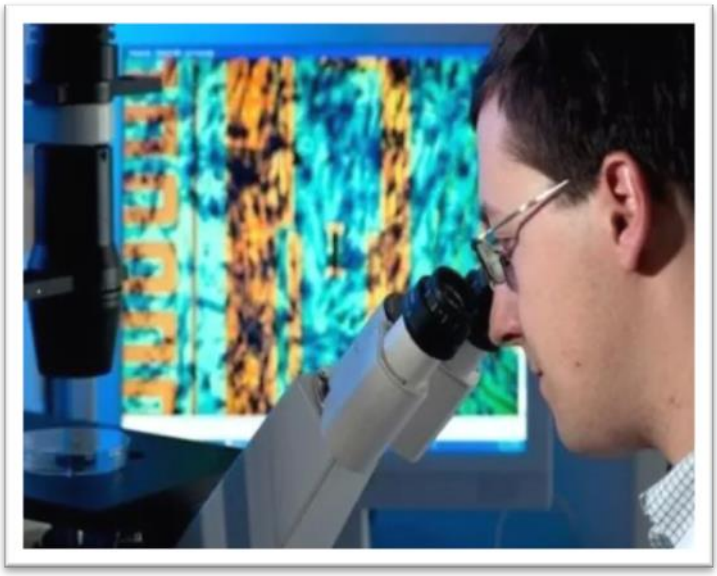
3.3. 食品工业

基于基因护照 2.0，可解析各类农牧业产品的发育机制，为培育具有高产、优质、等优良性状的产品奠定良好的基础，对推动世界农牧业生产有重要意义。同时，基因护照中基因组序列的获得为在育种中进一步利用野生资源的优势基因提出有力工具，为人类开辟新的食物来源。

3.4. 学术领域

电子病例挖掘。基因护照数据库是一个汇集了患者们所有基因数据的存储库。可用于直接改善患者的医疗体验。在招募患者进行临床试验时，基于基因护照数据库的电子数据挖掘可对患者进行匹配。换而言之，患者招募系统可以直接发掘到符合条件特定基因护照用户，为他们提供参与临床试验的机会。

病人分类数据库。WDNA 将根据基于基因护照数据库中基因序列特点进行分类，建立医疗行业的病人分类数据库。在医生诊断病人时可以参考用户的疾病特征、化验报告和检测报告来快速帮助病人确诊。在制定治疗方案时，医生可以依据病人的基因特点，调取相似基因、年龄、人种、身体情况相同的有效治疗方案，制定出适合病人的治疗方案，帮助更多人及时进行治疗。这些数据也有利于医药行业开发出更加有效的药物和医疗器械。



4. 基因行业痛点

基因技术虽然已经发展很多年，但实际应用和带给人们的价值仍然有限，人们对基因技术的认识不足，基因技术普及仍然不够，目前基因行业存在的痛点主要有 5 个方面：

第一是安全方面。目前的基因检测数据都是单点存储，中心化存储，这就意味着数据的存储有单点故障隐患，此外中心化存储还会导致数据的真实性遭到质疑，因为任何数据库维护和管理人员都可以修改数据。通过区块链去中心化，防篡改的技术可以解决单点存储问题和数据真实性问题。

第二是隐私方面。基因检测数据的主体是用户自身，基因检测机构有售卖用户基因数据的现象，暴露和侵犯了用户隐私权。通过基于密码学的隐私保护技术，数据授权技术可以保护用户基因数据的隐私。

第三是所有权方面。基因数据的 owner 本身就是用户自己，没有用户自身的授权，第三方不可以使用后售卖其基因数据。通过 WDNA 平台和公钥密码体系技术，可以让基因数据的所有权回归用户自己。

第四是数据共享方面。目前基因检测机构之间，医疗机构之间都没有将数据共享，很多同样的数据都反复重复检测。可以通过联盟链技术把基因行业整个生态结合在一起可以实现数据共享。

第五是成本方面。因为目前用户基因检测成本太高，所以无法普及。通过 WDNA 平台，可以普及基因技术，而且可以给机构带来用户流量，从而可以降低基因检测成本，我们平台设计多样化的基因产品，用户花很少的钱即可参与到基因检测中来。

针对以上痛点，WDNA 平台通过区块链技术可以解决这些行业痛点。

5. WDNA 平台特色功能

5.1. 个人基因数据安全存储

通过区块链实现去中心化存储可以保证基因数据的安全性，利用区块链的不可篡改性保证链上基因数据的真实性和可靠性。WDNA 平台主链上并不保存用户基因的原始数据，只是保存其原始基因数据的指纹信息，目的是保证其信息不可篡改。用户基因信息的原始数据保存在 WDNA 侧链，但基因原始数据的存储依然是去中心化的，分布式的，WDNA 不提供中心化的服务器保存用户的基因数据，从技术上做到透明，自证清白。从而保证用户基因数据的安全性，真实性和不可篡改性。随着越来越多的用户分享基因数据到 WDNA 平台，WDNA 在逻辑上构建了全球最大的基因数据库。利用这些数据，经过用户授权，可以进行大数据分析和人工智能研究，加速基因行业的发展。

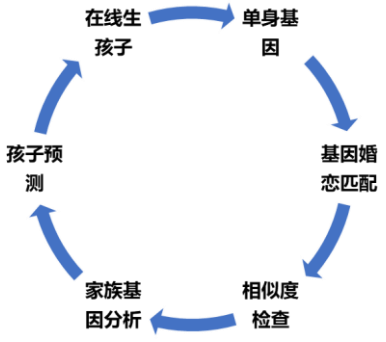
5.2. 掌控自己的基因数据

基因检测数据保存在区块链上，数据所有权回归用户自己，用户可授权分享基因数据，同时可以获取收益。WDNA 平台的用户在拥有了自己的基因数据后可以通过平台将数据授权给第三方机构访问从而获得收益，如授权给保险公司用于保费计算，授权给基因研究机构进行基因大数据分析和基因研究，授权给医疗机构进行医疗诊断，授权给婚恋交友对象，让对象更好的了解自己，找到最佳的伴侣。

5.3. 查看基因测序报告

用户基因数据上链后，可以在 WDNA 钱包 DAPP 中查看自己的基因测序报告，专业的测序报告晦涩难懂，用户可以通过 WDNA 平台邀请基因专家或基因专业机构进行报告解读，同时通过支付 WDNA Token 作为解读费用。

5.4. 基因婚恋社交



为了推广 WDNA 平台，普及基因技术，WDNA 平台推出基因婚恋社交功能。主要提供单身基因测试，基因婚恋匹配，性格相似度检测，家族基因分析，孩子预测等功能。

5.4.1. 单身基因

2014 年 11 月 20 日报道，科研人员发现一种“单身基因”，携带这种基因的人单身的几率比别人高 20%。这种基因可以降低大脑中负责感觉良好的化学物质血清素的浓度，使人对亲密关系感到不自在，这可能导致这个群体从一开始就难以构建交往关系—甚至导致一再分手。

WDNA 平台提供帮助用户检测是否携带单身基因，从而帮助单身用户认识自己，协助其构建和谐的夫妻或男女朋友关系。

5.4.2. 基因婚恋匹配

将基因检测纳入到婚恋交友当中，为广大单身人士提供一种更为科学负责的择偶匹配方式，提高婚恋匹配的成功率和可靠性。

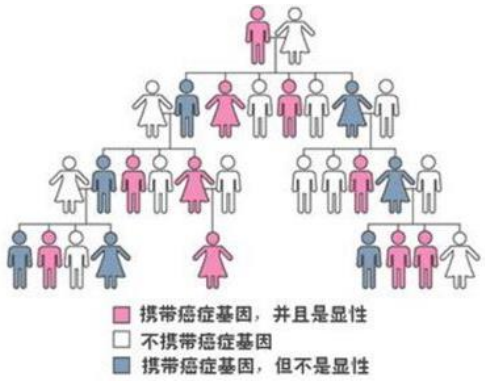
通过基因检测，给出包括遗传疾病、性格特质及抗病能力等几十项基因解读报告，通过基因特性为 WDNA 单身用户推荐婚恋对象，有效避免一些因潜在基因不匹配导致的性格、生活习惯、遗传因子不和等问题，最终实现科学高效的婚恋匹配。

5.4.3. 基因相似度检测

缘分的本质是基因，基因的相似性决定能否成为夫妻。两者基因相似是指基因片段中的 DNA 碱基数量以及序列基本相同。

WDNA 平台提供单身男女基因相似性匹配服务，帮助用户提高婚恋交友的成功率。

5.4.4. 家族基因分析

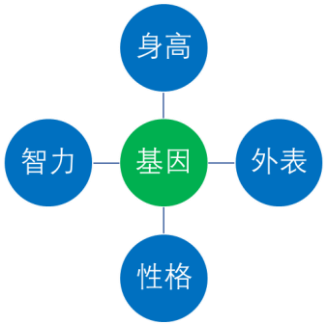


在 WDNA 婚恋平台，用户不仅可以查看相亲对象的基因匹配度，单身基因特性，还可以查询到其

家族的基因分析报告（需要对方授权），从而综合判断婚恋匹配度。

5.4.5. 孩子预测

通过基因技术预测一对男女匹配所生的孩子的身高，性格，智力和外表，帮助 WDNA 用户更精准的选择婚恋交友对象。



- **智力**：智力的影响约占 50%—60%，因为孩子的智力遗传来源主要来自母亲。人类与智力有关的基因主要集中在 X 染色体上。女性有 2 个 X 染色体，男性只有 1 个。男生是 XY，所以男生的智商全部都来自母亲的遗传，女生是 XX，所以女生的智商是父亲跟母亲各有一半影响
- **身高：**35%来源于父亲，35%来源于目前，30%来源于后天的努力
- **性格**：性格是父亲的遗传大。性格的形成固然有先天的成分，但主要是后天影响。比较而言，爸爸的影响力会大过妈妈。其中，父爱的作用对女儿的影响更大。
- **外表**：肤色，演讲，鼻子，耳朵，下颚，胖瘦，腿型等。

5.4.6. 在线生养孩子

结合基因技术，区块链技术，人工智能技术，大数据技术实现在线预测孩子长相，性格，智力，身高等。同时为了给用户更好的直观体验，结合 AR、VR 技术，除了在线预测，还可以直接实现在线生孩子，然后通过 3D 展示出来。

6. WDNA 技术方案

WDNA 基因链基于“开放，共享，共赢，创新”的设计原则， 在研究和学习业界主流区块链底层技术的基础上，搭建自身的区块链基础设施，面向基因领域和医疗健康行业，用区块链技术解决实际问题，打造全球基因区块链的生态体系。

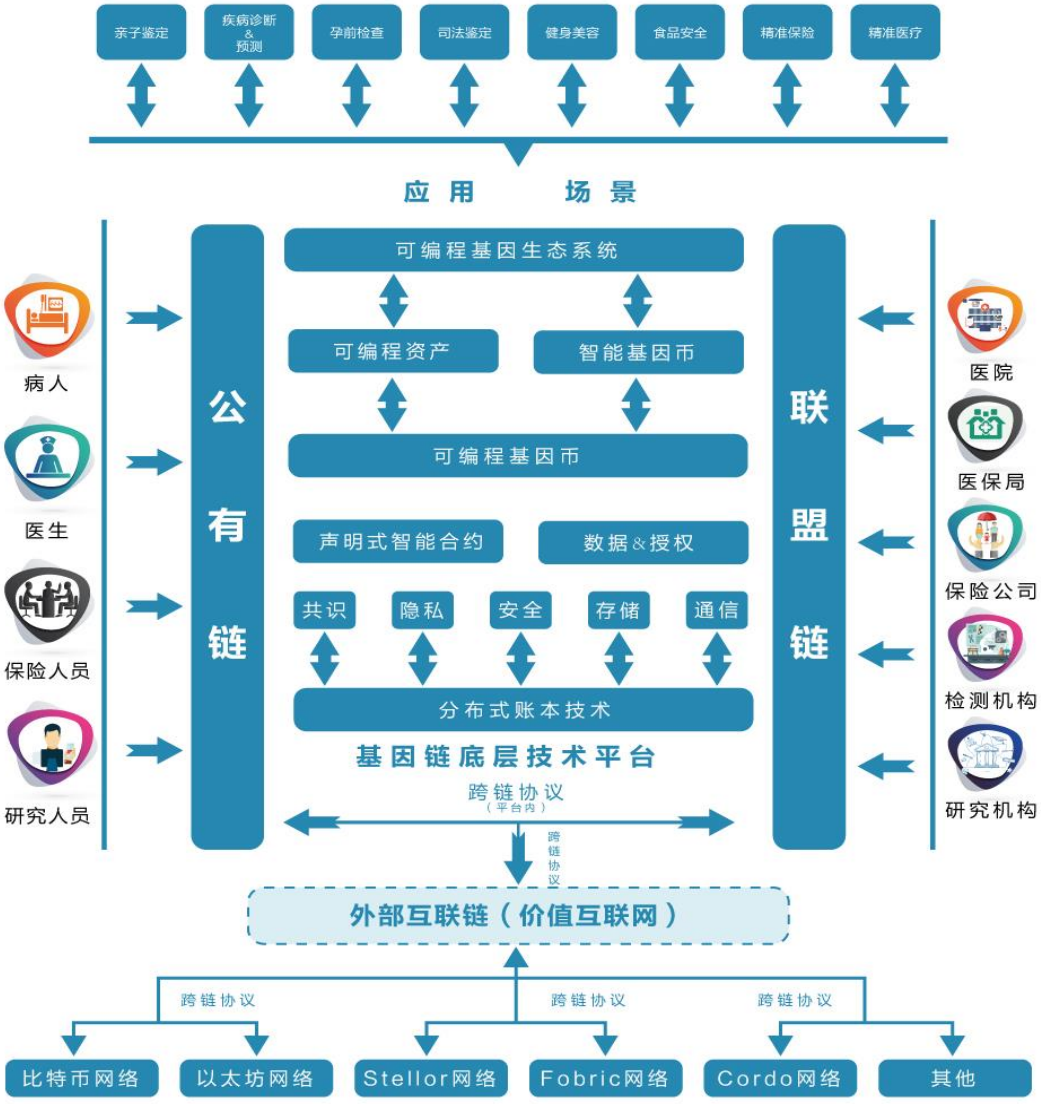
WDNA 基因链设计原则：

开放：在技术研发和自主技术创新上，我们采取开放包容的心态，学习和研究业界前沿的最新科技，接纳业界对 WDNA 平台的各种意见，学习其他平台的长处。

共享：在学习业界前沿技术的基础上，我们把我们自身的研发成果（包括技术和非技术方面的研究成果）公布于众，共享知识和研发成果，让大众参与监督平台的发展，集思广益。

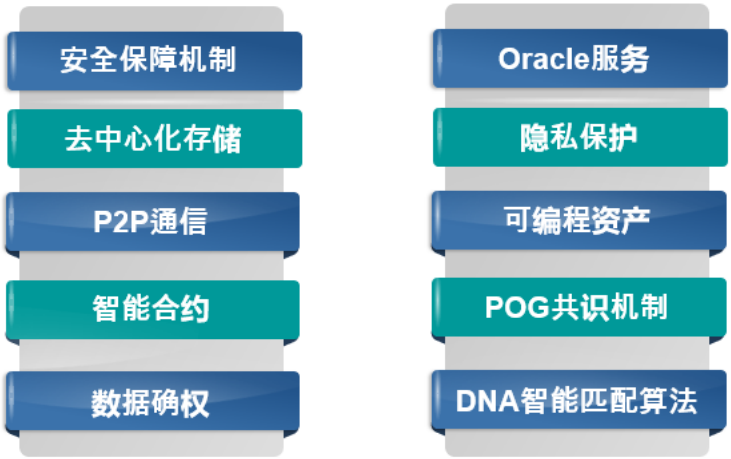
共赢：共赢是区块链的核心思维和本质特征。拥抱区块链，必须有共赢的理念和心态。在 WDNA 区块链的生态体系内，参与的个体和组织机构都是 WDNA 平台的受益者。WDNA 区块链生态平台，不仅仅是传统技术的创新应用，更是蕴含了基于区块链的新经济模式的理念。

创新：WDNA 区块链在研发前沿科技的基础上自主创新设计自己的底层区块链基础设施，在商业模式上开历史先河，本着服务用户解决行业痛点的原则设计独特的系统架构。

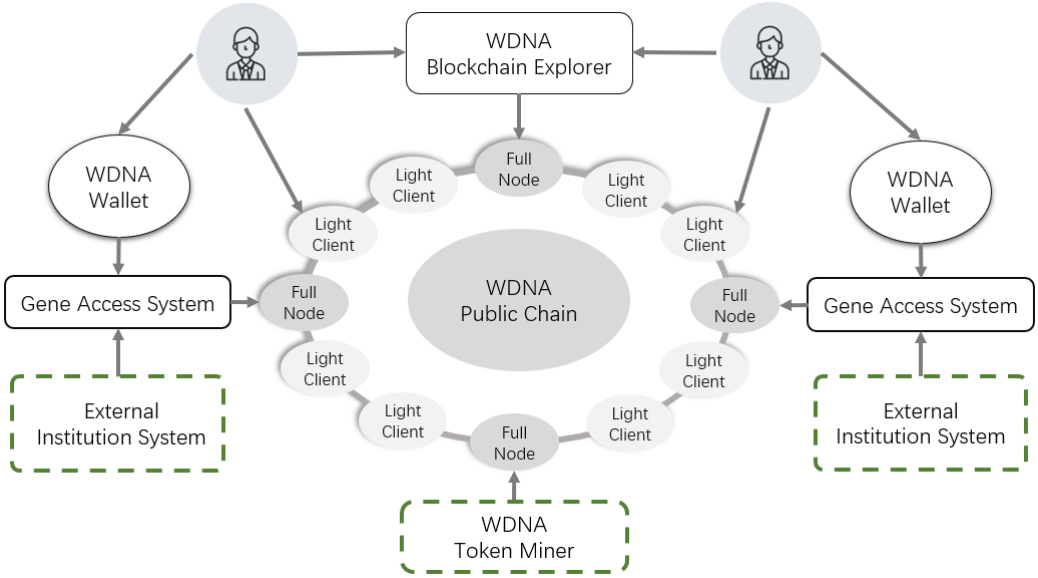


6.1. 平台总体架构

WDNA 底层技术平台基于当前前沿的分布式账本技术和区块链技术，在研究前沿科技的基础上，结合医疗健康和基因领域的行业特色加以改造，在账本存储扩展、数据隐私保护、数据访问授权、智能合约与外部世界交互、智能合约引擎、跨链资产转移等方面做了大量的优化、改造和创新。



6.2. 部分逻辑架构

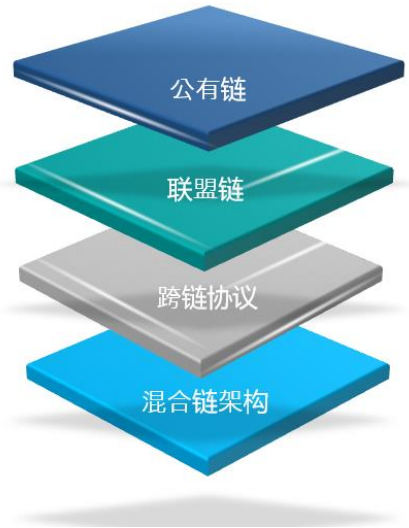


WDNA 基因公有链生态平台由公链，跨链协议，联盟链，侧链等多个组件组成。以上是公链的

部分逻辑架构图，整个项目的实施分阶段进行，目前项目还在进一步设计和开发中。

6.3. 混合链架构

区块链是一种类似互联网的具有革新性的新技术，它变革的是整个社会制度的底层基础设施，当前大多数大型金融机构和公司都是用传统的模式应用区块链，将区块链作为普通的 IT 技术，而其他方面的运作模式和治理模式都未跟上，导致单纯的以技术为导向的联盟链缺乏区块链应有的强健的生命力，这就是为什么联盟链发展已经好几年，仍然没有一个人们都认可的杀手级的区块链应用面世。而目前的公有链大多是没有实际应用场景的基础链（专注于底层技术基础设施建设），或者是类似比特币的只有资金转账功能的公有链。虽然这几年随着区块链的发展，公有链项目创新百花齐放，但大多数区块链公链项目仍然是空中楼阁，没有更实际业务场景结合。结合公有链和联盟链各自的优势劣势，WDNA 技术团队设计出了混合链架构，我们认为只有混合链才是区块链未来的发展方向和架构模式。区块链应用要最终落地，混合链是必然的发展方向。



WDNA 混合链架构充分发挥了公有链的优势：自由出入，更高程度的去中心化（技术架构上，政治上而非逻辑上），带有 token 的激励机制，同时也结合了联盟链的优势：面向机构参与者，授权准入机制，更适合区块链跟现实业务场景相结合的行业应用项目。WDNA 致力于做基因行业的公有链项目，采用混合链架构是顺应时代发展和实际业务需求的需要，使用自身研发的跨链协议，不仅解决了内部公有链和联盟链之间的价值交换，同时也解决了与外部公有链之间的价值转移。WDNA 跨链协议目前还在进一步研发之中。

6.4. 去中心化存储

WDNA 是面向全球基因行业的公有链，但是 WDNA 基因链的主链上只会保存基因数据的指纹

信息，而不会存储基因原始数据本身。用户个人的基因原始数据都会被用户自身的一对数据公私钥进行加解密，利用星际文件存储系统（IPFS）技术（目前的方案，后续可支持更灵活的存储方案），去中心化的存储在 WDNA 基因链的侧链上。基因原始数据采用非对称加密技术存储，陌生用户提供存储空间，却无法看到数据内容。

在量子计算机普及之前，公钥密码技术是被业界证明的安全可靠的加密技术。因为公钥是通过私钥计算出来，但是由于其背后的数学原理，很难反推（通过公钥计算私钥），因此 WDNA 平台的用户只要持有自身的私钥，保管好自身的私钥，即可保证自身基因数据的安全性。而基因数据的买方必须通过授权才能获得用户的基因数据。

WDNA 平台完全基于区块链技术实现，内部不设置中心化服务器保存基因数据，用户的基因数据所有权完全由自身掌控，数据之间的交易和传输都是 P2P 的，因为数据采用非对称加密，即使数据在传输过程被黑客截取，也因为没有私钥而无法解密数据，从而保证数据的安全性。

为了保证 WDNA 平台数据和交易的公开透明，WDNA 平台设计了自己的浏览器，用户可以通过 WDNA 浏览器查询交易细节，查询交易基因数据，让用户确保自身的数据的指纹保存在链上，让用户确保交易处理成功。WDNA 浏览器类似于 etherscan.io 的功能。

6.5. 底层技术选型

WDNA 是面向行业应用的区块链平台，专注于基因领域的行业应用区块链，其目标不是基础性公链，因此从 0 到 1 设计底层区块链基础设施是不明智的，正如没有必要每个公司都去开发计算机或手机操作系统一样，没有必要都去重复造轮子。然而目前市面上成熟的基础性公链技术框架太少，基本找不到可以商用的基础性公链。考虑成熟度等因素，WDNA 技术团队选择在以太坊源码基础上改进和创新以满足基因行业应用的需要，毕竟相比其他基础型公链项目，以太坊是目前唯一相对成熟的公链项目，历经多年的行业验证和技术积累，相对可靠和成熟，尽管性能吞吐量有限，但是基础相对稳定可靠，而性能方面的优化，WDNA 将根据不同的基因应用场景提供不同的解决方案和优化措施。

6.6.隐私保护

隐私保护一直是区块链领域一个重要的话题，特别是在联盟链应用上，企业比较关心数据的隐私保护问题。针对基因行业，如何防范区块链上用户的隐私基因数据被授权访问后的二次转卖？

这其实是区块链保护隐私的一个重要问题，利用零知识证明或者同态加密做到数据使用权和所有权的分离。隐私数据的授权访问是为了下一步对数据的使用，而在未来的区块链世界里，我们不再需要对隐私数据做授权访问，对于隐私数据的使用，也就是计算，都在用户这边进行，数据永远不暴露出来，对方只拿到计算结果，和对这个计算结果的一个密码学证明，保证结果可信，这样的方案就不会发生隐私数据的泄露。

作为区块链的早期应用，比特币设计上对隐私保护确实不足，并且这也不是比特币设计的主要目的。作为后来者的门罗币和 ZCash，是否在区块链隐私保护上做了更多的增强？

门罗币主要是采用环签名技术，但是环签名也有一个缺点，就是环签名中依旧需要与其他用户的公钥进行混合，因此可能会遭遇恶意用户从而暴露隐私。

ZCash 采用 zksnark 零知识证明技术实现其交易过程的隐私保护，是区块链领域第一个使用零知识证明保护交易隐私的成功案例，尽管如此，交易效率仍然很低。

WDNA 采用零知识证明，门限签名，同态加密技术，结合公钥密码学技术保护用户的隐私数据，实现用户基因数据的授权访问。

6.7.数据确权

目前互联网上的数据主要由国家机构和大型数据企业负责采集，绝大多数的数据并未被充分利用；而那些正在使用的数据，其模型简单、流转有限、使用场景单一，严重制约了数据市场的繁荣发展。主要因为中心化的数据市场，存在以下弊端:

- 数据所有权不属于产生数据的主体

在现有法律框架下，虽然个人数据的所有权没有明确的归属，但数据采集的机构或企业在采集用户的个人数据时没有起到告知的义务，以及对数据主体提供报酬或收益。不论这是否侵犯了用户个人数据的拥有权，但这至少影响了用户提供个人数据的积极性，造成了数据采集的困难。区块链的出现，让用户对数据的所有权的控制成为了可能，用户有了分享数据的积极性。

- 数据采集者没有积极性

目前的数据市场，数据采集者不论是自己进行采集，还是委托给第三方进行，其采集成本都是由最终的数据消费收回甚至没有收回。随着国内的移动互联网发展迅猛，现有的采集服务已经无法满足日益剧增的数据需求，急需一套新的激励方案促进数据采集者更积极主动地去采集用户数据。

- 数据使用场景不足

因为缺乏数据所有权的认定，在流转和使用过程中就会出现各类限制。最新修正的法律规定，在调用、流转个人隐私数据时，需要对数据对应的自然人进行充分的授权，未经个人允许，而直接销售其敏感数据的行为已经涉嫌犯罪。而现实中，这些数据因为没有做足够的细分和建模，其应用场景也非常有限。目前，数据消费的应用场景主要集中在金融借贷领域，而其他领域少有数据消费的行为。

在基因行业，上述问题同样存在，基因检测数据的所有权应该归属用户，而目前的现状是基因数据保存在检测机构手中。用户对数据所有权缺乏控制，会带来数据共享问题，信息孤岛问题，带来生活和工作的不便，比如基因行业的大数据和人工智能需要大量的用户共享医疗数据和基因数据。

WDNA 平台通过密码学技术实现数据的授权访问和用户对基因数据的所有权掌控。基因数据所有权回归主体，同时通过授权第三方访问基因数据可以获得收益，这增强了用户分享数据的积极性，让更多的用户加入 WDNA 平台，逐步可以构建全球最大的基因数据库。

6.8. 共识原理

共识机制是区块链核心技术之一，WDNA 平台提供两种可选的基于挖矿的共识机制：数据挖矿和计算挖矿。

6.8.1. 数据挖矿

数据挖矿作为 WDNA 平台中最重要的用户激励措施之一，通过数据挖矿可以鼓励更多的用户分享自己基因检测数据，构建 WDNA 全球基因数据库，越来越多的用户共享基因数据给基因行业

和医疗健康行业利用大数据和人工智能提升医疗服务提供了很大的帮助，进而给人类健康做出贡献。

数据挖矿的场景有很多，基本场景如下：

- 用户分享基因数据给机构。
- 用户分享基因数据给陌生人（基因婚恋社交）
- 用户使用 WDNA 币支付结算。

6.8.2. 计算挖矿

POW 挖矿是区块链最早使用的共识算法，也是最被广泛验证为真正安全的共识算法。目前大多数安全稳定的数字货币项目都采用 POW 挖矿算法作为共识机制。然而挖矿过程浪费大量的电力资源也是经常被业界批评的缺点，也因此诞生了很多 POS，DPOS 等共识机制。WDNA 平台采用类似 POW 的共识机制，只是把挖矿的算力应用到有价值的科学计算之上，如使用 WDNA 挖矿算力进行基因大数据分析和人工智能。

6.9. 跨链协议

在区块链所面临的诸多问题中，区块链之间互通性极大程度的限制了区块链的应用空间。不论对于公有链还是私有链来看，跨链技术就是实现价值互联网的关键。目前的跨链技术主要包括三大类：公证人机制（Notary schemes）、侧链/中继（Sidechains/relays）和哈希锁定（Hash-locking）。

尽管如此，目前跨链技术尚不成熟，通用的跨链协议仍然还在研发中。这让有跨链需求的区块链行业应用项目在技术选型时造成一定的挑战。

WDNA 平台在研究当前行业主流跨链协议的基础上抽象设计出自己的跨链 wrapper 协议，支持主流跨链协议可配置，在项目第一期，我们采用成熟稳定的见证人模式实现跨链，通过内置基于 0x 协议的跨链组件实现不同 ERC20 数字资产之间的资产转移和兑换。WDNA 跨链协议目前仍在设计和研发中。

6.10. WDNA 钱包

钱包的定义：在数字资产世界里，钱包是一个密钥 (包含私钥和公钥) 的管理容器。用户使用

私钥进行签名交易，从而证明拥有该交易的输出权，其交易信息并不是存储在该钱包内，而是存储在区块链中。

WDNA 钱包包含了基础的移动钱包功能，用户也可以在 WDNA 钱包中管理自己的数字资产，包括转账、收款、创建钱包、导入钱包等功能，还可以查看当前各种数字货币的行情。除此之外，用户还可以通过 WDNA 钱包查看自己的基因护照信息，包括基因检测报告，基因检测报告解读。

6.11. WDNA 浏览器

区块链浏览器是一种搜索工具，我们通过输入某钱包地址或某笔交易 ID，就可以查询此钱包的余额和任意一笔交易的详细信息：比如当前比特币的转账费用是多少、给你转账的地址有多少余额、一笔转账是否已经成功。也可以通过输入块高，块哈希等来搜索某一特定区块的所有内容。

WDNA 浏览器实现一般区块链浏览器的功能，是专门为 WDNA 平台用户设计的区块链浏览器。除了基本的区块链浏览器功能之外，还提供特定基因护照的基因测序信息，基因交友等信息的查询。

WDNA 浏览器的功能类似 etherscan.io，只是在功能上增强，而且专门面向基因行业，是 WDNA 平台的专属区块链浏览器。

6.12. DNA 智能匹配算法

从生物学角度来看，人类通常会寻找对自己最有吸引力的人做伴侣，这样可以有更好的基因匹配效果，以便能够产生最强壮的后代。在 WDNA 婚恋社交平台，我们的基因团队和区块链团队设计了独特的 DNA 智能匹配算法，帮助用户自动匹配优质婚恋对象，从而提高婚恋交友的效率和质量。

6.13. WDNA 可编程资产

在区块链时代，数据被作为资产可交易。数字货币的可编程性可以泛化到其他数字资产，数字资产附加了可编程性更加智能的适应特定的业务需求。对 WDNA 平台的资产附加特定的功能，让其不只是具备单一数字货币或单一资产功能，比如可以指定其只能在指定的时间、指定的地点、指定的商家，限定指定的消费、指定的频率进行使用。也可以指定特定场景获取的 WDNA 资产用于消费不能用于投资。总之，WDNA 平台的资产具备可编程特性，这也是顺应未来社会数字化可编程

化的发展趋势的前瞻性设计考虑。

6.14. Oracle 服务

简单的说，Oracle 服务又称预言机服务，是区块链获取链外数据的方式，目标是解决运行于区块链之上的智能合约和外部世界之间的链接问题。区块链之所以能得到全球那么多人的青睐，一方面是它去中心去中介的天然属性，另一方面就是智能合约了。但是区块链上的智能合约要想和外部世界进行交互，首当其冲需要解决区块链内、外数据通道问题。智能合约应用对预言机（Oracle）服务有着强烈的需求。WDNA 基因链平台不仅支持接入外部第三方的 Oracle 服务，也自主研发可靠的 Oracle 服务，作为用户的可选方案。

6.15. 安全保障机制

以太坊提供了图灵完备的智能合约，但是图灵完备机制是一把双刃剑，在其提供全生态体系的支持各种 dapp 应用开发的同时，也带来了安全性的挑战。此外量子计算机技术的发展也会威胁到传统基于公钥密码体系的系统的安全。因为无论是 RSA 算法、ECC 椭圆曲线算法，还是 DH 密钥协商算法，它们的安全根基都系在“一根绳上”—数论中的“大素数因子分解/离散对数”困难问题之上， 这对电子计算机是个难题，但对量子计算机来说并非难题。

WDNA 基因链考虑到智能合约的不同应用场景，针对联盟链设计了图灵完备的智能合约支持各种业务场景的合约设计，针对公有链设计了非图灵完备的智能合约提高系统的安全性，同时合约编写的易用性进行了独特的设计。为保证智能合约的安全，提供了一套安全检测工具和方法论帮助检查合约的安全。此外，底层区块链后续版本也在考虑采用的密码学算法支持抗量子设计，在安全上具有前瞻性的考虑，但这一抗量子的功能仍然在研发中。

6.15.1. 区块链项目安全保障体系

作为区块链项目方，应该在项目生命周期的每个阶段做好区块链平台的安全保障，毕竟这是用户数字资产安全的基石。WDNA 项目在开发阶段、运营阶段和推广阶段均设计了全方位的安全保障措施，以确保用户数字资产的安全。

开发阶段

开发阶段主要是通过多种措施保障代码本身的质量，这是最根本最直接的安全措施。完全依赖工程师的“聪明”和“优秀”与否来保障代码安全是不可靠的，也是不明智的，软件工程学告诉我们，再优秀的程序员，都难免保障系统代码的 BUG 不出现。WDNA 采用团队集体代码审计，请第三方专业安全公司进行渗透测试（模拟黑客攻击对业务系统进行安全性测试，比黑客更早发现可导致企业数据泄露、资产受损、数据被篡改等漏洞，并协助企业进行修复），漏洞分析与管理，安全加固措施，风险评估等多种手段保障区块链平台的代码级的安全。

运营阶段

运维阶段，从合约审计，安全运维，安全钱包等手段保障区块链平台和用户资产安全。

合约审计：与专业的专注于智能合约安全审计的公司合作，审查参与 WDNA 的用户和机构编写的智能合约的安全性。

常见的安全性漏洞有：

隐私泄露问题。智能合约对区块链上的所有用户可见，包括但不限于标记为 private 的资源，或可造成隐私信息泄露。通过函数可见性审核，敏感函数继承权限检测，函数调用权限检测等审查可以有效杜绝此类漏洞。

交易溢出与异常。由于智能合约本身的约束条件，如条件竞争、交易顺序依赖等，造成的交易溢出与异常。通过检查合约代码是否进行了必须的安全措施，如资金运算是否使用 SafeMath 等。

合约故障。由于智能合约代码中可能存在的不合理故障处理机制，造成的异常行为。此类问题可以通过检测栈高度限制，是否出现栈耗尽情况来杜绝。

安全运维：随着区块链系统运行，其自身存在的脆弱性和面临的威胁随时都在发生变化，安全运维就是在系统运行期间，不断的发现问题和解决问题，并优化安全策略，建立防护、检测和恢复的闭环安全机制，保证业务系统持续安全。安全运维主要从以下几个方面采取措施：

- 防护。应用系统调优、安全加固、安全设备运维。
- 检测。脆弱性检查、代码安全审计、渗透测试、信息安全风险评估、WEB 远程监控、安全巡检、驻场服务。
- 响应和恢复。应急响应、安全通告

安全钱包：向用户提供安全的资产管理钱包是项目平台方义不容辞的责任和义务。WDNA 平台为用户提供多种安全钱包方案供用户选择。常规普通钱包，多重签名钱包和冷钱包。

常规普通钱包。对于大多数资金量不大，要求使用方便快捷的用户可以选择这种钱包，这类钱

包的特点是简单方便，一个私钥对应一个钱包地址。这类钱包也是目前市面上广为流传的钱包。

多重签名钱包。相比于常规钱包，多重签名钱包更安全。WDNA 的多重签名钱包基于密码学中的多重签名技术。

比特币的多重签名实现有两种类型的地址，一种是 MS(Multiple Signature),一种是前面提到的 P2SH(pay-to-script-hash).

WDNA 的多重签名钱包在研究比特币多重钱包实现的基础上设计而成，有 2-of-2 和 2-of-3 两种可选模式。

冷钱包（硬件钱包）。主要是针对拥有资产较多，对安全性要求较高的高端用户。目前市面上主流的冷钱包有 ledger, trezor, keepkey, 库神等。

WDNA 推荐用户使用安全可靠的冷钱包，后续也会推出自己的冷钱包。

推广阶段

在推广阶段，WDNA 主要做好的安全保障工作是反欺诈，反钓鱼和中间人攻击。严格来说，防止中间人攻击对项目方来说没有有效的方法和手段，只有给用户提供安全意识和宣传。对于个人用户来说，要防范 DNS 劫持应该注意不点击不明的连接、不去来历不明的网站、不要在小网站进行网上交易，最重要的一点是记清你想去网站的域名，当然，你还可以把你常去的一些涉及到机密信息提交的网站的 IP 地址记下来，需要时直接输入 IP 地址登录。

6.15.2. 用户数字资产安全

向用户普及安全意识

随着区块链技术运用的越来越广泛，以及数字货币投资越来越普及，很多人开始慢慢进入到数字货币投资市场来了。但目前仍旧有很多小白，对数字货币和钱包技术不甚了解，钱包安全意识缺乏，经常造成资产丢失的事情。即使项目平台方的平台非常安全，用户的安全意识不够，仍然无法保障用户资产的安全。WDNA 平台肩负普及基因技术，关注普通大众健康，同时普及用户数字钱包的安全意识。

安全操作方法培训

WDNA 会组织钱包的安全操作方法, 通过视频或线下 MEETUP 的形式向用户讲解钱包安全操作方法，向普通大众宣传基因技术和 WDNA 平台的价值和使命。

WDNA 资产防丢策略:

在创建完钱包之后，立即备份钱包，采用双重备份和多次备份两种策略。双重备份是指 Keystore 备份和助记词备份，多次备份是指在备份完 Keystore 和助记词之后，要验证备份是否正确，反复验证，确认无误即可。

一定不能遗失了私钥。这里的私钥包括助记词、Keystore 和明文私钥，有些小白在备份助记词时，抄写过后并没有做验证，或者字迹过于潦草，导致后期很难辨识，这些都会导致无法再找到自己的钱包。所以我们在备份钱包时要仔细认真，在后期保管钱包时，要善于使用一些安全的管理工具，确保自己可以随时找到私钥。

WDNA 资产防盗策略:

防盗的实质是防止我们的私钥泄露，或者被黑客盗取。而在防盗策略上，Keystore 和助记词(或者明文私钥) 的侧重点有所不同。

Keystore 防盗策略: 由于 Keystore 是被加密过后的私钥，并且一般是以 PDF 文件形式存在，采用"抄写"这种策略明显是不科学的，所以可以存储在 U 盘里或者密码管理工具里。存储 Keystore 时要和密码分开存储，这样只要密码强度足够高，即使被黑客盗取了 Keystore ，也很难破解，备份 Keystore 时也要多处存储，比如你只存在 U 盘里，如果 U 盘丢失，那么也相当于丢失了钱包。

助记词防盗策略: 在存储助记词时，就需要更加谨慎一些，因为助记词毫无安全性可言，一旦被第三方窃取，那么我们的资产将面临巨大的威胁，所以建议采用物理介质备份，抄写在一张纸上，并且妥善保管，抄写时要注意准确性，也要注意长久保存，不要出现字迹看不清楚等问题。

建议一旦发现自己钱包出现不是自己操作的转出交易，或者意识到自己的私钥已经泄露，要立即停止使用该钱包，并将资产转移至一个新建的钱包。

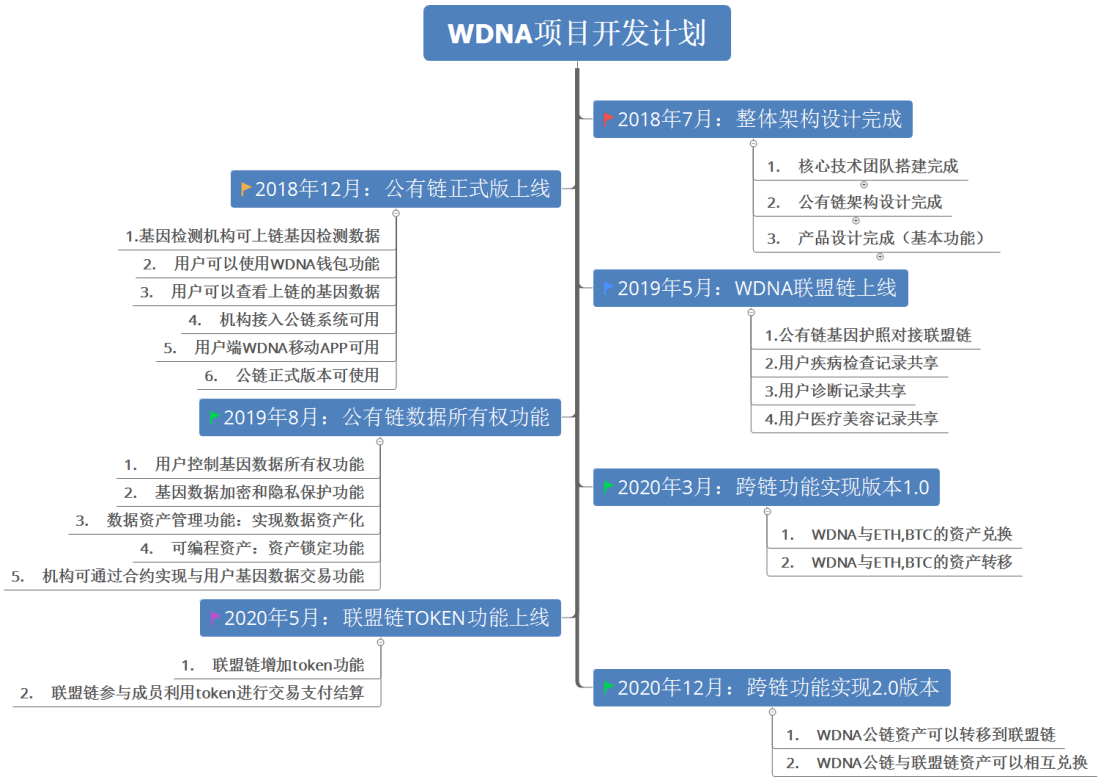
6.16. 结算机制

比特币是区块链的第一个应用项目，也是区区块链最成功的应用，但是比特币应用比较单一，虽然比特币可以实现资金的支付，清算，结算全生态服务，但是只能用在资金转移应用上，其他复杂的业务功能无法实现，不能进入具体的行业应用。而当前的联盟链因为国家政策等原因，基本上都只能做支付，清算，无法实现用数字货币进行结算，结算仍然采用传统的模式进行。WDNA 采用公有链和联盟链相结合的混合链架构, 将公链中流通的 WDNA 币用于联盟链各个机构的之间具体业务的支付、清算和结算，让区块链真正应用到行业具体场景。

具体结算场景:

- 用户请基因专家解读基因测序报告可通过支付 WDNA 作为报酬。
- 基因机构之间，医疗机构之间可以通过 WDNA 进行结算。
- 用户和机构之间，如用户去做基因检测也可以通过 WDNA 进行结算。
- 病人通过 WDNA 平台咨询医生，可以通过支付 WDNA 支付咨询费。

7. 开发计划



8. 总结

无论区块链技术还是基因技术，其发展目前仍处于比较初级和前沿的阶段，WDNA 团队抓住这个时代赋予的契机，创新的发起了 WDNA 世界基因链的项目，致力于解决基因行业的当前痛点，关注人类健康，普及基因知识，最终的目的是让全球的民众都可以从基因技术和区块链技术的价值中收益，提升当前基因行业和医疗健康行业的办事效率，做全球基因行业的行业标准和行业规范。