Node 区块链加速器

区块链与创新创业

http://www.node.ac

李晋

西安电子科技大学 通识课程 2021春季学期

Node 区块链加速器

PART 4
区块链的应用与挑战

Node 区块链加速器

4.1
区块链的特性与功能

区块链的一些特性

- 历史数据公开透明、不可伪造、不可篡改、不可销毁、时间戳
- 去中心化，或多中心化，或弱中心化结构下的多方信任关系
- 无需第三方监督的履约执行
- 防双花带来的价值传递可能
- 匿名性
- 去中心化——是手段，不是目的
- 冗余、低性能——代价

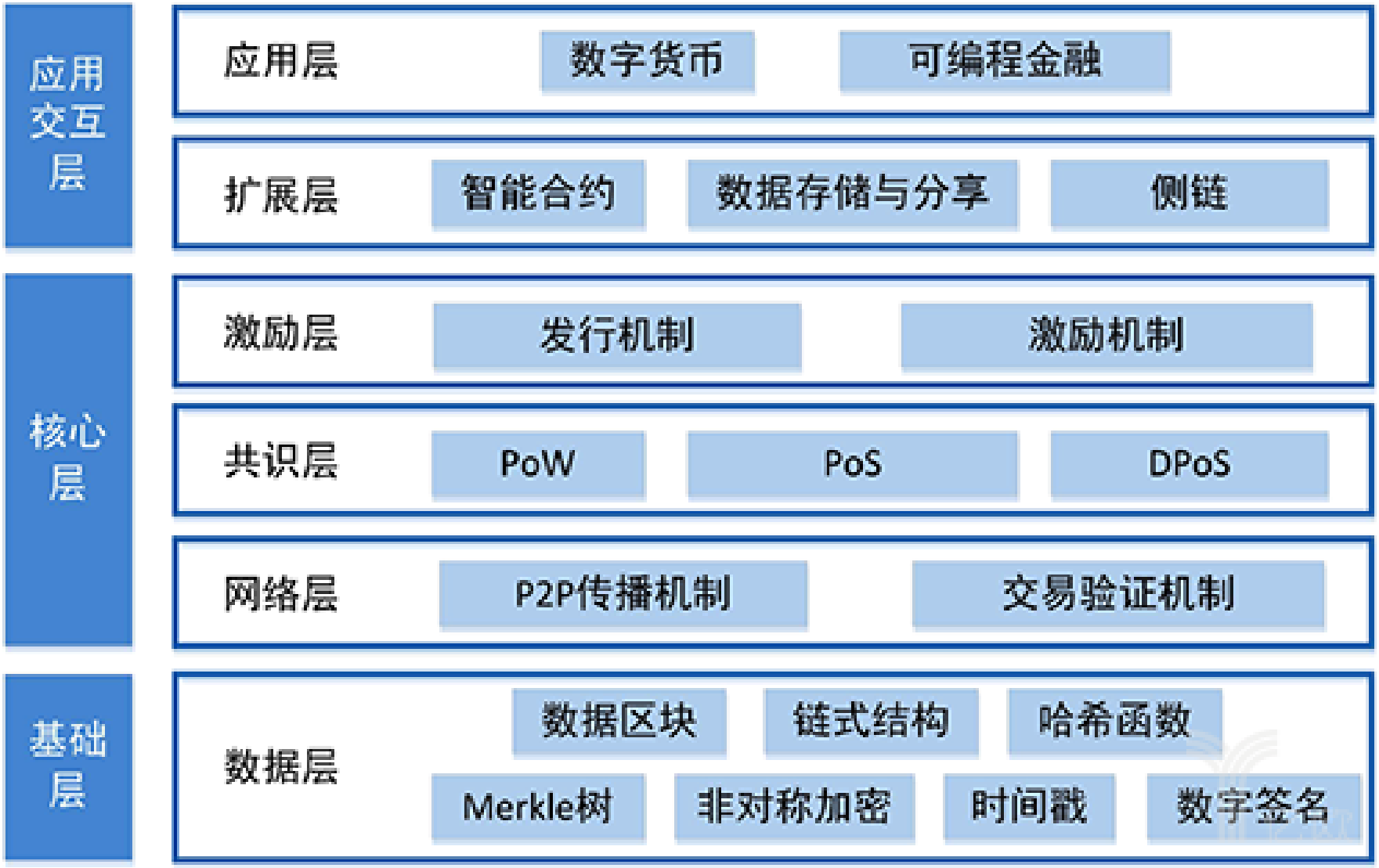
特性举例：存在性证明

- 时间点后向证明
- 时间点后向证明
- 时间区间证明

哪些场景适合使用区块链?

- 基于区块链技术的应用，会用到区块链哪些特性、优势?
- 是否有劣势，甚至硬伤?
- 评估：带来的好处 > 采用的成本+弊端+使用门槛?
- 实施周期、难度、风险?
- 现实情况：大部分处于PoC概念验证阶段，落地难度大，有各种各样问题；企业付费难，政府买单为主；哪些是营销噱头?
- 不要被眼前的难题阻碍，但也不要过于乐观

区块链分层全景图



（来源：CCID）

Node 区块链加速器

4.2 区块链的技术大类：公有链、联盟链、私有链

区块链的分类

- **公有链 public blockchain**：无官方发行机构，参与者自行组成，任何节点都可以随时加入和退出，权利对等。如：Bitcoin，Ethereum，Ripple，Qtum，EOS，等等
- **联盟链 consortium blockchain（许可链 permissioned blockchain）**：不同节点权限不同，如只读节点、可写入节点，需要身份验证。如：Hyperledger Fabric，Fabric改进版（如纸贵Z-Ledger），国产开源BCOS
- **私有链 private blockchain**：建立在某机构内部，规则由机构自己来设定。如由于内部审计，也用于开发过程。可用公链代码搭建
- **混合链 hybrid blockchain**：公有链、联盟链混合

区块链的分类

- **公有链 public blockchain**：无官方发行机构，参与者自行组成，任何节点都可以随时加入和退出，权利对等。如：Bitcoin，Ethereum，Ripple，Qtum，EOS，等等
- **联盟链 consortium blockchain（许可链 permissioned blockchain）**：不同节点权限不同，如只读节点、可写入节点，需要身份验证。如：Hyperledger Fabric，Fabric改进版（如纸贵Z-Ledger），国产开源BCOS
- **私有链 private blockchain**：建立在某机构内部，规则由机构自己来设定。如由于内部审计，也用于开发过程。可用公链代码搭建
- **混合链 hybrid blockchain**：公有链、联盟链混合

区块链的分类

- **公有链 public blockchain**：无官方发行机构，参与者自行组成，任何节点都可以随时加入和退出，权利对等。如：Bitcoin，Ethereum，Ripple，Qtum，EOS，等等
- **联盟链 consortium blockchain（许可链 permissioned blockchain）**：不同节点权限不同，如只读节点、可写入节点，需要身份验证。如：Hyperledger Fabric，Fabric改进版（如纸贵Z-Ledger），国产开源BCOS
- **私有链 private blockchain**：建立在某机构内部，规则由机构自己来设定。如由于内部审计，也用于开发过程。可用公链代码搭建
- **混合链 hybrid blockchain**：公有链、联盟链混合

区块链的分类

- **公有链 public blockchain**：无官方发行机构，参与者自行组成，任何节点都可以随时加入和退出，权利对等。如：Bitcoin，Ethereum，Ripple，Qtum，EOS，等等
- **联盟链 consortium blockchain（许可链 permissioned blockchain）**：不同节点权限不同，如只读节点、可写入节点，需要身份验证。如：Hyperledger Fabric，Fabric改进版（如纸贵Z-Ledger），国产开源BCOS
- **私有链 private blockchain**：建立在某机构内部，规则由机构自己来设定。如由于内部审计，也用于开发过程。可用公链代码搭建
- **混合链 hybrid blockchain**：公有链、联盟链混合

Node 区块链加速器

4.3
应用案例解析

区块链应用分类

1. 数字货币、数字金融
2. 通证经济：更高效、数字化的分配机制，激活系统各参与方活力
3. 行业应用：利用区块链技术解决现实问题、促进生产关系，提高生产效率
4. 企业链改：股改的未来发展方向
5. 互联网基础设施

（以上5项是交叉应用的）

Node 区块链加速器

应用类别1：
数字货币、数字金融

一 加密数字货币

- BTC、BCH、LTC、XRP、Zcash、Monero
- 稳定币：USD Tether，TrueUSD，USDC，PAX，GUSD，BitCNY
- 国家主权数字货币/法定数字货币/央行数字货币（CBDC）：如委内瑞拉石油币、Libra、中国央行将推出的DCEP

可编程货币与数字金融

- 可编程货币：以区块链技术为底层的加密数字货币，可以用运行于其上的程序代码直接实现业务逻辑

- 数字金融：用新一代互联网技术手段（ABCD）改造传统金融的新时代金融体系

数字金融

- 银行跨界结算：建立不同银行间信任，提高结算效率，降低结算成本
- 融资证券：ABS、ICO、STO
- 供应链金融：解决信息不对称，增加供应链中各方及与银行的信任关系，从而提高融资授信效率
- 保险：增强交易及结算的效率和透明度

Node 区块链加速器

应用类别2：通证经济

Token通证

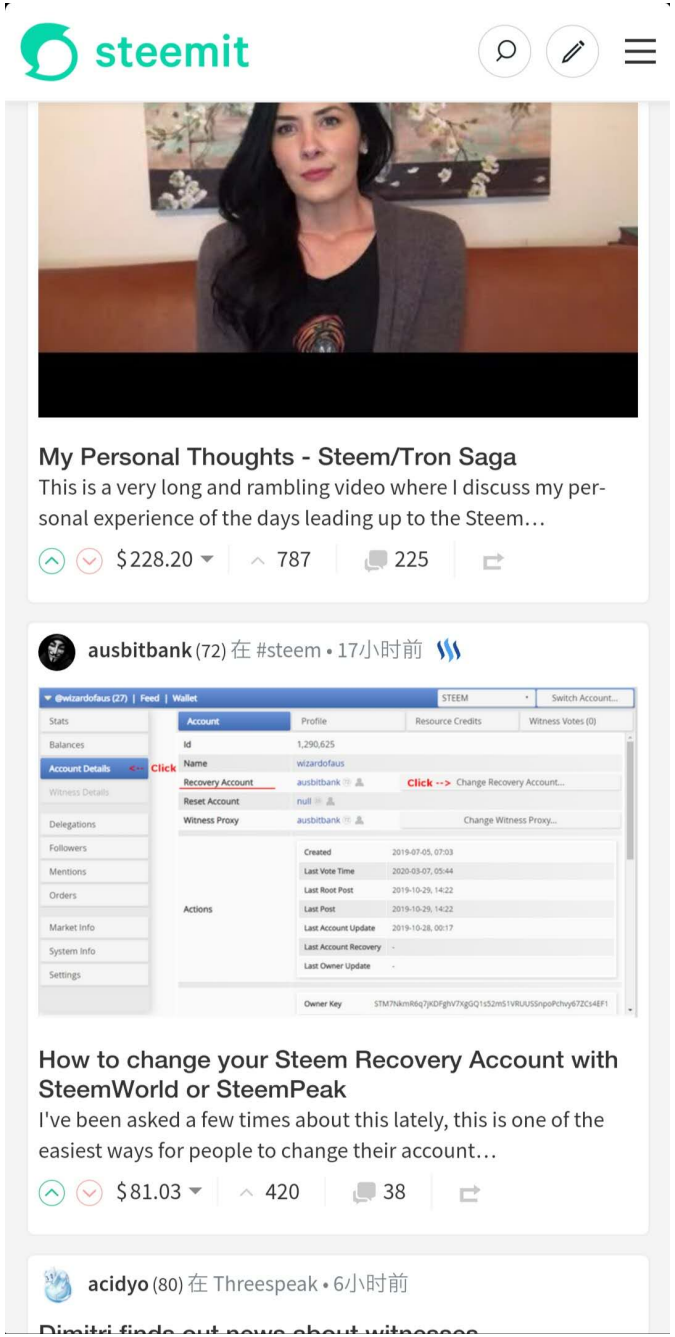
- 通证（Token）即符号，也译为代币
- 可以简化理解为积分，但又优于积分
- 采用有公信力的记账符号达到分配权益给系统各参与方，实现经济激励，激活组织内外部的各方贡献价值
- 是“游戏化设计”理念最佳的实施工具
- 由于以太坊的可编程特性，使得构建具备标准操作接口的Token非常简单

Node 区块链加速器

通证应用举例：Steem

案例：Steem

- http://steemit.com
- 针对Facebook、Twitter、Reddit等社交媒体存在的一个问题：对参与者的贡献没有激励
- 提供有价值内容 -> 得到回报
- 内容、评论点赞、转发、推荐好友加入等



案例：Steem

- Proof of Brain
- 未解决难点：羊毛党
- 为什么不直接用法币（微信现金打赏）？
  - 认知、财务成本等
  - 投票好于付款
  - 降低交易摩擦，提高交易效率
- 由于单一币种体系的“三元悖论”问题，故采用了多币种设计

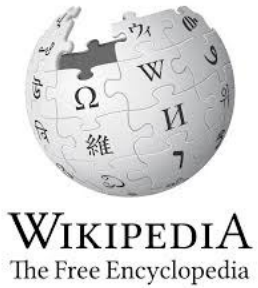
三元悖论（不可能三角）

- 固定汇率
- 资本自由进出
- 独立货币政策

Steem多币种设计

- Steem（STEEM）
  - 目前市值$2.6亿
  - 入场或退出，都要购买或卖出STEEM。购买后，转换为SP或SMD，避免稀释。
  - 每年增加100%供应。每天稀释0.19%（通胀率），但与价格波动相比仍微不足道。
  - 90%的通货膨胀分配给现有STEEM持有人。
- Steem Power（SP）
  - 保护利益长期持有者
- Steem Dollar（SMD）后改为 SBD
  - 稳定币

类似属性的系统



Node 区块链加速器

通证应用举例：游戏道具-Crypto Kitties

Node 区块链加速器

应用类别3：
行业应用

政策风向标

习近平在中央政治局第十八次集体学习时强调 把区块链作为核心技术自主创新重要突破口 加快推动区块链技术和产业创新发展

2019年10月25日 18:21 新华社

新华社北京10月25日电 中共中央政治局10月24日下午就区块链技术发展现状和趋势进行第十八次集体学习。中共中央总书记习近平在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

浙江大学教授、中国工程院院士陈纯就这个问题作了讲解，并谈了意见和建议。

中共中央政治局各位同志认真听取了讲解，并进行了讨论。

习近平在主持学习时发表了讲话。他指出，区块链技术应用已延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域。目前，全球主要国家都在加快布局区块链技术发展。我国在区块链领域拥有良好基础，要加快推动区块链技术和产业创新发展，积极推进区块链和经济社会融合发展。

习近平强调，要强化基础研究，提升原始创新能力，努力让我国在区块链这个新兴领域走在理论最前沿、占据创新制高点、取得产业新优势。要推动协同攻关，加快推进核心技术突破，为区块链应用发展提供安全可控的技术支撑。要加强区块链标准化研究，提升国际话语权和规则制定权。要加快产业发展，发挥好市场优势，进一步打通创新链、应用链、价值链。要构建区块链产业生态，加快区块链和人工智能、大数据、物联网等前沿信息技术的深度融合，推动集成创新和融合应用。要加强人才队伍建设，建立完善人才培养体系，打造多种形式的高层次人才培养平台，培育一批领军人物和高水平创新团队。

习近平指出，要抓住区块链技术融合、功能拓展、产业细分的契机，发挥区块链在促进数据共享、优化业务流程、降低运营成本、提升协同效率、建设可信体系等方面的作用。要推动区块链和实体经济深度融合，解决中小企业贷款融资难、银行风控难、部门监管难等问题。要利用区块链技术探索数字经济模式创新，为打造便捷高效、公平竞争、稳定透明的营商环境提供动力，为推进供给侧结构性改革、实现各行业供需有效对接提供服务，为加快新旧动能接续转换、推动经济高质量发展提供支撑。要探索“区块链+”在民生领域的运用，积极推动区块链技术在教育、就业、养老、精准脱贫、医疗健康、商品防伪、食品安全、公益、社会救助等领域的应用，为人民群众提供更加智能、更加便捷、更加优质的公共服务。要推动区块链底层技术服务和新型智慧城市建设相结合，探索在信息基础设施、智慧交通、能源电力等领域的推广应用，提升城市管理的智能化、精准化水平。要利用区块链技术促进城市间在信息、资金、人才、征信等方面更大规模的互联互通，保障生产要素在区域内有序高效流动。要探索利用区块链数据共享模式，实现政务数据跨部门、跨区域共同维护和利用，促进业务协同办理，深化“最多跑一次”改革，为人民群众带来更好的政务服务体验。

习近平强调，要加强对区块链技术的引导和规范，加强对区块链安全风险的研究和分析，密切跟踪发展动态，积极探索发展规律。要探索建立适应区块链技术机制的安全保障体系，引导和推动区块链开发者、平台运营者加强行业自律、落实安全责任。要把依法治网落实到区块链管理中，推动区块链安全有序发展。

习近平指出，相关部门及其负责领导同志要注意区块链技术发展现状和趋势，提高运用和管理区块链技术能力，使区块链技术在建设网络强国、发展数字经济、助力经济社会发展等方面发挥更大作用。

Node 区块链加速器

存在性证明应用举例：版权

一 版权领域痛点

作家毕飞宇小说《推拿》被侵权仅获赔5万，近年作家屡被侵权

取证难导致作家维权成本高

深圳商报记者 谢晨星

近日，出版界两件侵权案件相继宣判，引发业内关注。作家毕飞宇诉编剧陈梓侵权小说《推拿》一案，毕飞宇及人民文学出版社胜诉，获得5万元赔偿；翻译家马爱农诉中国妇女出版社抄袭译著《绿山墙的安妮》一案二审宣判，维持一审判决，马爱农应获赔3万元。据悉，近年来作家、翻译被侵权案件频发，本报记者专访了相关法律人士，对作家维权进行了支招。

不是第一次被侵权

毕飞宇的小说《推拿》2008年9月由人民文学出版社出版发行，2011年获得第八届茅盾文学奖，至今已经销售近30万册。小说推出之后，已经被翻译成英、法、西班牙、阿拉伯等语言，接连被改编为同名电视剧、话剧和电影。2013年9月3日，人文社与毕飞宇联合向北京市东城区法院提起诉讼，称陈梓出版的同名书籍虽是电视剧《推拿》的剧本，却并未获得毕飞宇的同意，侵犯了毕飞宇《推拿》著作权，同时也混淆市场误导读者，侵犯了人文社的权利。诉讼请求为：1、停止出版发行西苑版《推拿》；2、连带赔偿毕飞宇经济损失20.4万元；3、连带赔偿人民文学出版社经济损失40.8万元及合理支出20129.4元。

对此，毕飞宇表示，“这不是我第一次被这个编剧侵权，当年《青衣》改编成电视剧的时候，陈梓就曾反向改编成小说出版。因为我跟他也认识，所以当年她把《青衣》改编成小说的合同上，我特地加上条款，不准以《推拿》名义出版任何出版物。”

3月19日，法院作出一审判决：判两被告侵权行为成立，应承担停止侵害、赔偿损失的民事责任，“鉴于原告未提供相关损失证据”，对索赔金额不予全额支持，“综合考虑原告作品知名度，被告的侵权程度、过错等因素”，判定被告陈梓毕飞宇经济损失5万元。同时认定两被告未对人民文学出版社构成侵权。

对此判决结果人文社和毕飞宇均感不满。人文社表示，仅判罚5万元，无法对侵权者形成警示作用。同时，认定两被告对人文社不构成侵权，明显为其“免除”责任。毕飞宇和人文社均表示要继续上诉。

侵权成本太低

其实，此类事件在出版界已十分常见。去年，知名编剧李檬出版了《致我们终将逝去的青春》等剧本集，但原著作者辛爽妈表示只授权了原著小说的电影改编权，并未授权将改编剧本再出版的权利；2008年，热播电视剧《马文的战争》的原著作者叶兆言也曾遭遇侵权事件。“叶兆言的小说《马文的战争》被购买了电视剧版权，之后热播的电视剧《马文的战争》和同名小说《马文的战争》，两部作品中都没有提及‘叶兆言’。更早的还有2005年电视剧《暗算》播出后，麦家不满于杨健署名“第二编剧”以及片头无“原著麦媒体上公开向麦家赔礼道歉，并赔偿麦家经济损失6万元。

对此，小说《推拿》的责任编辑赵萍表示，作者叶兆言诉网名电视版编剧陈彬，最后认定陈彬及北大出版社侵权，共同赔偿叶兆言54万余元。“之所以赔那么多，是因为北大出版社比较诚实。我们对陈梓版《推拿》印数的取证却遭遇了阻力，去印厂也拿不到印单。”

去年7月，翻译家马爱农发现中国妇女出版社2012年出版、译者署名“周黎”的《绿山墙的安妮》，与自己1986年翻译的、人民文学出版社出版的同名图书有97.32%的相同内容。对于该案她提出的要求是：被告公开赔礼道歉并支付精神损害抚慰金5万元，赔偿原告经济损失及合理费用12.4万余元。朝阳法院去年12月判定被告停止侵权并赔偿马爱农各项损失共3万元。国觉判罚太轻，马爱农再上诉。3月21日，北京市三中院作出二审判决，结果是“维持原判”。对此，马爱农表示十分失望，“一审判决仅判处被告赔偿3万元。这样的判罚力度，根本没有起到保护正版、打击抄袭的作用。”

对此类事件，记者采访了深圳华途律师事务所的吴昊律师，他告诉记者，维权成本高、侵权成本低是目前著作权纠纷的特点之一。他指出，陈梓因为对毕飞宇的小说进行改编而享有对改编作品的著作权，将剧本出版属于行使著作权的行为。但改编者行使著作权不得侵犯原

约定不明是直接原因

吴律师表示，除了抄袭等故意侵权的情形外，引起著作权纠纷的重要原因之一就是授权使用的范围约定不明。因此他建议，著作权交易各方在作品开始授权时就应该把改编作品的使用方式约定的更加细致、清晰，充分考虑到后续可能的版权链条的各个环节。此外，还可以通过合同明确约定违约责任。一份专业的合同可以更好地保护守约方的利益。

而对于侵权赔偿过低，吴律师表示：由于未看到毕飞宇和马爱农两案的案卷，还无法评价两案的赔偿金额是否过低。他说：“侵犯著作权或者与著作权有关的权利的，赔偿的计算方式有三种：1、以被侵权人实际损失计算；2、以侵权人违法所的计算；3、法定赔偿，由法院根据情况判决给予50万元以下的赔偿。而且三种计算方式的使用是有顺序的，当前一种方法无法计算的时候才能适用后一种方法计算。因此，作者维权时，首先需证明自己的损失，或者想办法查清对方的获利情况。如果权利人的实际损失或者侵权人的违法所得都不能确定的，将由人民法院根据侵权行为的情节，判决给予五十万元以下的赔偿。”对于具体赔偿金额的确定，法官具有自由裁量权，但这种自由裁量需要充分考虑作品的性质、作品（作者）的知名度、作品独创性程度、侵权的主观故意、侵权范围等多种因素。在这些方面，如果原告没有尽到举证义务，也可

■文化看台

数字时代，作家维权难

我国文学界和出版界有了向苹果索取稿酬的计划。中国文学著作权协会会长陈建功说，将联合数十家出版社和报刊社向苹果网上应用商店开展维权行动。

维权

年过六旬的作家陈建功担任中国作家协会副主席，他的作品以“京味儿”著称。上世纪80年代末，他提倡用电脑代替笔来写作。

“当初我所理解的‘电脑’，不过是一个便捷的书写工具，随后又知道它具有通信传输功能，当时我所做的，也就是尝试安装一个调制解调器，用电脑进行点对点通讯而已。当时我还为自己的‘先锋’姿态自鸣得意。”

网络给作家带来方便，也带来烦恼。陈建功说，纷至沓来的刊登者、转摘者令人瞠目结舌，“我们不得不面对着网络侵权盗版更为严重和更加难以控制的局面，还不得不面对数字出版产业发展过程中暴露的许多亟待解决的版权问题。”

2009年，中国文著协曾代表作家和出版社与谷歌和百度谈判。与谷歌的谈判因谷歌退出中国市场而暂告一段落，与百度的谈判于2011年10月达成战略合作协议。目前，它还与亚马逊及中国移动浙江阅读基地、多看科技、超星、汉王科技等国内数字出版企业合作开展维权。

成立于2008年10月24日的中国文著协是文学作品著作权集体管理组织。

难度

中国版权局和国际复制权组织联合会近日在杭州举办“数字环境下的版权集体管理国际研讨会”。有关方面负责人表示，中国著作权集体管理组织不仅要解决传统环境下的版权问题，还要面对新技术带来的问题和挑战。

“去年我们售卖的版权许可费用达到8亿元人民币，中国的人口比英国多20倍，你们收的钱应该比我们多得多。”英国版权许可机构CEO凯文·菲茨杰拉德说。

据了解，中国文著协三年来，累计为200多家文摘类报刊和十来家教育出版社转付给5000多名作者500多万元稿酬。

浙江少儿出版社副总编辑、儿童文学作家孙建江是其中的一位。“前段时间我收到文著协汇来的一笔稿酬，来自于四篇被收入人民教育出版社教材的作品，有一篇作品发表到现在已经快30年了。”

数字时代，版权维权工作更难。中国文著协总干事张洪波说，权利人在数字出版商手里只能拿到低分成的版权收益，而且收益的结算周期很长，出版商的销售数据也不透明，如果要维权，面临着成本大获赔少的困境。“权利人力量分散，各自为战，无法对侵权方构成压力”。

“中国数字出版产业2011年的产值达到1337亿元，但是产业链利益分配不平衡，著作权人利益严重受损，缺乏定价话语权和谈判主动权，新技术方式又使侵权盗版更加猖獗。”张洪波说。

尊重

新闻出版总署版权管理司司长于慈珂认为，公众已习惯了在互联网上享受免费午餐，集体管理组织和网络运营商还没有建立起运行良好的商业模式，难以收取互联网作品的使用费，权利人又不愿意将权利授权给集体管理组织，使后者缺乏代表性，难以有效开展活动。

事实上，中国的著作权集体管理组织最初开展活动时就招致公众质疑。新闻出版总署副署长阎晓宏说，这项制度在中国属于新生事物，很多人没有版权费收取和分配的概念。“一听收费，老百姓就会以为是‘乱收费’，其实这不是财政收费，而是著作权人应得的作品使用费，在尊重知识和尊重创新的大环境下，我们应该大力宣传这些概念。”

最有助于改变现状的工作是立法。阎晓宏说，他所在的部门正在制定教科书法定许可付酬办法和修订出版文字作品报酬规定等。 新华社

数字作品如何确定权利归属？

如何有效进行侵权证据取证？

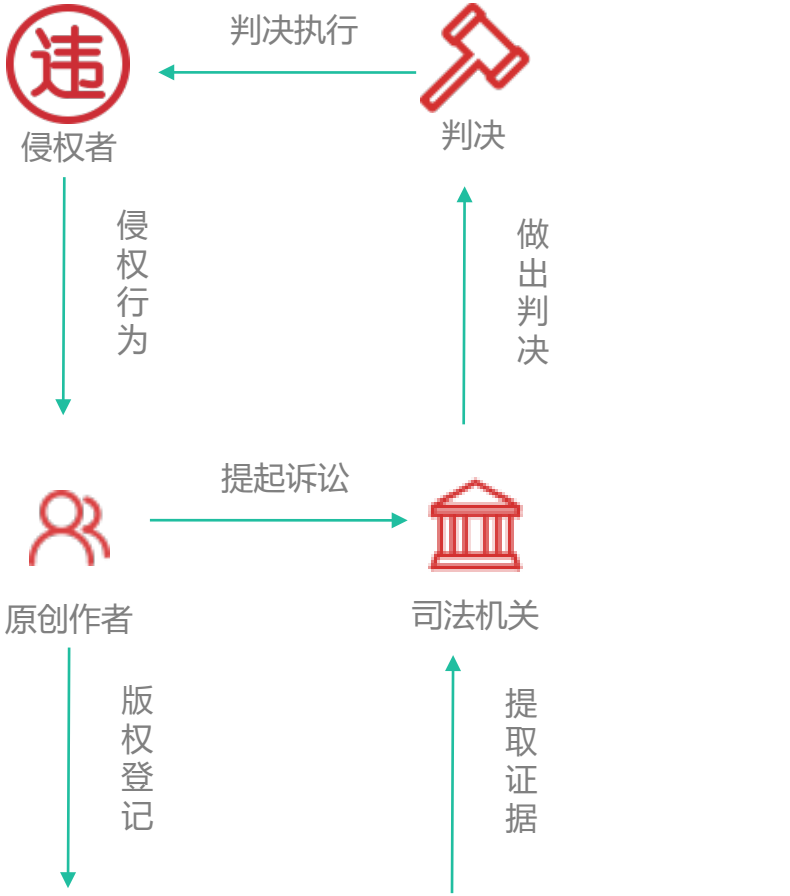
如何针对数字作品快速授权？

如何直观呈现证据法律效力？

区块链版权解决方案

- 目标：创作即确权、使用即授权、发现即维权

纸贵科技 区块链版权产品



不可篡改

法律效力

快速登记确认

Node 区块链加速器

纸贵科技 区块链版权产品

- （1）选择文件、获取数据指纹：选择需要存证的文件，通过哈希算法计算出该文件和关联信息的数据指纹。
- （2）数据写入区块链：在用户确认后，系统将得到的数据指纹写入区块链中，一经写入便无法篡改。
- （3）获取存证结果：根据用户需求生成存在证书供用户保留，也可根据用户需求，提供纸质书面报告。
- （4）数字指纹验证：根据客户需求，在用户需要对存证的指纹进行验证时，提供数字指纹比对查询。

纸贵科技 区块链版权产品

- （1）侵权取证：
- 当发现侵权行为时，快速调用版权服务中的侵权取证接口，对侵权网站进行页面抓取取证，并将取证结果保存在联盟链中；系统对侵权URL地址进行域名解析，通过预言机服务将URL对应的侵权内容进行存储，并生成可供第三方检测的存证过程合理性证据，将侵权行为固化为证据进行保存；固化后的证据保存在区块链中，数据永久存储且不可篡改，符合法律对电子证据的要求。
- （2）侵权追踪：
- 对于已进行侵权存证操作的侵权内容，版权服务提供持续性的侵权监控，侵权追踪等服务，确保侵权方对于侵权内容采取相应处理

Node 区块链加速器

存在性证明应用举例：教育

区块链教育行业应用：成绩单上链

往届学生成绩会从系统删除

只有固定人员可查看成绩

成绩单造假普遍、成本低

人为改动成绩

传统成绩单痛点

永久存档

随时可查

上链后的成绩单

不可伪造

不能非法篡改

区块链教育行业应用：成绩单上链

本科生成绩单

姓名：
学院：

入学年月：　学号：　学制：4年制　专业：　已完成学分：
出生日期：　性别：男　学分成绩：　专业班：　应修读学分：

课程	学分	成绩
第一学年（2014-2015）第一学期		
专业教育（）	0.3	90
军事理论	2	64
军事训练	1	通过
图学基础与计算机绘图	2	40
大学体育（）	1	69
大学英语（）	4	71
思想道德修养与法律基础	3	58
计算机导论与程序设计基础	5	66
第一学年（2014-2015）第二学期		
大学物理（Ⅱ）	5	61
大学生心理健康教育	1	良好
大学英语（Ⅱ）	4	65
形势与政策（Ⅱ）	0.3	80
物理实验（）	1	及格
程序设计基础课程设计	1	优秀
马克思主义基本原理	3	73
第二学年（2015-2016）第一学期		
中外名曲鉴赏	2	0
军事训练	1	通过
国家英语四级	1	372
大学体育（Ⅱ）△	1	60
大学生职业发展	1	95
形势与政策（）	0.3	通过
新生研讨课	1	优秀
舞蹈鉴赏	2	0
第三学年（2016-2017）第一学期		
专业教育（Ⅱ）	0.3	85

课程	学分	成绩
中国近现代史纲要	2	61
兵学与中国文化	2	0
大学英语（Ⅲ）	4	60
实验实践能力达标测试（Ⅰ理工类物理）	0.3	不及格
实验实践能力达标测试（Ⅰ理工类计算机）	0.2	不及格
形势与政策（Ⅲ）	0.3	70
电路、信号与系统实验（）	0.5	0
离散数学（）△	3.5	60
西方美学史	2	0
金工实习	2	良好
第三学年（2016-2017）第二学期		
大学体育（Ⅳ）	1	0
大学物理（）△	3	60
大学英语（Ⅳ）	4	60
形势与政策（Ⅳ）	0.3	通过
数据结构△	4	60
概率论与数理统计△	3	60
毛泽东思想和中国特色社会主义理论体系概论	6	64
物理实验（Ⅱ）△	1	0
电子线路实验（）	1	0
电路、信号与系统实验（Ⅱ）	0.5	0
高等数学A（）△	6	60
第四学年（2017-2018）第一学期		
专业教育（Ⅲ）	0.2	70
信号与系统△	4	60
大学体育（Ⅳ）△	1	0
形势与政策（Ⅴ）	0.3	0
微机原理与系统设计	3	0

课程	学分	成绩
操作系统课程设计	1	0
数字电路与逻辑设计△	3	7
无人机系统导论	2	81
模拟电子技术基础△	4	60
电子技术应用课程设计	1	0
电子线路实验（Ⅱ）	1	0
电装实习	1	良好
线性代数△	3	60
计算机组织与体系结构课程设计	1	0
计算机通信与网络	4.5	8
高等数学A（Ⅱ）△	6	60
第四学年（2017-2018）第二学期		
大学体育（Ⅳ）△	1	0
实验实践能力达标测试（Ⅱ）	0.5	不通过
就业指导	1.5	通过
形势与政策（Ⅵ）	0.3	通过
微机原理与系统设计△	3	0
微机原理与系统设计课程设计	1	0
操作系统△	4	60
数据库系统△	3	60
物理实验（Ⅱ）△	1	0
电路分析基础△	4	60
离散数学（Ⅱ）△	2	60
科技制作-3	1.5	通过
第五学年（2018-2019）第一学期		
大学体育（Ⅲ）△	1	60
大学体育（Ⅳ）△	1	0
编译原理△	3	60

备注：左侧为链上生成的成绩单主页面；
右侧为扫码后跳转的具体成绩页面。（以学生四年总成绩为例）

Node 区块链加速器

存在性证明应用举例：遗嘱

存在性证明应用：遗嘱

- 遗嘱是合约的一种
- 初级阶段：遗嘱内容的存在性证明，取代传统纸质合约、公证
- 终极阶段：围绕数字资产的智能合约执行

其他存在性证明应用

- 统计数据（如：新冠病毒疫情）
- 公益慈善（如：捐款数据公开）
- 合同（非智能合约）
- 房契
- 国土边界

Node 区块链加速器

区块链行业应用举例：摇号

区块链应用举例：摇号

- 买房摇号
- 上学摇号
- 抽奖
- 核心不在于技术，在于利益和法律

Node 区块链加速器

区块链行业应用举例：医疗

区块链+医疗

- 解决：
  - 1.数据所有权问题
  - 2.信任问题（个人与机构间，机构与机构间）
  - 3.利益问题

区块链+医疗

- 医疗健康数据
- 临床实验数据
- 隐私数据交易和使用的监管
- 医疗设备/药物溯源
- 科学研究数据共享
- 保险计费、理赔

医疗健康、数据交易领域案例：Nebula Genomics

- Nebula Genomics: Blockchain-enabled genomic data sharing and analysis platform
- 基因数据共享和分析平台

Nebula Genomics

Blockchain-enabled genomic data sharing and analysis platform

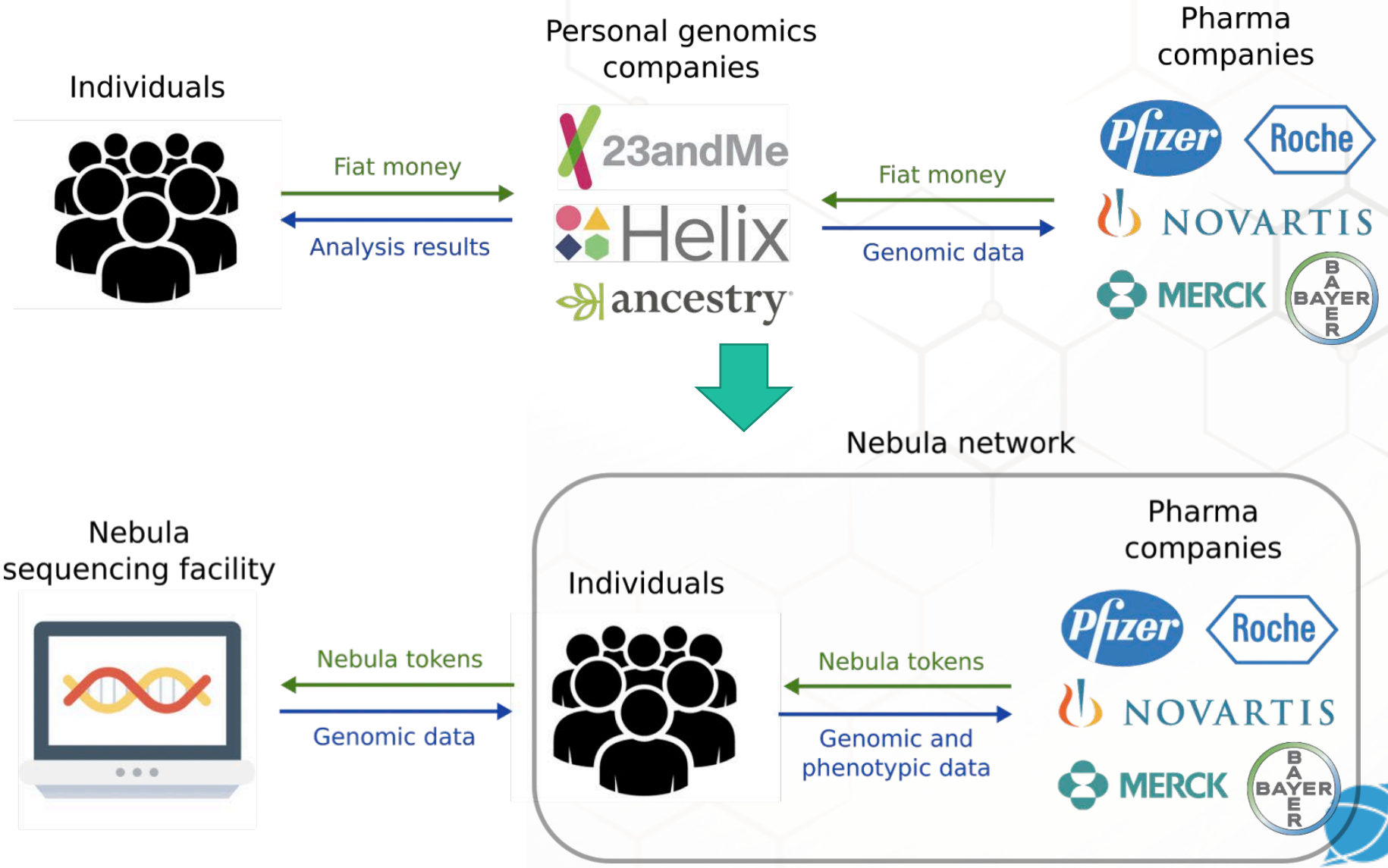
Dennis Grishin
Kamal Obbad
Preston Estep
Mirza Cifric
Yining Zhao
George Church

v4.52
02/07/2018

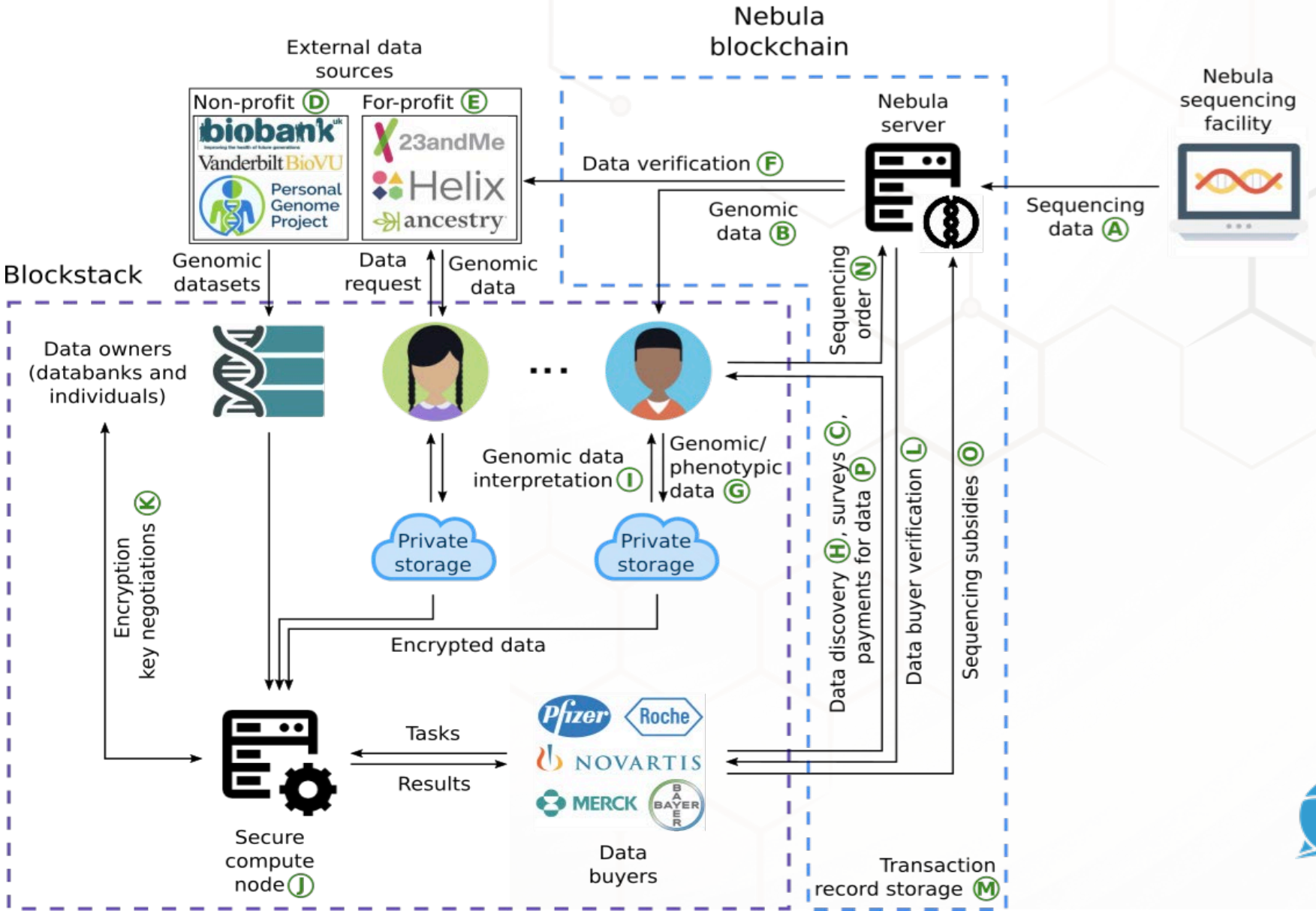
Nebula Genomics：解决的问题

- 目前基于测序成本低于1000美元，未来几年将降至100美元。个人测序将普及，并对医学诊断、疾病研究、个人护理产生帮助
- 基因数据的价值：研究人员共享将对疾病发现、新药物研发有积极促进
- 用户掌控本该属于自己的数据：用户可以选择是否出售自己的数据（可以脱敏）
- 降低测序成本：数据需求方直接采购个人基因数据（没有中间商赚差价），用户获得相应回报，抵消部分的基因测序成本
- 定义标准数据格式，解决数据不兼容问题
- 加快数据流转，发挥数据价值
- 基因海量数据处理：需要更高效的算力，数据传输（约200G/人）

Nebula Genomics：改变目前行业商业模型



Nebula Genomics：技术架构



Node 区块链加速器

区块链行业应用举例：司法

区块链+司法：3个层面

1. 应对区块链引发的一系列新的法律问题：

- 加密货币成为新型犯罪工具（深网、暗网，如洗钱、非法交易工具）、新兴募资方式（易导致非法集资）、产业合规性及监管（数字货币交易所、挖矿）
- 对立法、司法、执法提出新挑战，既要加强监管，又不能扼杀技术发展

区块链+司法：3个层面

2. 区块链作为技术工具，其如下特性可提供案件证据和鉴定标准：

- 存在性证明（时间戳、不可篡改），可追溯，自审计，智能合约

区块链+司法：3个层面

3. 区块链为法律行业自身使用的信息系统提供支撑技术：

- 案件信息的上链，公开透明（自证），法律行业数据共享流通平台

Node 区块链加速器

区块链行业应用举例：溯源

Node 区块链加速器

应用类别4：企业链改

企业链改

- 企业资产上链、流通和变现
- 从股改到链改：解决绝大多数企业由于不能上市导致股份不能流通的问题
- 需要监管政策及法律的健全，不然会引入合规风险

Node 区块链加速器

应用类别5：
互联网基础设施

区块链应用：互联网基础设施

- Namecoin
- IPFS、Filecoin
- Orchid
- Telegram
- 算力交易

区块链应用总结

- 区块链不是万能的，要理性区分
- 区块链的“共识协议”是建立在机器的共识算法上，试图建立人的共识
- 区块链需与传统IT系统融合
- 要洞察“潜在需求”
- 经济可行性是根本
- 行业落地需要长期试错迭代，要有耐心
- 潜力不可估量，志存高远、活在当下

4.4 技术挑战和热点方向

技术挑战和热点

- 挑战：扩展性、性能
- 目的：解决拥堵，提高负载能力，降低系统成本
- 方案：
    - 大区块：BCH倡导
    - 分片（sharding）：ETH倡导
    - 二层扩容
    - 侧链
    - 更好的共识协议

技术挑战和热点

- 挑战：更好的共识协议
- 目的：提高性能、降低成本、适用于应用场景
- 方案：
    - PoW
    - PoS、PoW+PoS
    - DPoS
    - PBFT
    - Tendermint
    - Algorand
    - 可插拔共识协议
    - 甚至改变区块链底层架构：DAG，Hashgraph

技术挑战和热点

- 热点：隐私保护及密码学应用
- 目的：隐私保护、数据安全性
- 方案：
    - 环签名
    - 零知识证明
    - 同态加密
    - 抗量子密码
    - 国密

技术挑战和热点

- 挑战：跨链
- 目的：实现资产的跨链流动，价值的无界传输
- 方案：
    - 公证人机制
    - 侧链/中继
    - 哈希锁定

技术挑战和热点

- 挑战：预言机 Oracle
- 目的：实现链上与链外世界（包括物理世界）的数据交换

技术挑战和热点

- 热点：去中心化身份（Decentralized Identity，DID）
- 目的：用户隐私，身份复用

技术挑战和热点

- 挑战：系统安全
- 目的：防止攻击，保障高可用性

技术挑战和热点

- 挑战：合约程序正确性
- 目的：防止代码逻辑或实现漏洞导致的安全问题，包括资产损失等
- 方案：
    - 软件开发工具
    - 形式化方法（程序自动化验证）：定理证明、模型检测
    - 第三方审计（包括逻辑功能审计）

Node 区块链加速器

4.5
技术之外的挑战

技术之外的挑战

- 区块链更大的挑战不是技术
  - 诈骗项目、投机者众多，引发整个行业遭广泛质疑
  - 合规合法问题
  - 行业采纳的风险顾虑
  - 人才匮乏
  - 资本市场的贪婪与短视
  - 。。。

Node 区块链加速器

课后作业

课后作业（三选二）

1. 举一个当前在讨论的区块链应用案例，简要分析其用到的区块链特性，其优势及劣势。
2. 想一个普通用户使用的具体产品 idea，可以用到区块链的特性（比如可以是现有互联网产品的改造），并基于区块链设计为简要的系统（只写简单的设计方案）。
3. 区块链在本次新冠病毒防控中能发挥什么作用？

Node 区块链加速器

扩展阅读

参考资料（本次课）

Nebula Genomics 白皮书

《区块链溯源应用白皮书(1.0 版本)》 by 可信区块链推进计划

Orchid 白皮书： https://orchidprotocol.com/whitepaper.pdf

区块链中的随机数
https://mp.weixin.qq.com/s/-yrmyEsKjZiCUxgY1CMuKQ

参考资料（增加中）

《浪潮之巅（第3版）》（吴军）

《信息系统的发展与创新》（蔡希尧）

《科技想要什么》（凯文·凯利）

《Mastering Bitcoin（精通比特币）》 2nd Edition

《密码工程实践指南》

《为什么我们的钱变薄了》（罗斯巴德）

《人类简史》（尤瓦尔·赫拉利）

《 商业游戏化：从入门到精通实战指南 》