因为相信，所以遇见

区块链的确定性与不确定性

分享人：胡成武

目录

CONTENTS

01

最小知识集

1 最小知识集-本章内容

1.1 最小知识集-区块链基础

狭义定义

一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构， 并以密码学方式保证的不可篡改和不可伪造的分布式账本。

广义定义

利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式

1.1 最小知识集-区块链基础

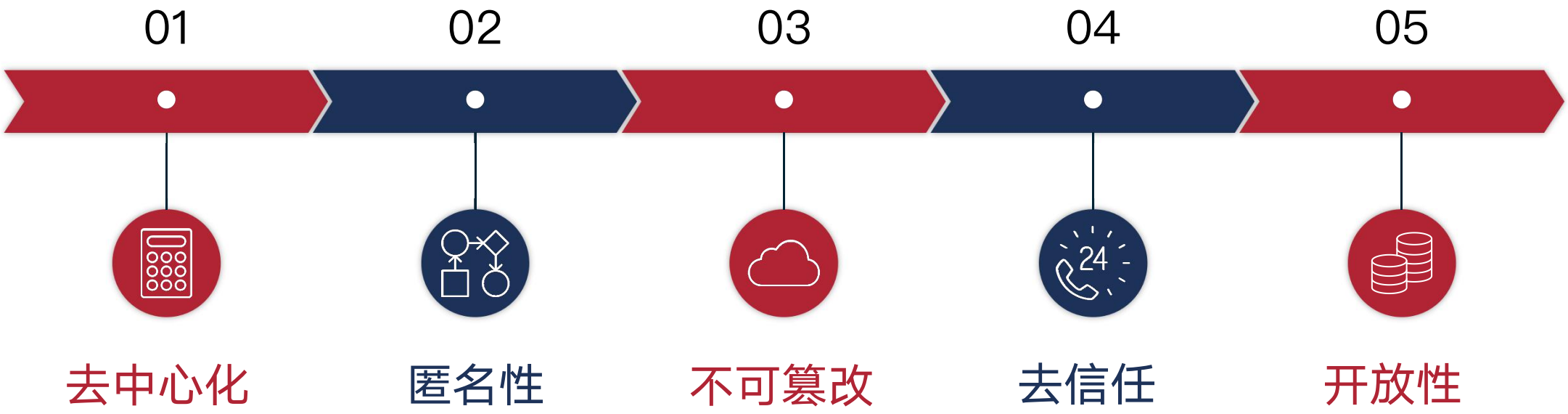
共识算法

共识机制用于解决分布式系统的一致性问题，其核心为在某个协议(共识算法)保障下，在有限的时间内，使得指定操作在分布式网 络中是一致的、被承认的、不可篡改的。在区块链系统中，特定的共 识算法用于解决去中心化多方互信的问题。POW:工作量证明、POS:权益证明、DPOS：委托权益证明。

智能合约

智能合约是一种用计算机语言取代法律语言去记录条款的合约。智能合约可以由一个计算系统自动执行的传统合约的数字化版本。
与传统的合约相比，智能合约有三大特点:数据透明、不可篡改、永久运行。

1.2 最小知识集-区块链特性



1.3 最小知识集-区块链分类

公有链

公有链是指全世界任何人都可读取、发送交易，且交易能获得有效确认的、也可以参与其中共识过程的区块链。

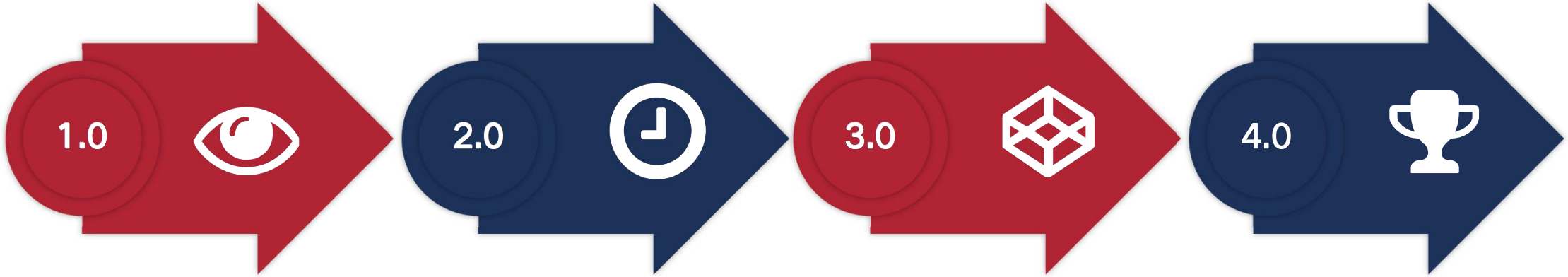
联盟链

联盟链是指由某个特定群体的成员和有限的第三方参与区块生成及节点验 证的区块链。化的特征。

私有链

私有链是指区块链的写入权限仅掌握在某个人或某个组织手中，数据的访问以及编写等有着十分严格的权限。

1.4 最小知识集-区块链发展



数字货币

2009年1月3日比特币诞生，以比特币为代表的数字货币阶段。

智能合约

2013年末以太坊白皮书发布。用户可以基于其智能合约开发各种应用。可编程区块链。

分布式社会

2018年越来越多的应用落地，区块链应用元年。区块链进入可编程商业经济阶段。

大融合

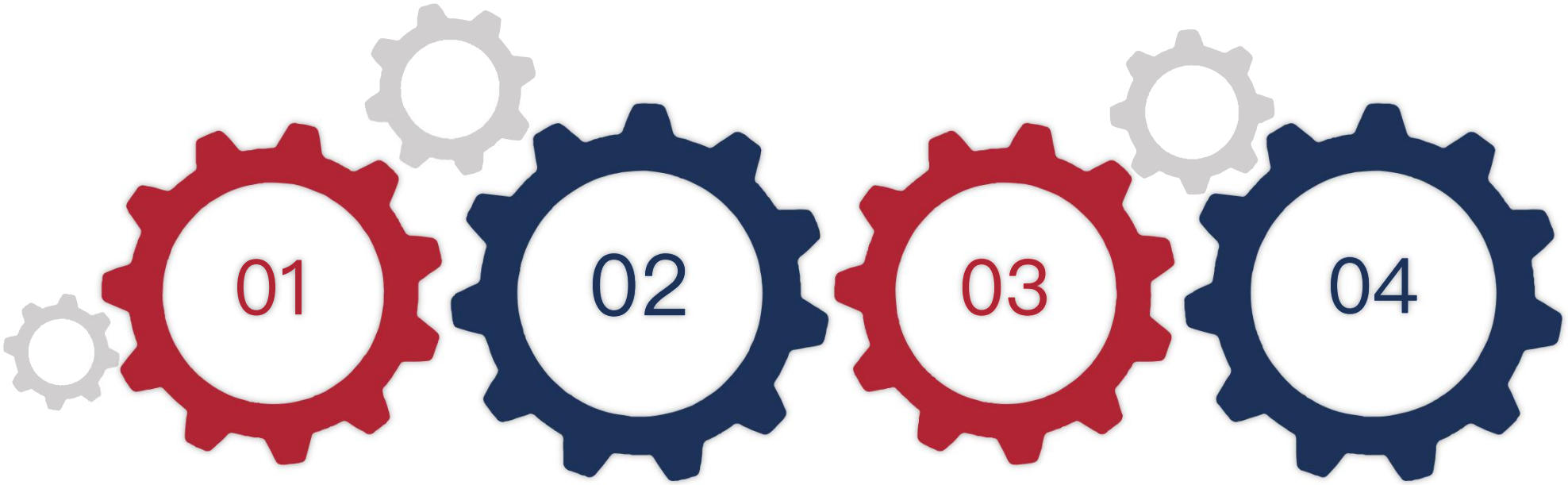
未来10年（可能更久），以超级计算、物联网、大数据、人工智能、区块链（跨链）等技术大融合阶段。

02

场景与应用

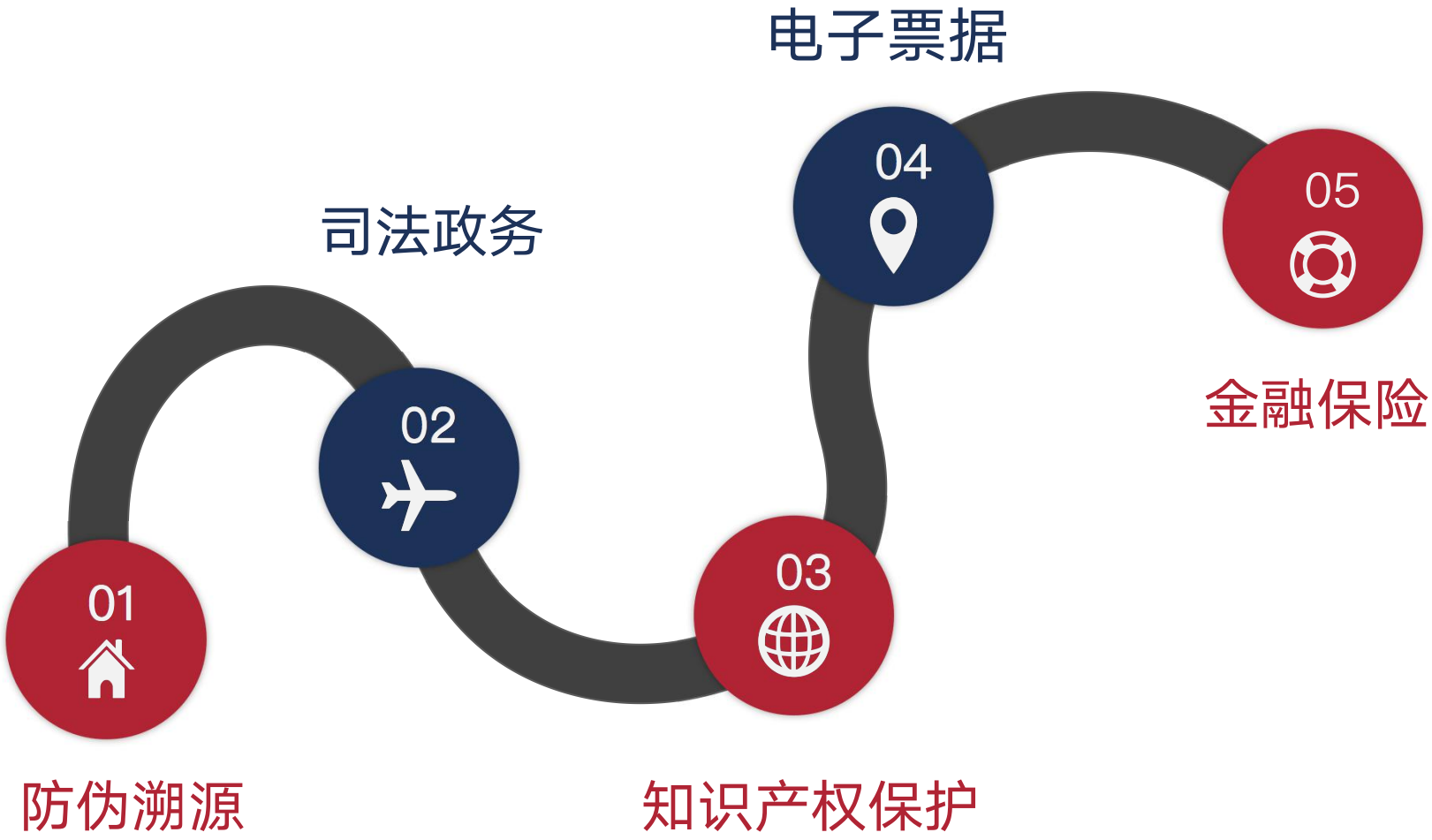
2 场景与应用-本章内容

2.1 场景与应用-不需要区块链



无数据存储	非公开透明	唯一写入人	无需可信第三方
单机小游戏、小工具	国家安全、商业机密	单机版的个人程序	面对面交易

2.2 场景与应用-适合区块链



2.2.1 场景与应用-防伪溯源

溯源，是一种追溯根源行为，通常是指物品或者信息在**生产**、 **流通**、**传输**的过程中，获得物品或者信息的关键数据，把数据按照一定的格式和方式进行**存储**。通过正向、逆向查询存储的相关数据，就可以对物品信息进行**追溯根源**。

溯源可以实现所有批次产品从原料到成品、从成品到原料 100%的双向追溯功能。溯源最大的特色就是数据的安全性，每个人工输入的环节均被软件实时备份。

溯源系统建立后，一旦发生相关事故，监管人员就能够通过该 系统判断企业是否存在过失行为，企业内部也可借助该系统查找是 哪个环节、哪个步骤出现了问题、责任人是谁，避免了由于资料不全、责任不明等给事故处理带来的困难，使问题得到更快的解决

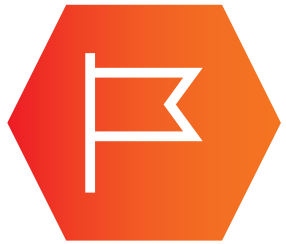
2.2.2 场景与应用-知识产权保护-行业痛点

确权效率低

寻求本国知识产权行政部门对自己作品的权属进行确认，即到国家版权局登记。

确权成本大

作品著作权收费标准是100元起、通常登记单件作品的市场价需要 500 多元。对于短小文章或单幅摄影作品而言，成本显然就较高了。



举证维权难

如果作者将侵权人诉至法院时，网站已删除该涉案作品，作者在没有提前通过公证机构固定证据的情况下，就较难获得胜诉。

2.2.2 场景与应用-知识产权保护-区块链解决方案

确权

原创者把自己的作品上传到区块链，会把原创作品计算哈希值，再加盖时间戳上传到链上。这样你的作品会有一个唯一标志，作品哈希值会同步到区块链上的所有节点上。

行权

可以利用区块链技术构建一个版权交易平台，作品使用权的流转都会被追踪，交易过程透明公开可溯源，使内容创作者的数字内容价值得以体现。

维权

由于区块链的去中心化、不可篡改等特性，所以原创作者通过提交其在链上的哈希值确认其知识产权，大大增强其可信度，现实中也会被法院采纳为证据。

03

通证经济学

3 通证经济学-本章内容

3.1 通证经济学-基础概念

什么是通证

通证的本质是可流通的加密数字权益证明。是社群基于某种共识的基础上，以数字形式存在的权益凭证。

通证生态经济体

在利益相关方组成的生态之间使用通证作为媒介进行激励，以确保其社群生态自组织正反馈自生长，完成社群的熵减以及社群体福利最大化。相对于当前互联网的烧钱模式，**通证生态经济体能够用未来的经济收益作为今天的激励**。

3.2 通证经济学-通证属性

通

代表流动性和通用性。流动性：全球、全时。通用性：类股权、类债权、类物权、通证一切。

证

价值共识的基础。通过加密算法以及分布式共识机制，让通证具有可追溯不可篡改特性。

值

理论上非必须，但是现实商业中，没有它，就没有通证存在的意义。

3.3 通证经济学-通证思维

01
共享共赢

通证的本质是合理的分润，利益重构。首先是分，其次是分什么：通证生态体股权、债权、物权。怎么分：行为挖矿、消费挖矿或者交易挖矿。

02
共建共治

分布式思维的本质是权、责、利的去中心化。比如上市公司引进外部董事。

03
代码即法

代码即通证世界的法律。合约的代码化，通过代码来约束合约的执行。

04
共识性

通证生态体是以社群共识为基石进行构建的。如果共识破裂，则链可能分叉，通证价值降低或者归零。

3.1 通证经济学-通证与区块链

生产力与生产关系

区块链解决信任的问题，他试图构建一个低摩擦系数的世界，属于生产力范畴；而通证则是重构利益分配，属于生产关系范畴。

彼此独立

并非所有的区块链系统都需要通证，其绝非必须。

相互支撑

通证的安全性需要以密码学位基础的区块链的保证。通证则使区块链可以进行可靠的价值传输与交换。

04

确定性与不确定性

4 确定性与不确定性-本章内容

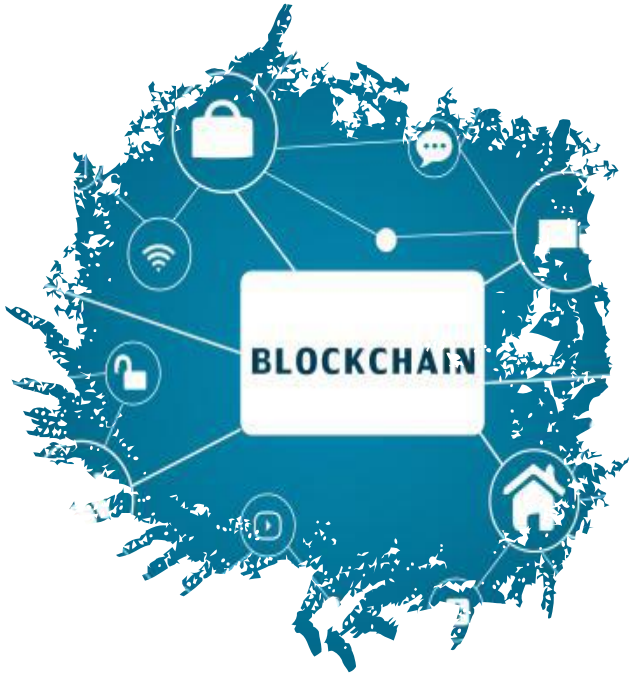
4.1.1 确定性与不确定性-确定性-政策确定性

2018年5月28日习近平总书记在在中国科学院第十九次院士大会、中国工程院第 十四次院士大会上的讲话指出“以人工智能、量子信息、移动通信、 物联网、区块链为代表的新一代信息技术加速突破应用”，对区块链 应用给予了极大的肯定。多地政府以专项基金、资源形式予以大力支 持，促进区块链应用的快速落地。

2019年10月24日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。**区块链已经上升为国家战略。**

4.1.2 确定性与不确定性-确定性-技术确定性

区块链是一整套算法加密体系的结合，属于底层的可信数据建 设基础设施，可以在众多领域得到广泛的应用。未来随着**链上扩容**（出块速度、区块容量、分片）、**链下扩容**（侧链、隔离见证、闪电网络）等技术方案的落地，其性能将大大提高。而基于混币、环签名、零知识证明等技术方案也将极大的提高区块链的**安全与隐私保护**性能。



4.1.3 确定性与不确定性-确定性-应用落地加速

在国家各相关部委、政策的支持下，越来越多的国企、央企以及大型金融、互联网企业参与区块链技术研究与应用落地试验。其中包含：中国移动、国家信息中心、中国银联、中国联通、国家电网、中信银行、中国银行、民生银行、平安银行、腾讯、阿里、百度、京东、网易等。

杭州区块链公司：公信宝、巴比特、比原链、英特链、EOS原力、秘猿科技、趣链科技、复杂美、云象等。

4.2 确定性与不确定性-不确定性

监管不确定 01

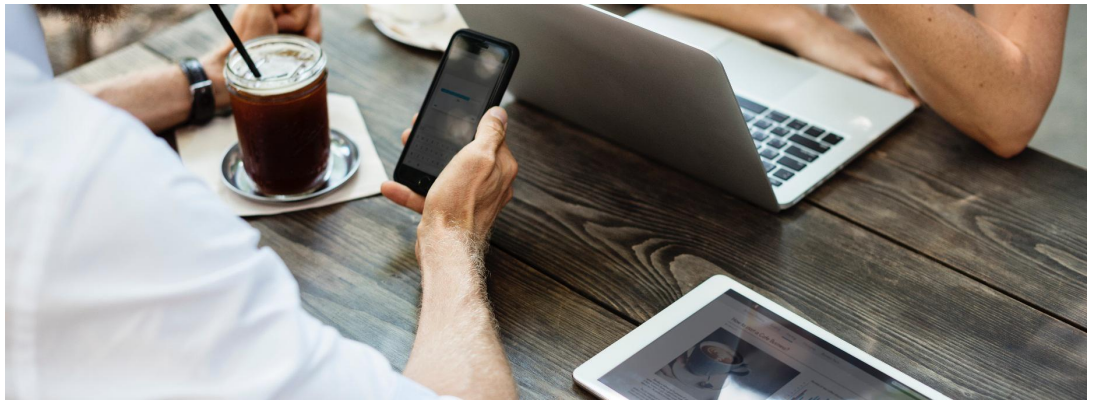
数字货币、隐私保护、数据交易、客户知情权(KYC)和反洗钱(AML)法律.

算力集中 02

当前比特币、以太坊等主流POW共识币种算力集中，导致其去中心化特性变弱。

分叉:共识危机 03

区块链既然是不可篡改的，那么为何可以分叉？由矿工团体创建BCH、The DAO。



4.3 确定性与不确定性-如何应对

世界唯一不变的就是变，
积极拥抱变化。

趋势的力量：资产证券化到
资产通证化

不确定的乐观主义

悲观者正确、乐观者成功

Thanks

大部分人因为遇见所以相信，少部分人因为相信所以遇见