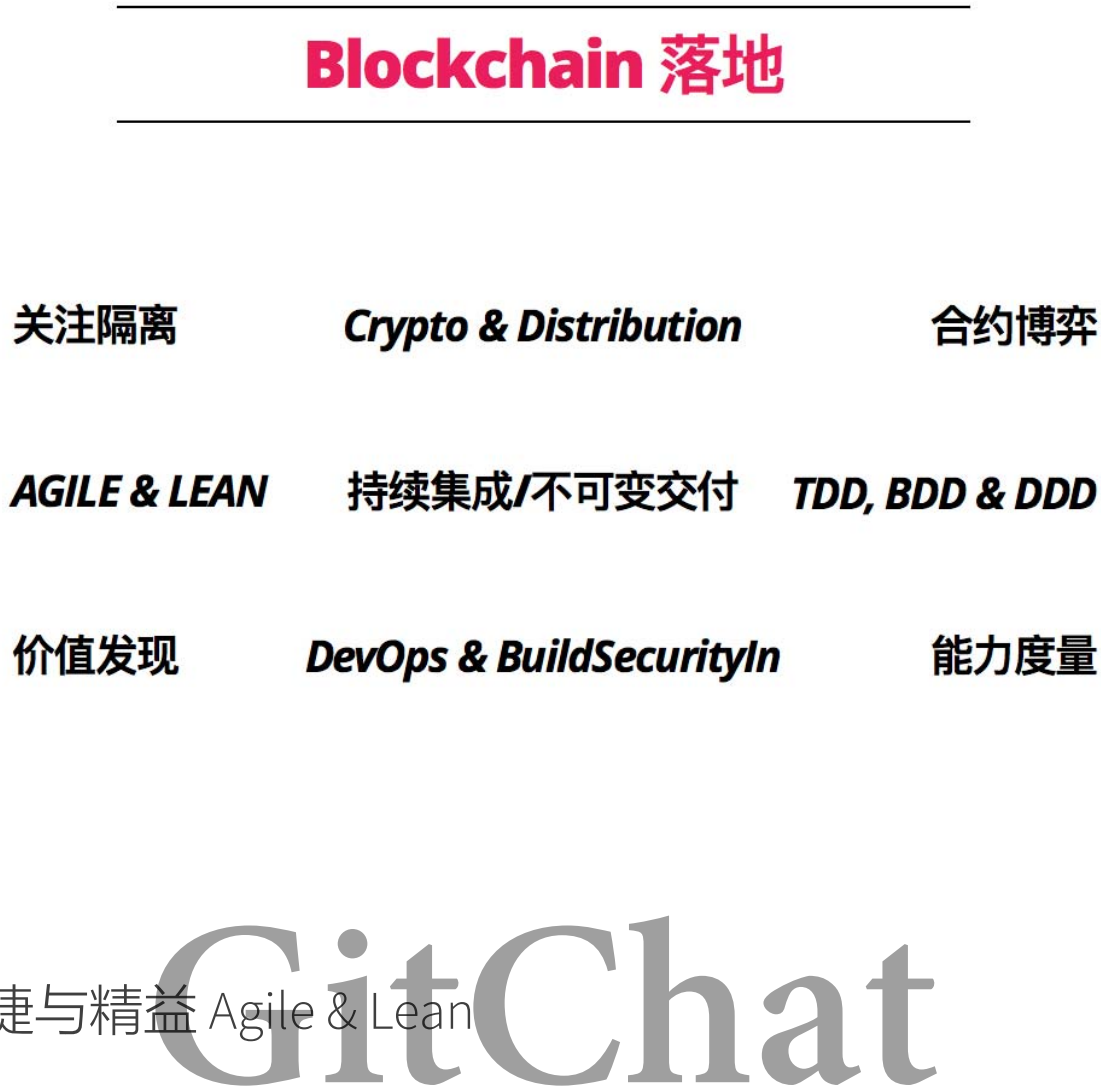
区块链落地中的九大问题与解法

ThoughtWorks与其卓越的客户群一直以领导数字化创新，用实践带来变革为己任，在区块链领域也不例外，我们和客户一起在一些领域，如供应链、小微企业金服等，探索了区块链产业化的方案，并且通过探讨和实践总结出端到端落地的方法。本文希望通过分析区块链落地的现状和问题域，结合区块链的核心价值与工程实践，分享我们在区块链创新中的关键活动与最佳实践。

随着行业关注度的提升，区块链从“黑科技”中脱胎换骨，一跃成为炙手可热的技术新星，但是区块链的落地仍然存在许多的问题。区块链虽然是一门新兴技术（尽管其依赖的密码学和分布式技术早已在其他系统中使用许久），区块链的落地，本质上仍然是软件开发与交付运营的过程，面对这些问题，我们希望能采用ThoughtWorks在实践中总结出的最合适的过程方法去帮助区块链应用落地。

在和客户的交流与对行业的观察中，我们总结出这样几个现状：

针对区块链的落地现状，我们总结出了下列九大问题域，并且在几个项目上做了验证。

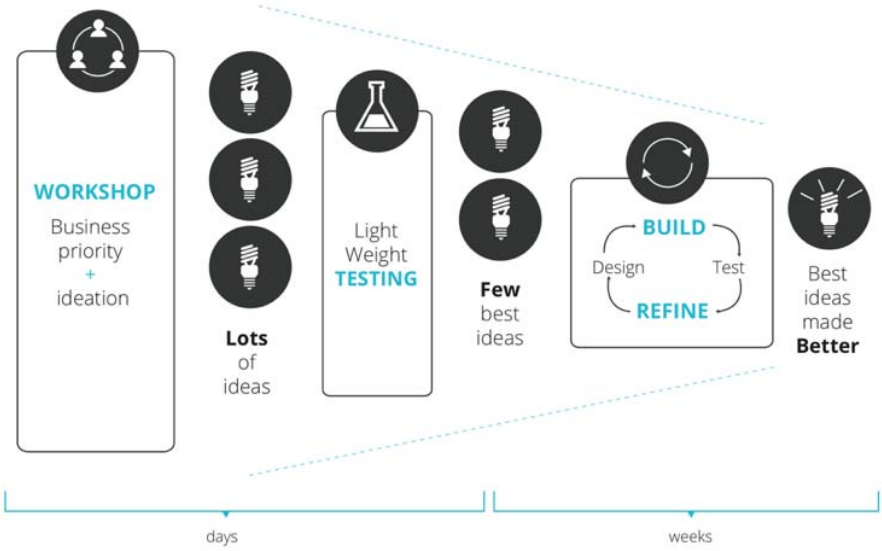


敏捷与精益 Agile & Lean

首先，我们认为敏捷和精益的方法，在区块链的开发与落地仍然适用，众所周知敏捷与精益都需要通过快速反馈，获得系统和项目的运作状态，并且依据其现状制定对策，而区块链应用中，由于其落地实践并不多，更加需要通过反复迭代回顾的方式推进项目落地。

Agile & Lean

我们的持续创新方法，从市场出发，
识别、测试、提炼最佳的与愿景匹配的 blockchain 实践和创意

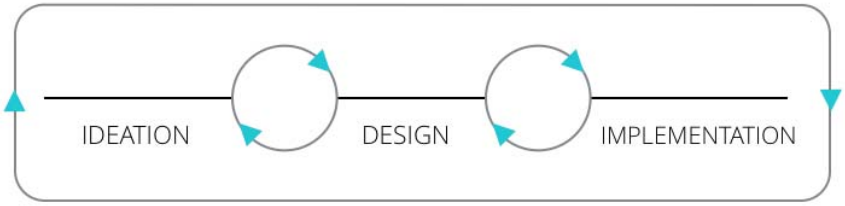


此外我们也需要从市场出发，由商业模式驱动出区块链落地的具体方案，并且在识别、测试、提炼的过程中，寻找区块链的价值点。

端到端的区块链创新实践

全面完整的端到端服务，
覆盖 blockchain 创新产品的整个生命周期

- Decentralized Thinking
- Product Research
- Architecture Assessment
- Innovation Workshops
- Prototyping
- User Testing
- Co-Design Workshops
- Blockchain Application Development
- Cloud-based DevOps
- BuildSecurityIn® Blockchain



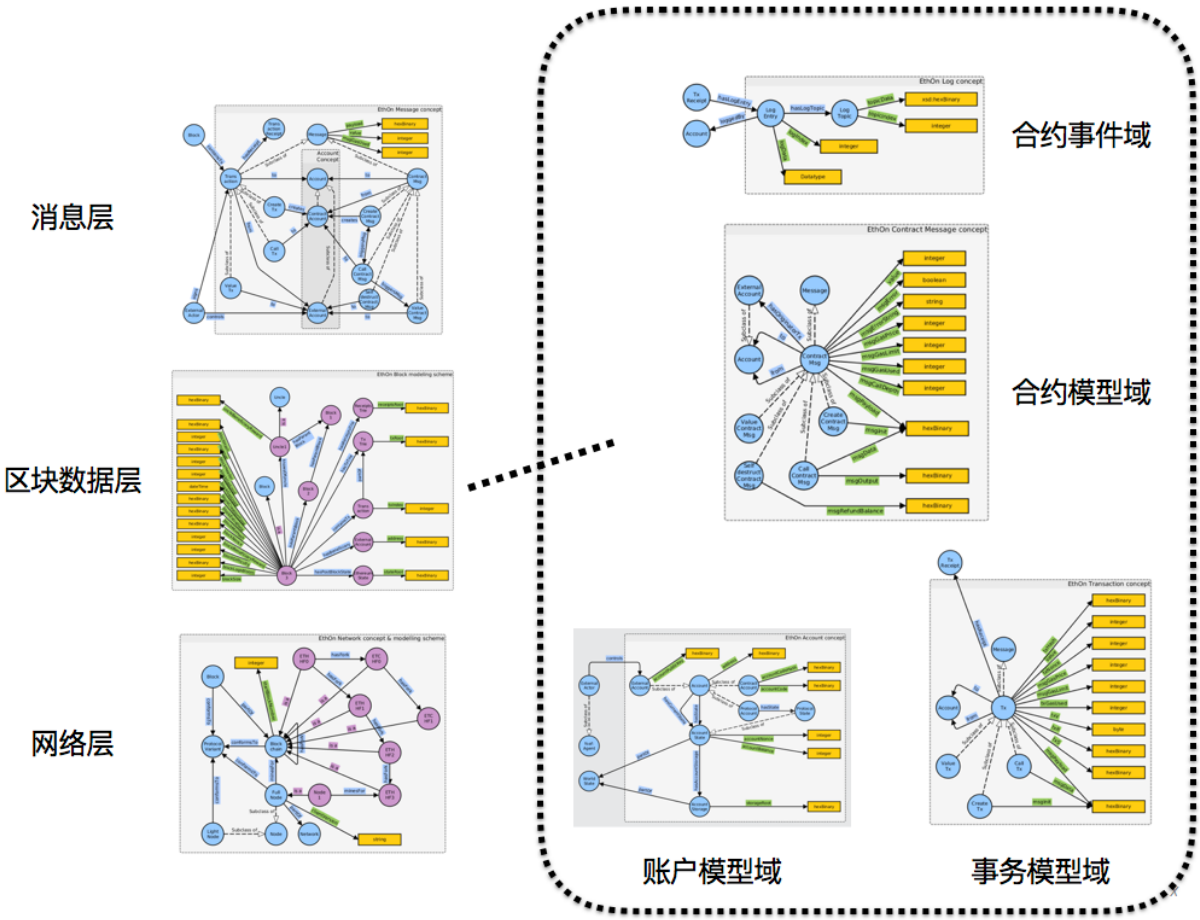
区块链落地并非单纯的使用区块链技术，它与传统的软件开发相似，仍然需要多方的配合，不管是设计还是开发，甚至安全运营环节，都需要多方共同协作完成。

关注隔离 Separation of Concerns

区块链落地亟待“关注点隔离”，企业对于区块链的诉求究竟是平台？还是应用？还是服务？

关注隔离

关注点混乱是目前阻碍应用落地的罪魁祸首，而遵守分层隔离原则进行落地开发，可以帮助产品团队识别出落地重点。



以太坊社区就依靠这种方式，对其平台、应用、服务做了细致的分层分领域拆分。我们可以通过EthOn提供的本体论看到，区块链的网络层、区块数据层、消息层需要分离，区块链数据中的账户模型、事务模型、合约模型、合约事件等领域也需要进一步解耦。

价值发现 Value Discovery

区块链的一大贡献，就是提供了一种数字化的价值迁移模型，它可以在某些场景下替代原本需要依赖权威共识保障的背书和行权。

我们在进行区块链落地开发之前，会对项目的愿景进行梳理，其中最重要的环节就是价值发现，在于业务人员的沟通中，我们需要识别出业务场景下的的价值与迁移（Value migration）。这里的价值可以是企业的资产，也可以是用户的数据，我们将其量化后转变为可以计算的价值点，通过区块链的特性能力解决其在业务场景下的痛点，这样在后续的应用落地中，就可以依靠这些价值约定来驱动出功能。

与此同时，价值发现也可以帮助我们在梳理愿景时就分析各个价值点的优先级，对任务进行有效的排列，也可以减少不必要的时间浪费。

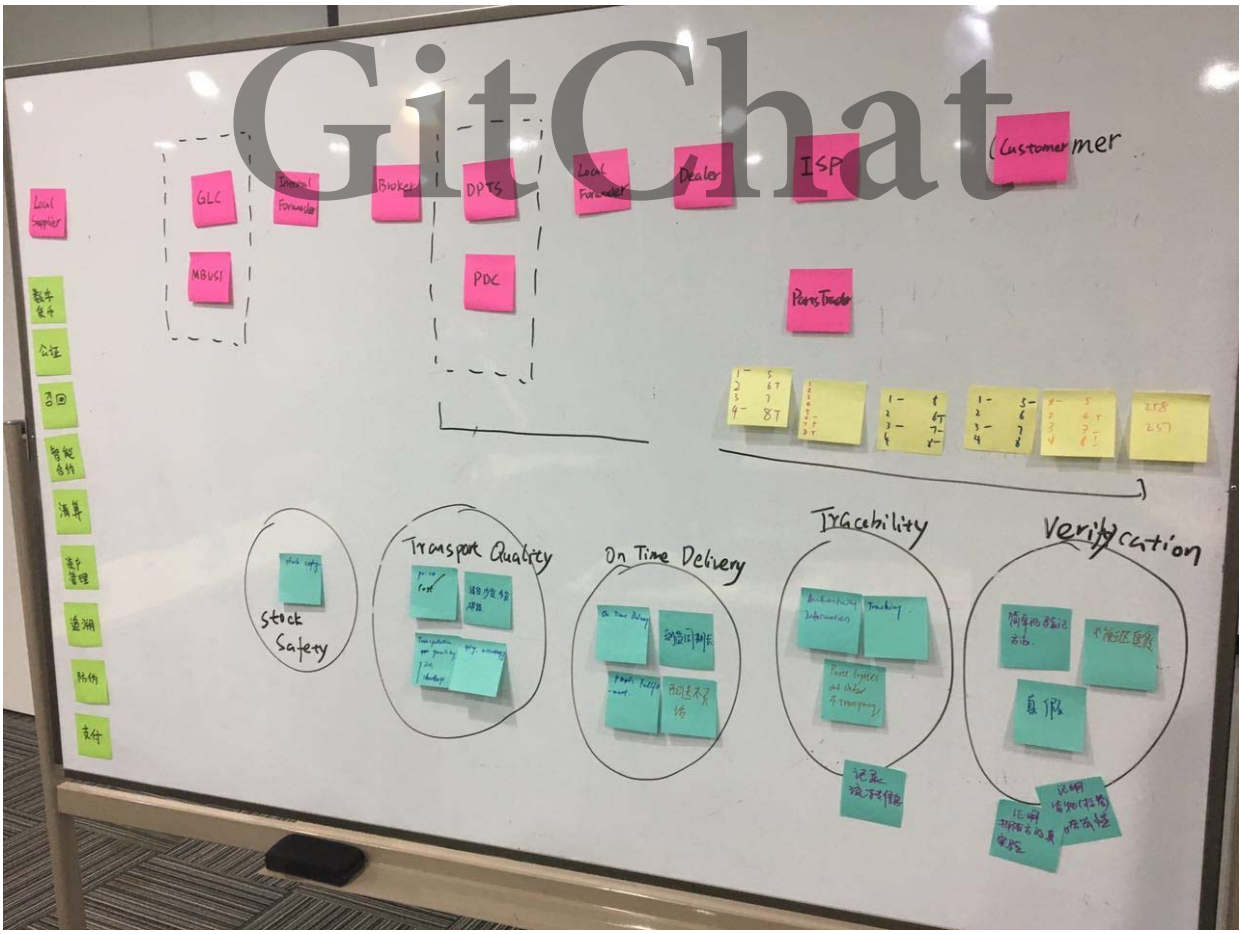
合约博弈 Contract Gaming

由萨博提出的智能合约模型，可以说是区块链产业的一大进步。

智能合约以区块链为载体，承载多方博弈中的价值，将规约与行权数字化。我们可以通过区块风暴的一系列活动，分析出区块链落地中可能存在的合约博弈点。

区块风暴通常包含下面几个步骤：

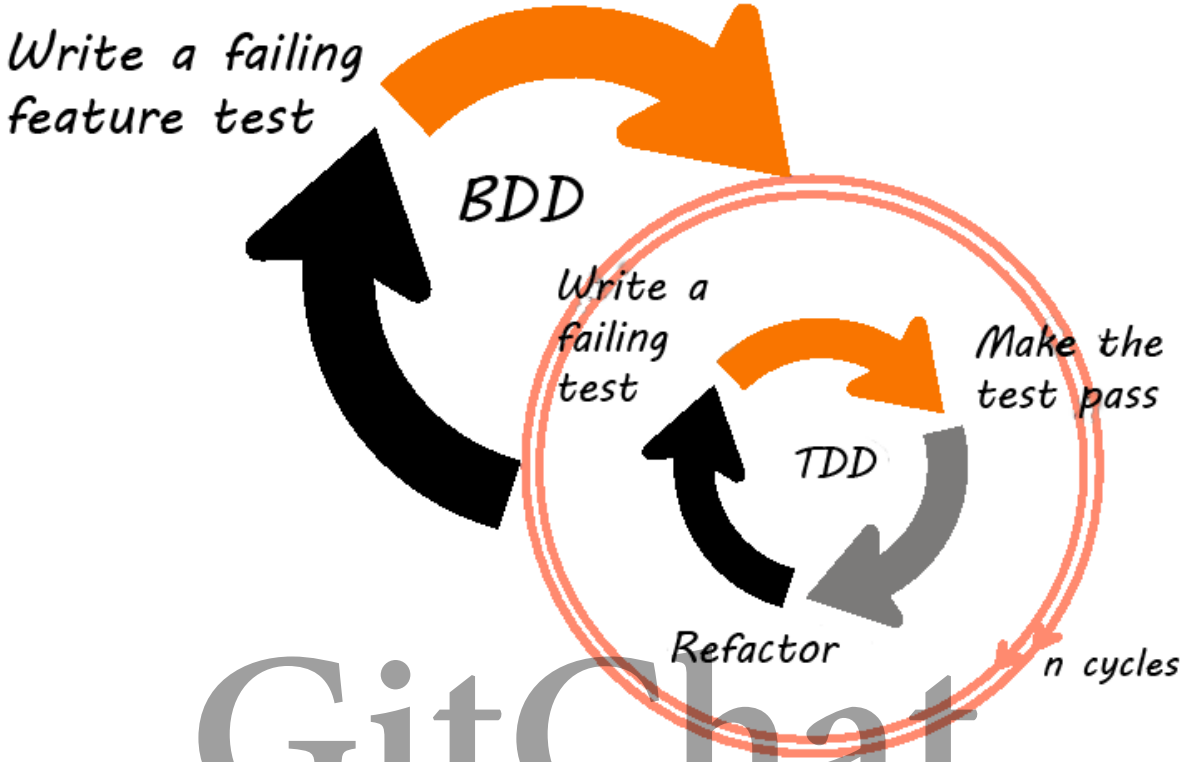
- 价值风暴 Value Storming ：针对业务中的价值进行发掘。
- 交易/事务风暴 Transaction Storming ：针对业务中的交易和事务（价值转移）进行梳理。
- 事件风暴 Event Storming ：将每个合约状态转移的事件映射到业务流中。
- 博弈风暴 Gaming Storming ：寻找合约中的博弈点，对其进行集中讨论。



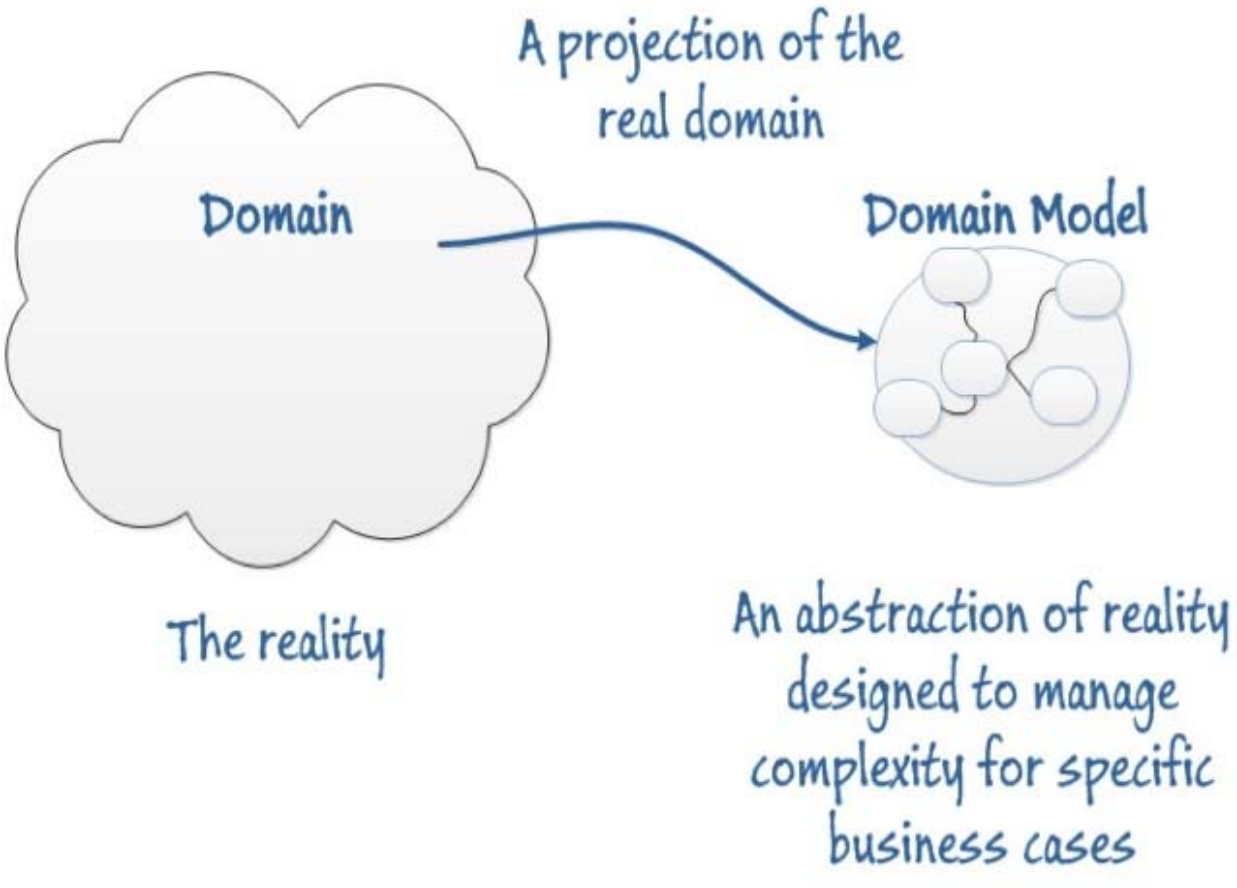
这四个头脑风暴，通过大量讨论识别系统中可能存在的价值点、交易、事件、博弈，并且将其映射到组织和组织间原本的业务流当中，可以将每个合约落地时所需的指导规约提前确定，帮助开发。

TDD，BDD & DDD

在区块链的开发过程中，我们依然采用测试驱动开发、行为驱动实现、领域驱动设计的最佳实践，帮助我们保证代码质量、确定业务需求、约束关注边界。



TDD可以保障合约的细节实现满足需求，并在重构迭代中为开发团队提供强大的信心支撑。BDD可以作为业务人员与区块链应用开发团队的沟通桥梁，以规范的业务描述形容规约。



而DDD则可以帮助架构师约束边界、拆分架构与组织，三者结合可以帮助开发团队在各个迭代中交付高质量、体验佳、清晰的区块链应用。

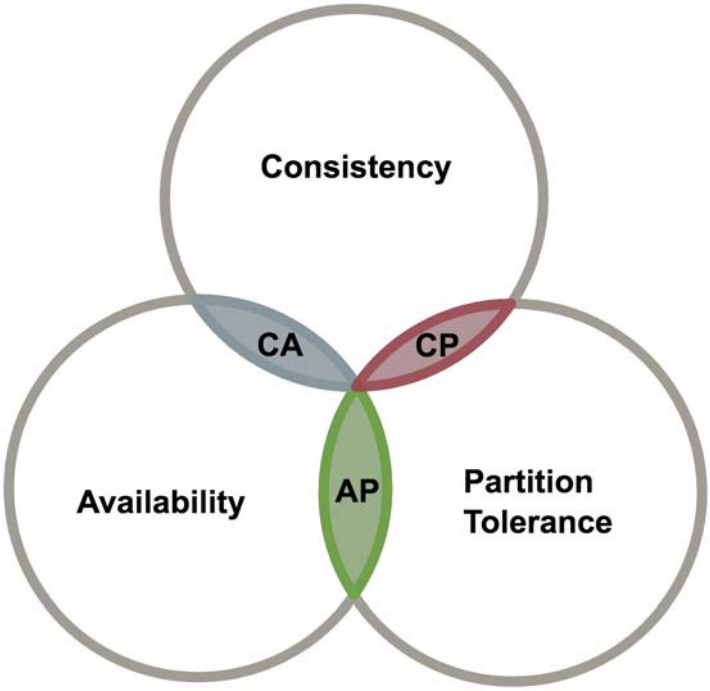
能力度量 Ability Evaluation

在技术选型的过程中，我们需要考察区块链框架和平台的能力，通常区块链的能力度量会从分布式的性能和系统完备等多个方面考虑。我们建议开发团队在选型前，先行评估下列能力。

能力度量

- ☐ 一致性
- ☐ 分区容错性
- ☐ 可用性
- ☐ 吞吐量
- ☐ 延迟
- ☐ 仲裁
- ☐ 可维护性
- ☐ 可扩展性
- ☐ 可测试性
- ☐ 可重用性
- ☐ 可追溯性
- ☐ 可恢复性

针对每个维度的能力度量，我们都可以希望尽可能量化和标准化，例如对于分布式系统中的一致性、分区容错性、可用性三者需要进行合理的权衡。区块链是一个高一致性高可用性的数据库，也由此带来了一系列性能瓶颈，我们可以通过一些裁剪（如SPF、闪电网络等）对其特定场景的性能进行优化。



而针对平台提供的基础开发设施，开发团队也需要有更完整清晰的认识，如Bitcoin、Ethereum、Hyperledger之间的的可扩展性差异，由其本身平台底层设计约束，开发人员

需要了解非图灵完备系统与图灵完备系统，非防停机问题系统与防停机问题系统之间的区分，才能判断选用何种平台作为落地框架。

密码学与分布式 Crypto & Distribution

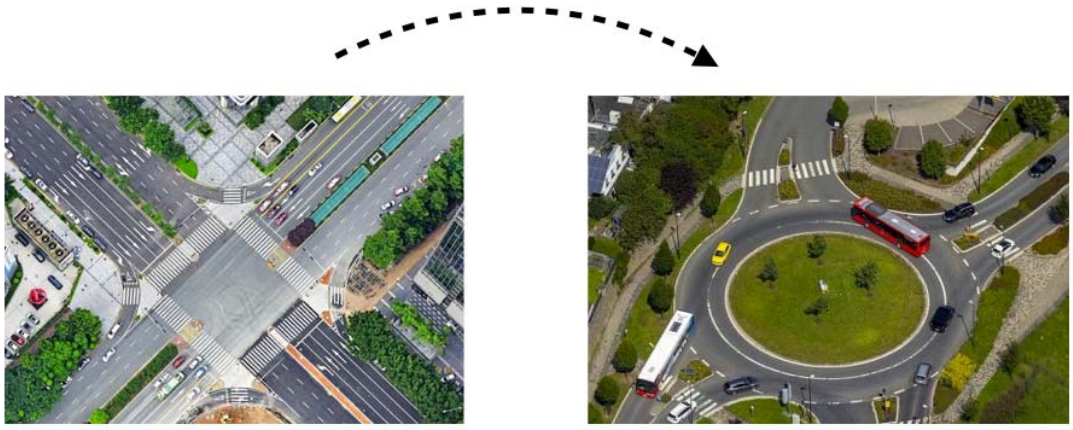
密码学与分布式系统是区块链应用的两大基础理论支撑，在区块链应用的落地过程中，我们也不可避免地需要讨论密码学与分布式问题。

其中密码学最核心的作用是将数字资产与价值数字化，因此不同的密码学原语（如摘要、签名、零知识证明、哈希谜语、同态加密等）都是为了满足信息系统与现实事务的映射，通过密码学技术完成数字孪生，是区块链的一个核心议题。

去中心化的分布式系统，是区块链的另一大创举，比特币为首的区块链应用，通过完善的协议规约，完成了高容错的去中心共识协议（如POW、POS、PBFT等），这就好比十字路口转变为环形岛的设计，而去中心化场景下的应用落地，也给传统业务区块链化带来了机遇和挑战，如何分析和适应去中心的场景，就对应用团队提出了新的要求。

Crypto & Distribution

去中心化



持续集成与不可变交付 Continuous Integration & Immutable Delivery

持续集成与持续交付已经成为IT业界的最佳实践，而区块链的去中心化特性，对开发团队在这一领域的能力提出了更高的要求。

持续集成/不可变交付

Delivery is immutable

So, Migration plan is necessary

区块链开源社区还在稳步的积累过程中，不可变交付也成为了新的难题，区块链在部署之后便很难进行迭代发布，尤其是合约一旦部署便不可修改，需要对留存在合约中的价值物进行迁移，这就要求开发团队将可能发生的迁移与部署问题考虑完善。

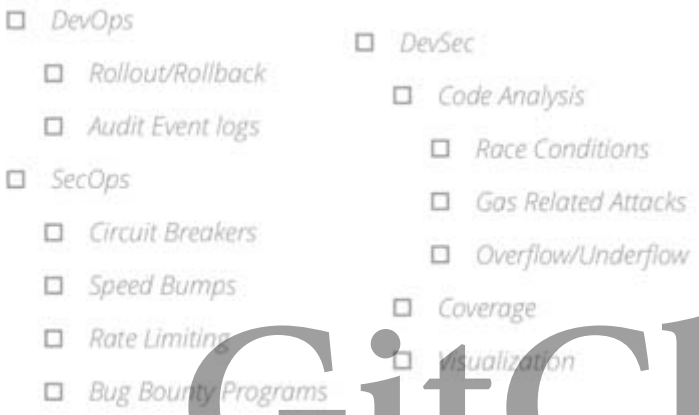
持续集成/不可变交付

木头轮子再精美，也上不了高速公路

Truffle与OpenZepplin在持续集成与不可变交付方面为以太坊开发提供了支撑区块链应用落地的工具与标准库，使用类似的工具可以帮助我们管理不可变的部署与迁移过程，并且享受业界在生产环境久经考验的标准化框架（如ERC Token、Math函数等）。

开发运维与内建安全 DevOps & BuildSecurityIn

随着区块链的一些应用逐渐落地，其工程实践如DevOps与内建安全的体系也在逐渐的完善，ConsenSys就总结了一些区块链的最佳实践供社区的开发者们参考，在开发运维方面，回滚与审计已经形成了一些实践，安全运营方面也有诸如断路器（Circuit Breaker）、减速带（Speed Bump）、限速器（Rate Limiting）等模式，也有一些公司采用Bug Bounty的方式进行悬赏。



此外在代码安全层面，我们也建议开发者尽可能使用现有的工具进行静态分析与可视化，同时提高测试覆盖率，以提高安全性与交付质量。

一个样例 SAMPLE

我们采用持续迭代的形式，在社区试验了数场区块链落地的 Workshop，其中基于以太坊的知识分享激励合约 **PonziTTT** 旨在培养更多区块链应用落地实践的布道者（Train the trainer），也已经经历了数轮迭代，两个线上版本的演化，你可以在 github 上找到我们的推进过程与代码。

在这个样例项目中，我们的学员也总结了一些问题，如：

- 博弈点需要确定。
- 不可变交付，要求严格测试。
- 数据访问，难以简单实现保密。
- Gas机制，用户体验受影响。
- 模块化调用与跨链通信，仍然需要等待标准。

面对这些问题，我们也找到了各自的方向：

- 合约博弈的引入可以帮助产品更好地运作。
- 引入测试工具，尽可能使用标准库，减少安全风险。
- 不可以依赖简单的实现做数据访问控制。
- 参与大都会（metropolis）的讨论，与社群一同制定Gas Billing新标准。

我们也期待未来的进展中能给大家带来更多的分享，也欢迎更多渴望落地实践的朋友能参与进来。

期待 Expectation

综上，我们为区块链落地过程中遇到的这九大问题：**敏捷与精益、关注隔离、价值发现、合约博弈、TDD/BDD/DDD、能力度量、密码学与分布式、持续集成与不可变交付、开发运维与内建安全** 分别找到了解决的研究方向，但是这些方法仍然等待着我们去深化和探索。

我们也期待看到区块链社区与业界能有更多的力量投入到关注实践与落地的应用场景里来，一起完善区块链落地中的最佳实践，希望这场技术创新能在开发者们脚踏实地的摸索中爆发出更大的能量。