Chromia Platform white paper 平台白皮书

Executive Summary 摘要

Chromia is a new blockchain platform for decentralized applications, conceived in response to the shortcomings of existing platforms and designed to enable a new generation of dapps to scale beyond what is currently possible.
Chromia 是为分散应用程序提供的一个崭新的区块链平台，旨在解决现存平台的缺陷，开创分散应用程序的新时代。

Motivation 动机

While platforms such as Ethereum allow any kind of application to be implemented *in theory*, in practice they have many limitations: bad user experience, high fees, frustrating developer experience, poor security. This prevents decentralized apps (dapps) from going mainstream.
虽然像以太坊这样的平台理论上可支持任何应用程序的执行，但实际运用中却存在很多局限：不良的用户体验、高昂的平台费用、欠佳的开发者体验、较低的安全性。这些都阻碍了分散应用程序走向主流的步伐。
We believe that to address these problems properly we need to seriously rethink the blockchain architecture and programming model with the needs of decentralized applications in mind. Our priorities are to:
要解决这一系列问题，我们需要重新认真了解区块链架构，以分散应用程序的需求为中心来设计模块。我们的首要任务是：

- Allow dapps to scale to millions of users. 使分散应用程序面向数百万用户。
- Make the user experience as smooth as with a centralized application: no fee for every interaction, no waiting time. 使用户体验像中心化应用程序一样平稳，每笔交互都不收费，无等待时间。
- Allow developers to build secure applications with minimal effort, using familiar paradigms. 使开发者能用最少的精力，参照相似的范例来开发安全的应用程序。

Technical design & features 技术设计和特征

We believe that within a decentralized application ecosystem a blockchain serves the role of a **shared database**: It stores application data and makes sure that data additions, updates and transformations are authorized and consistent with the application's rules. For this reason, Chromia is designed and optimized to serve the role of a shared database in the best way possible. It features:
在一个分散应用程序的生态系统中，区块链扮演着**共享数据库**的角色。它存储应用程序数据，确保数据的添加、更新、转化都有授权，且遵照应用程序的规则。为此，Chromia 应运而生，力争成为最佳的共享数据库。它的特征有：

- A relational model[1]: Blockchain data and application state are stored in a relational database. This model is considered to be best in class in terms of flexibility, versatility and consistency.
  关系模型：区块链数据和应用程序状态被存储在关系数据库中。这一模块被认为在灵活性、通用性和相容性方面是最一流的。
- Horizontal scaling: Each dapp gets its own blockchain (or, perhaps, multiple blockchains). Each blockchain is run by a subset of nodes, thus by increasing number of nodes we can increase total throughput.
  横向扩展：每一个分散应用程序拥有自己的区块链（或许可能有多个区块链）。每一区块链通过节点的子集来运行，这样就可以通过增加节点数量来增加总产量。
- Rich indexing and querying: Dapps can quickly retrieve information they need directly from nodes running the application. Dapp blockchain logic can perform complex queries without severe performance degradation.
  强大的检索和查询：分散应用程序能快速从运行的应用程序节点中直接获取它们需要的信息。分散应用程序的区块链逻辑可以在没有严重绩效降级的情况下完成复杂的查询。
- A relational programming language: Chromia dapp backends are written in a specialized language which is deeply integrated with the relational model. This model increases programmer productivity and ensures application consistency.
  关系编程语言：Chromia 的分散应用程序后端由专业语言编成，与关系模型深入融合。这一模型使得程序员更加高效，且应用程序相容性也得以保证。
- High I/O throughput: data queries and updates are delegated to a heavily optimized relational database, allowing dapps to perform a large number of queries and data update operations.
  I/O 高吞吐量：数据查询和更新的速度代表了极度优化的关系数据库，使分散应用程序能处理大量查询和数据更新。
- PBFT[2]-style consensus: Transactions can be confirmed within seconds.
  PBFT 式共识：交易在数秒内就能确认。
- First-class dapps: Dapps do not arise from “smart contracts” in Chromia, but are considered first-class entities. Chromia gives dapp developers a high degree of flexibility and control. For example, Chromia does not charge dapp users for each transaction they make, instead collecting fees from dapps as a whole. This leaves developers free to create their own fee and resource use policies.
  一流的分散应用程序：在 Chromia，分散应用程序并非起源于“智能合约”，而是一个一流的个体。Chromia 给予分散应用程序开发者更强的灵活性和控制权。例如，Chromia 不对分散用户的每笔交易进行收费，而是整体收费。这使得开发者能自主制定费用和资源使用政策。

---

[1] Codd, E.F (1970). "A Relational Model of Data for Large Shared Data Banks". 大型共享数据库的数据关系模型 Communications of the ACM.计算机协会通信 Classics. 13 (6): 377–87; https://dl.acm.org/citation.cfm?doid=362384.362685

[2] Castro, M.; Liskov, B. (2002). "Practical Byzantine Fault Tolerance and Proactive Recovery""实用的拜占庭式容错和主动恢复”. ACM Transactions on Computer Systems.计算机系统上的 ACM 交易 Association for Computing Machinery. 计算机协会 20 (4): 398–461. https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.127.6130

Chromia is implemented on top of the existing Postchain[3] framework developed by ChromaWay.
Chromia 在幻彩大道开发的后链架构上运行。

Chromia offers the same level of openness, transparency and decentralization as other public blockchains. In Chromia *miners* are replaced with *providers.* Providers own nodes which produce blocks. It has been suggested that the four largest mining pools of both Bitcoin[4] and Ethereum[5] could exert significant control over those networks if they colluded. We aim to ensure that the minimum number of node providers whose collusion would be required to exert such control on Chromia exceeds this number significantly. It can therefore be said that the Chromia model does not tend towards centralization any more than the oldest and most trusted public blockchains.
Chromia 与其他公有区块链一样开放、透明、去中心化。在 Chromia，矿工被供应商所取代。供应商拥有能够生产区块的节点。有人建议，如果比特币和以太坊的四大矿池串通，将对那些网络形成极强的控制。而我们力求确保节点供应商的最小量远超这一数字。那么我们可以说 Chromia 模型并不像最古老的，最受信任的公有区块链那样走向中心化。

Chromia' PBFT-style consensus is further hardened by anchoring[6] to make sure that finality is at least as strong as the finality of Proof of Work (PoW) blockchains such as Bitcoin and Ethereum. To alter the history of an anchored portion of Chromia block history it would be necessary to combine PoW blockchain reorganization with a malicious collusion of a sufficient number of Chromia nodes.
ChromiaPBFT 式共识通过侧链来加固，确保它的终端至少同比特币、以太坊这样的 PoW 区块链一样强健。为了改变以往 Chromia 区块中的侧链比例，我们有必要将 PoW 区块链与 Chromia 一定数量的恶意串通节点进行重组。

Uses 使用

Chromia is a general-purpose platform which is suitable for almost all kinds of dapps. It is particularly well suited to cases which require high I/O capacity or which involve management of complex data sets.
Chromia 是一个面向大众的平台，它适用于几乎所有种类的分散应用程序。尤其适用于对 I/O 吞吐量有高要求的或者需要管理复杂数据的情况。

---

[3] https://chromaway.com/products/postchain/
[4] https://blockchain.info/pools
[5] https://www.etherchain.org/charts/topMiners
[6] We originally described Anchoring as "side-chains" 我们最初将锚定形容为"侧链"https://bitcointalk.org/index.php?topic=313347; a more formal discussion of anchoring can be found in the BitFury white paper "On Blockchain Auditability".对于锚定更正式的讨论可以在 BitFury 白皮书"区块链可审核性"中找到 https://bitfury.com/content/downloads/bitfury_white_paper_on_blockchain_auditability.pdf

Massively multiplayer online games (MMOGs) are one example. Chromia is capable of hosting entire game worlds in the blockchain, making sure that they evolve according to predetermined rules and ensuring that no one can cheat. Blockchain gaming is becoming increasingly popular, but MMOGs are currently out of reach because no existing blockchain platform can support them. We believe that implementing a MMOG will be the best way to showcase the capabilities of Chromia. MMOGs have a very demanding set of requirements; the capacity to run MMOGs implies that Chromia is suitable for demanding and complex dapps of all kinds.
多用户在线游戏（MMOG）就是一个很好的例子。Chromia 可在区块链上支持整个游戏世界，并确保按照既定的规则进行，没有人可以作弊。区块链游戏正日趋受欢迎，但 MMOG 却很少有人涉足，因为现有的区块链平台都无法支持他们。而 MMOG 的运行恰恰最好展示了 Chromia 的实力。MMOG 对平台有着十分苛刻的要求，因此 MMOG 的运行意味着 Chromia 有能力应对任何复杂的分散应用程序。

Design rationale 设计原理

Overview of problems with existing platforms 现有平台问题概述

Ethereum was a first blockchain to offer a platform for decentralized application development. Many application prototypes were created, but developers faced the following issues:
以太坊是为分散应用程序发展提供的第一个区块链平台。它创建了许多应用程序标准，但开发者会面临以下问题：

- Limited capacity. Because network capacity is limited, and usage fees are proportional to load, transaction fees can be $1 or more for complex applications. This cost, typically paid for each interaction with an application, makes most applications too expensive to be practical.
  有限容量。因为网络容量有限，且使用费是按比例收取，交易费可达 1 美元，一些复杂的应用程序会更贵。高昂的成本使得大多数应用程序都贵的离谱。
- Prohibitively expensive I/O operations, for the same reason. For example, a contract cannot iterate through a list of users since the cost of this action would exceed the block gas limit. Thus developers have to jump through hoops to implement something as simple as an interest payment to a list of users.
  同样的原因导致过高的 I/O 操作费。例如，一份合约不能对多个用户使用，因为这一操作的成本超出了区块的限制。因此，开发者不得不向用户们重复类似于利息支付那样的简单操作。
- Poor data modelling tools and poor support for queries. Application developers have to resort to centralized indexing and caching layers, or using third party services which do not provide the same security guarantees as the base layer.
  欠佳的数据模型工具和查询支持。应用程序开发者不得不通过中心索引来获取应用层，有时还需借助第三方服务，但这样又得不到同等的安全保障。
- Error-prone contract language which has resulted in many high-profile heists.
  易出错的合约语言已导致许多备受瞩目的拦劫。
- No provision for contract upgrades at the platform level, this functionality has to be implemented as a separate layer which further increases complexity.

在平台层面没有合约升级的条款，在单独应用层实现这一功能更加剧了复杂性。

- Users having to pay fees for every interaction results in poor UX. Slow confirmations are a major usability issue.
  用户需要为每一次交互付费导致了不好的用户体验。确认速度慢是一个主要的使用问题。
- Poor light client support. Three years after beginning development efforts the Ethereum Foundation was still struggling to offer a production-quality light wallet.
  不良的轻客户端支持。在开发平台三年后，以太坊基金仍旧在研发产品级质量轻钱包。

Applications designed with a large audience in mind need to be flexible and responsive. They require a platform which empowers the developer to allocate resources in a way that suits their users. Even if Ethereum and other platforms currently in development tackle scalability issues, they will not be able to provide a sufficient degree of developer autonomy and will remain a somewhat hostile environment for dapps.
面向大批量客户群的应用程序必须具有灵活性和快速响应能力。它们要求平台赋能开发者完成用户所需资源的配置。即使以太坊等其他平台目前正发展解决可扩展性的问题，他们依旧无法给开发者提供足够的自主权，对于分散应用程序而言仍旧会是个糟糕的运行环境。

We believe that to address these problems properly we need to seriously rethink the blockchain architecture and programming model with the needs of decentralized applications in mind.
要解决这一系列问题，我们需要重新认真了解区块链架构，以分散应用程序的需求为中心来设计模块。

Blockchain as a database 作为数据库的区块链

The main role of a blockchain in a decentralized application context is to manage data in a secure and consistent manner. Thus it can be understood as a database, particularly, as a secure decentralized database. Another major role of a blockchain is prevention of double-spending, but this is a special case of data consistency constraints.
在分散应用程序的环境中区块链的主要职责是以安全和始终如一的方式管理数据。所以它可被定义为一个数据库，一个安全的去中心化数据库。区块链的另一个重要职责是防止重复消费，但这是针对数据一致性约束的一个个例。

Blockchains which are optimized for payments, such as Bitcoin, can adopt highly specialized (and optimized) data models. But a platform designed for hosting diverse decentralized applications needs a general-purpose data model.
像比特币这样优化付款的区块链可以采用高级定制化（和优化）的数据模型。但一个承载多样化分散应用程序的平台需要的是一个多用途的数据模型。

Most blockchain platforms nowadays use key-value data stores (examples: Ethereum, NEO, Fabric). This model is, in theory, complete, and enables the use of high-performance data stores such as LevelDB. However, this model is very low-level. It requires application developers to implement details such as serialization and indexing, a daunting challenge.

现行的多数区块链平台都使用关键值数据存储（如：以太坊，NEO,Fabric 等）。从理论上讲，这一模型完整且可以使用像 LevelDB 这样高效的数据存储。但是，这种模型是非常低层次的。它要求应用程序开发者执行序列化和检索等细节，这无疑是一巨大挑战。

Compounding this, blockchain platforms typically do not expose the full functionality of key-value stores, such as the ability to use arbitrary-sized keys and iterate through keys. For example, in EVM all keys are 256-bit integers and iterating through stored keys is impossible. For these reasons, implementing proper indexed data access on the EVM is both difficult and inefficient.
综合以上情况，区块链平台无法展示关键值存储的所有功能，比如任意大小值和重复值的使用能力。在 EVM 中所有值都是 256 比特整，重复使用存储值也是无法实现的。为此，在 EVM 上执行适当的检索数据权限是困难且无效的。

Relational model 关系模型

For the reasons stated above, we consider our choice of data model to be the lynchpin of our blockchain platform.
综上所述原因，我们将数据模型的选择视为区块链平台的关键。

The relational model has been the gold standard for database management for the last five decades. Rooted in mathematics and logic, it is known to be able to model complex data in an efficient way.
关系模型在过去的五十年里都是数据库管理的黄金标准。从数学和逻辑角度出发，关系模型被认为可以高效建立复杂数据模型。

As decentralized applications deal with increasingly complex data structures, the power of the relational model becomes more and more apparent. Further, most software engineers are already familiar with it so they won't have to learn new concepts in order to implement an application.
由于分散应用程序处理着日益复杂的数据架构，关系模型的力量也日趋明显。此外，大多数软件工程师都已熟悉关系模型，无需再为执行应用程序学习新的理念。

A relational model also allows us to leverage the power of SQL database management systems which have been optimized for decades. Instead of dapp code which traverses memory cells one by one, we can send a query to the DBMS and let it use its sophisticated query planning, data structures and caching capabilities to carry out the query as fast as possible.
关系模型也使我们能利用已经被优化了几十年的 SQL 数据库管理系统。与其让分散应用程序代码一个个穿过记忆细胞，我们可以向 DBMS 发送一个查询请求，让它运用其精细的查询设计、数据架构和获取能力来快速开展查询。

Of course, the choice of data model is a trade off. The relational model might have the following disadvantages:
当然，数据模型的选择也是一个折中的考量。关系模型也有以下的一些缺陷：

- Performance is hard to predict and depends on the query planner. This is not a significant disadvantage in the context of Chromia because each dapp will be run in an

isolated manner; slow queries will affect only the dapp which performs them rather than the system as a whole.
性能的好坏很难预测，它取决于查询计划者。这对于 Chromia 也并非是一个重大缺陷，因为每一个分散应用程序都以单独的方式运行，查询缓慢只会影响分散应用程序，而不是系统本身。

- It is impossible to impose hard bounds on query execution time. Again, this is not a problem in the case of Chromia because it affects only the application which issues slow queries.
  对查询执行时间规定明确界限并不切实可行。同样，这对 Chromia 而言也不是问题，因为它只对查询速度慢的应用程序有影响。
- Parallelization of SQL databases is a complex area of active research. As far as we know, no blockchain platform offers 100% fully automatic parallelization on a massive scale. Thus there is no evidence that a relational model is worse than other models. In addition, we believe that the relational model will make logical sharding and sidechain mechanisms easier to implement.
  SQL 数据库的平行化是有效调查的一个难点。据目前了解，尚未有区块链平台能在大范围内提供 100%自动平行化。所以，没有证据可以证明关系模型不如其他模型。另外，我们认为关系模块将会使逻辑分片和侧链机制更易执行。

First-class decentralized applications 顶尖的分散应用程序

In Ethereum all code lives in “contracts”. It does not differentiate between individual wallet contracts and complex multi-user contracts, they all use the same resource metering nad programming model. An Ethereum-based dapp will use one or more contracts (possibly a contract for each user) and front-end components. In fact, many Ethereum applications make use of centralized caching, rendering their “decentralized” credentials somewhat dubious.
在以太坊上，所有的代码存活于“合约”中。私有钱包合约与复杂多用户合约并未区分开，他们利用的是同一资源测量程序模型。一个基于以太坊的分散应用程序会用一个或多个合约（也许一个用户一份合约）和前端组件。事实上，许多以太坊应用程序利用中心化缓存来补偿“去中心化”证书，这多少有些可疑。

While this approach is quite elegant and can scale to different kinds of applications, it is very inconvenient for dapps designed for mass use. End-users have to pay for every interaction with their dapp, in proportion to the computational and storage resources required for their transaction. In other words, Ethereum doesn’t give decentralized applications the flexibility to manage resources themselves. For example, a “freemium” business model is outright impossible. This creates a barrier for decentralized application adoption: most users are not ready to pay for every single click.
虽然这一方法十分明智，可以分布到各不同种类的应用程序，但对于大范围使用的分散应用程序来说很不方便。终端用户需要为他们分散应用程序上的每一次交互付费，与他们所需的计算和存储资源成正比。换言之，以太坊没有给分散应用程序该有的灵活性来管理他们自己的资源。例如，“免费增值”的商务模型是完全无法实现的。这给分散应用程序的使用添加了一道屏障，大多数用户并未准备好为他们的每一次操作买单。

Chromia solves this issue by provisioning resources on the decentralized application level:
Chromia 通过在分散应用程序层面提供资源来解决此问题：

- Each dapp has its own blockchain (sidechain)
  每个分散应用程序拥有自己的区块链（侧链）
- Fees (collected to maintain nodes) are paid by the dapp as a whole, not by end-users directly
  由分散应用程序统一付费，而非终端用户
- Thus dapps are free to implement their own resource management policies, which can thus be aligned with economic rather than technical needs
  分散应用程序能够执行自己的资源管理政策，可以更好的统一经济需求，而非技术需求。

Every blockchain needs an anti-spam mechanism, but this mechanism doesn't have to be tied to fees. For example, a dapp might allow only 1 action from a user each 15 seconds, thus a single user won't be able to spam the blockchain with billions of transactions. A dapp can also mitigate Sybil attacks through limiting new user registration to some reasonable rate and/or requiring invitation or a deposit.
每个区块链都需要一个反垃圾信息机制，但这一机制并非要与费用挂钩。例如，一个分散应用程序可能在 15 秒内只允许用户有一次操作，因此单一用户不会在区块链上有数十亿次交易。分散应用程序还可通过一定程度限制新用户注册量或通过邀请、押金的方式注册来减轻 Sybil 攻击。

In this model, we do not need to measure the resources used by each operation. Instead, we provision resources to the application as a whole: each dapp's blockchain will run on a certain set of nodes. Typically it will have its own dedicated CPU thread.
在这一模型下，我们无需衡量每一操作的资源。相反，我们将资源整体运用到应用程序上：每一分散应用程序的区块链通过一定数量的节点运行。它将有自己专属的 CPU 螺纹。

This removes resource metering overhead (we no longer care how many instructions were executed, as an application cannot use more resources than it was given) allowing dapps to perform faster and scale better.
这一资源转移使得分散应用程序运行更快，延伸更广（我们不用再关注执行了多少指令，因为应用程序已最大化使用其资源）。

If a dapp needs more than one execution thread, it can consist of multiple shards each of which will be a sidechain.
如果一个分散应用程序需要多个执行螺纹，它可包含多个分片，即侧链。

Besides scheduling, having dapps as first-class citizen on the platform allows the following features:
除了调度，作为平台上的顶尖市民，分散应用程序拥有以下特征：

- Token economics integrated with a fee model, i.e. fees are taken from profits "earned" by an application 代币经济与费用模型融合，如程序的支出可在其所获盈利中支取

- Built-in governance 内置管理
- Updates 更新

Programming model 编程模型

The Postchain framework on which Chromia is based allows us to use existing open source SQL database software (specifically, PostgreSQL) to implement data store and query capabilities. However, we cannot allow dapps to perform arbitrary SQL queries as said queries might be unsafe, ambiguous or lead to excessive resource use.
Chromia 所在的后链框架允许我们利用现有开放的 SQL 数据库软件来执行数据存储和查询。但是，我们不允许分散应用程序随意执行 SQL 查询，因为查询可能不安全、模糊不清或导致资源滥用。

Most dapp blockchain platforms use virtual machines of various kinds. But a traditional virtual machine architecture doesn't work very well with the Chromia relational data model, as we need a way to encode queries rather than just operations.
大多数分散应用程序区块链平台使用各种虚拟机器。但是传统的虚拟机器在 Chromia 关系数据模型上运行的并不理想，因为我们需要对查询编码，而不仅仅是操作。

For this reason, we are taking more language-centric approach: a new language called Rell ([Rel]ational [l]anguage) will be used for dapp programming. This language allows programmers to describe:
为此，我们采取更多以语言为中心的方法：一种叫做 Rell（关系语言）的新语言将应用于分散应用程序的编程。这一语言使程序员能描述：

- Schema / data model 模式/数据模型
- Queries 查询
- Procedural application code 程序代码

Rell will be compiled to an intermediate binary format which can be understood as code for a specialized virtual machine. Chromia nodes will then translate queries contained in this code into SQL (while making sure this translation is safe) and execute code as needed using an interpreter or compiler.
Rell 会编制一个二进制格式，可理解为一个专属虚拟机器的代码。Chromia 的节点就会将带有此代码的查询翻译成 SQL，用编译器来执行代码。

Rell will have the following features:
Rell 有以下特征：

- Type safety / static type checks. It's very important to catch programming errors at the compilation stage to prevent financial losses. Rell will be much more type-safe than SQL, and it will make sure that types returned by queries match types used in procedural code.
  输入安全/静态类型检查。在编辑阶段发现编程错误很重要，可以防止不必要的经济损失。Rell 比 SQL 在编写时更加安全，它可确保查询反馈输入与代码输入相匹配。
- Safety-optimized. Arithmetic operations are safe right out of the box, programmers do not need to worry about overflows. Authorization checks are explicitly required.
  安全优化。算术操作安全可用，程序员无需担心超限。授权检查是明确要求的。

- Concise, expressive and convenient. Many developers hate SQL because it's very verbose. Rell doesn't bother developers with details which can be derived automatically. As a data definition language, Rell is up to 7x more compact than SQL.
  精准、可表现、方便。许多开发者不喜欢 SQL，因为它及其繁琐。Rell 不会过多打扰开发者，细节之处可自动获取。作为一个数据定义语言，Rell 比 SQL 简洁 7 倍多。
- Allows meta-programming. We do not want application developers to implement the basics from scratch for every dapp. Rell will allow functionality to be bundled as templates.
  支持元编程。我们不想让应用程序开发者忙于为每一个分散应用程序执行最基础的内容。所以，Rell 支持模板功能。

We identified that no existing language or environment has the feature set required for this task, and thus development of a new language is absolutely necessary.
我们意识到现存的任何语言或环境都无法完成此任务，所以开发一种新的语言迫在眉睫。

We designed Rell in such a way that it is easy to learn for programmers:
我们设计的 Rell 易于程序员学习：

- Programmers can use relational programming idioms they are already familiar with. However, they don't have to go out of way to express everything through relational algebra: Rell can seamlessly merge relational constructs with procedural programming.
  程序员可以运用他们已经熟悉的关系编程语言。但是他们无需用关系代数来表述所有东西。Rell 可以将关系架构与程序编程完美融合。
- The language is deliberately similar to modern programming languages like JavaScript and Kotlin. A familiar language is easier to adapt to, and our internal tests show that programmers can become proficient in Rell in matter of days. In contrast, the ALGOL-style syntax of PL/SQL generally feels ancient and weird to modern developers.
  该语言和 JavaScript 和 Kotlin 这样的编程语言非常相似。一种熟悉的语言更容易被采纳，我们的内部测试显示程序员几天内就可熟练运用 Rell。相反，PL/SQL 使用的 ALGOL 型语法显得和当今行业有些格格不入。

The Ethereum programming model is typically described as very error-prone. Bugs in Ethereum smart contracts have resulted in losses totalling hundreds of millions of dollars[7]. In Chromia, we aim to eliminate most common sources of problems through a better programming model (no weird interactions between different smart contracts as in the DAO case[8][9]) and safer languages.
以太坊编程模型被认为极易出错。以太坊智能合约中的故障已导致总计数亿美元的损失。在 Chromia，我们希望通过更优的编程模型和更安全的语言来消除这些最常见问题的根源。

[7] A list of the most serious Ethereum vulnerabilities can be found here 可访问以下链接找到最严重的以太坊脆弱性清单: https://www.dasp.co/
[8] https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/
[9] https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/

On Ethereum code is immutable, it is often impossible for a developer to fix her dapp unless she retains full control, thus making it not-quite-decentralized. In Chromia, upgrades can be deployed through a built-in governance and transition mechanism.
在以太坊上的代码是不可变的，开发者想要处理分散应用程序必须保持对程序的完全控制，这样就做不到去中心化了。在 Chromia，程序更新可以通过内置的管理和转变机制来完成。

Consensus & nodes 共识&节点

Model overview 模型概述

It is clear that the full node model doesn't scale particularly well. If we require users to run a full node which has a complete copy of the system state then dapps are severely limited in what computations and storage resources they can use.
很显然，全节点模型并没有延伸的很好。如果我们要求用户运行拥有系统状态全部备份的全节点，那分散应用程序可用的计算和存储资源就变得极其有限。

With the aim of achieving better performance at scale we propose a model in which individual dapps are hosted on a subset of validator nodes, which establish consensus on any modifications to the dapp state, and handle client queries. The system should permit any user to run a full replica node if desired, but the system should not depend on these replica nodes for operations.
为了能在延伸性方面能有更佳表现，我们推出了让单一分散应用程序在验证器子节点上运行的模型，这样对分散应用程序状态的任何修改都可达成共识，也可处理客户查询。系统应该允许任何用户运行想要的全复制节点，但不应该将常规运行依赖于此。

Sybil control mechanism Sybil 控制机制

The research done by our team indicates that commonly used Sybil control mechanisms like PoW and Proof of Stake (PoS) are unsatisfactory[10]: neither of them guarantees a sufficient level of Sybil attack mitigation, or even a particularly good measure of decentralization. Evidence indicates that most PoW-based blockchains, including Bitcoin, might be de facto controlled by a small group of entities. This problem is particularly bad for smaller cryptocurrencies which do not yet have an independent mining ecosystem. PoS also comes with no decentralization guarantees, and DPoS[11] in particular is prone to formation of cartels and bribery.
调查发现，像 PoW 和 PoS 这样常见的 Sybil 控制机制表现都不尽如人意。它们都无法保证对 Sybil 攻击有一定层级的减轻，甚至好的去中心化方式都没有。事实证明，包括比特币在内的多数基于 PoW 的区块链都很可能是由一小群个体控制的。这一问题对于小型加密货币尤为突出，因为它们没有自己独立的挖矿生态系统。PoS 也没有去中心化保障，DPoS 甚至有垄断和贿赂倾向。

Thus instead of following commonly used approaches we will design Chromia consensus and Sybil control mechanisms from first principles.

---

[10] https://download.wpsoftware.net/bitcoin/pos.pdf
[11] Delegated Proof of Stake 股份授权证明机制, https://bitshares.org/technology/delegated-proof-of-stake-consensus/

因此，摒弃过往常用的方法，我们设计出了 Chromia 共识和 Sybil 控制机制。

First we observe that what Chromia is trying to achieve can be compared to cloud computing: an application which redundantly uses multiple cloud hosting providers can be considered a decentralized application, in the sense that failure or censorship of a single cloud hosting provider does not result in a shutdown of the whole application. A cloud computing model also allows users to use thin clients instead of hosting a complete replica of application backend on their personal device.
首先，我们发现 Chromia 所想要达成的可比作为云计算：一个过多使用多个云代管供应商的应用程序可被认为是一个分散应用程序。单一云代管供应商的故障或审查不会导致整个应用程序的瘫痪。云计算模型也使得用户可以使用瘦客户，而不是在他们个人设备上运行一整个应用程序后端。

The essential roles in the Chromia model are defined as follows. Chromia software runs on *nodes*, physical or virtual instances of computing power. Nodes are controlled or perhaps owned by some kind of individual, organisation, or collective which we refer to as a *provider*. *Users* connect to such nodes to post transactions, query data or synchronize their private replicas.
Chromia 模型定义的基本职责如下。Chromia 软件在节点上运行，这些节点是物理或虚拟的运算力。节点被一些个人、组织或集体所控制或拥有，我们将他们称之为供应商。用户连接这些节点以完成盘后交易、数据查询或同步私人备份。

A Byzantine fault tolerant network is distinguished from a merely fault tolerant network by its ability to tolerate *arbitrary and potentially malicious behaviour* by network participants. The concept of *nodes* is sufficient for designing a fault tolerant network, but to target proper Byzantine fault tolerance we must account for conscious *provider* entities with the potential to coordinate multiple nodes.
根据对网络用户容忍任意和潜在恶意行为的能力，可以将拜占庭式的容错网络与一般容错网络区分开。 节点的概念足以设计一个容错网络，但为了能达成拜占庭式容错，我们必须对有意识的供应商个体负责，这可能会需要协调多个节点。

Crucially, to keep a dapp decentralized we need to make sure that the nodes which run its blockchain(s) belong to *different and non-colluding* providers. In that case the application can tolerate a subset of providers experiencing failures, being compromised or performing hostile actions.
关键地，为保证分散应用程序能去中心化，我们要确保节点在不同供应商区块链上运行。这种情况下应用程序能够容许供应商出错，能够做出妥协或采取敌对措施。

For this to work, network participants need to i) know which nodes each provider controls and ii) make sure that providers are *actually* distinct. The latter cannot be done mechanically, but it can be done socially. There is overwhelming evidence that Microsoft and Google are different providers, but there's no mechanical way to prove it.

为了使其工作，网络用户首次要知道每个供应商商控制的对应节点，其次要确保确实是不同供应商。后者无法以理论方式完成，但可以通过社交来实现。微软和谷歌是不同的供应商，这点显而易见，但却没有理论方式来论证它。

We believe that *all* decentralised consensus ultimately depends on “social consensus”. Fully automated decentralised systems are a fantasy, in the end it is people who determine the rules of the system. Chromia acknowledges this, and includes it as a fundamental design principle. In practice, provider distinctness will be achieved as follows:
我们认为所有的去中心化共识根本上都是“社交共识”。全自动的去中心化系统很奇幻，最终都是靠人来制定系统规则。Chromia 认同这一点，并将其视为基本的设计原则。实际上，供应商的差异可以通过以下方面体现：

1. Initially, ChromaWay will select a set of distinct providers. We believe that our extensive knowledge of blockchain and IT industry will allow us to choose well, and we are incentivized to select providers that the users will accept. Users who are concerned about provider uniqueness are welcome to do their own research.
   最初，幻彩大道会选一组不同的供应商。我们相信良好的区块链和 IT 行业知识储备能让我们做出很好的选择，并且我们也趋向选择用户会接受的供应商。若对任一供应商的独特性有质疑，都鼓励用户开展自己的调查。
2. Eventually, once the system has a sufficiently diverse set of providers, we will allow providers themselves to vote to add new providers and the system will no longer depend on ChromaWay as a gatekeeper.
   最终，一旦系统有足够多的供应商，我们会授权这些供应商们自主投票来添加新的供应商，系统就不再需要幻彩大道这个把关者。

Consensus 共识

We assume that each blockchain within Chromia will be associated with a set of validator nodes which is a subset of all nodes belonging to Chromia.
我们假定 Chromia 的每一区块链都和一组验证器节点相关联，这些节点都是 Chromia 上的子节点。

This subset of nodes will run a BFT consensus algorithm. Since the set size is limited, PBFT-like algorithms are the optimal choice -- they are well-researched, work well with sufficiently small sets of validators, and provide definitive finality, making reorganization impossible.
这些子节点都会运行 BFT 共识运算法则。由于大小有限，PBFT 式运算法则是最佳选择。他们经过充分调研，与小验证器工作良好，并可提供终极定论，使重组成为可能。

However, we also need to consider a systemic risk. While we assume that collusion between providers running the nodes is unlikely, it can potentially happen. Also a majority of nodes might be compromised via a “zero-day” exploit of some kind. Signature-based consensus (such as PBFT and PoS) fails in a catastrophic way[12], making the whole chain invalid.

[12] https://download.wpsoftware.net/bitcoin/pos.pdf

然而，我们也需要考虑系统风险。虽然我们假定不同供应商不可能一起运行节点，但这一情况也可能发生。同时，大量节点也可能会由于当天零利用而被归并在一起。基于签名的共识（如 PBFT 和 PoS）出现灾难式的故障，使得整个链失效。

We need an additional mechanism to harden security. Proof-of-Work has the properties we want: even if a PoW miner is compromised, an attacker still has no power over blocks which are already mined, he will have to re-do the work to overwrite them.
我们需要附加的机制来巩固安全性。工作量证明拥有我们所需的属性：即使一个 PoW 矿工被破解，攻击者仍无法跨越已开采的区块，他必须不断地重写。

We can improve the security of a signature-based consensus by anchoring blocks in a PoW-based blockchain, such as Bitcoin or Ethereum. This can be done cheaply -- a single Bitcoin transaction anchoring the entirety of Chromia every few blocks costs very little -- and it will guarantee that Chromia confirmation strength will be *at least as strong as Bitcoin* for blocks which are anchored. For example, a user who makes high-value transactions and prefers to rely on Bitcoin security can wait until an incoming payment is confirmed via Bitcoin anchoring before they send goods.
我们可以通过在比特币或以太坊这样基于 PoW 的区块链上锚区块来提升基于签名的共识安全性。这可以以廉价的方式来实现，用单笔比特币交易来锚 Chromia 的一部分区块花费很少，而且还可保证 Chromia 的确认优势至少和比特币所锚的区块相当。例如，一个信赖比特币安全性的用户如果进行高值交易时，他可以等到通过比特币锚定的应收账款确认后再发货。

Node compensation 节点补偿

Nodes will be compensated for hosting dapps, each dapp requires computational resources and storage and should be able to pay providers for them. Chromia will establish a market-place where providers can offer capacity of their nodes.
代管分散应用程序的节点可以得到补偿，每一个分散应用程序都需要计算资源和存储，并给供应商们支付这些服务。Chromia 会为供应商们提供一个市场，用来销售他们节点的容量。

Initially ChromaWay will offer nodes, later we anticipate more providers to join. We anticipate that in the long run the cost of using node resources will roughly match the cost of cloud computing such as AWS EC2.
最初幻彩大道会提供节点，之后我们期望更多的供应商加入。从长远看，我们预估使用节点资源的成本将和 AWS EC2 这样的云计算成本相差无几。

Miscellaneous features 其他特征

We believe that to meet the requirements of high performance decentralized applications Chromia has to meet the following requirements:
要想达到分散应用程序的高性能要求，Chromia 必须满足以下要求：

- Confirmation time: ~1 second (necessary for good UX, real-time user interactivity…)
  确认时间：1 秒左右（对好的用户体验和实时用户交互是有必要的）

- Transaction rate: >500 TPS per sidechain. Overall rate in the whole system is unlimited.
  交易率：每侧链大于 500 TPS。整个系统的总比率是没有限制的。
- IO capacity: >100k updates and reads per second
  IO 容量：每秒写读大于 100k

Preliminary tests of the Postchain framework demonstrate that it is possible to meet and exceed these requirements.
后链框架的前期测试表明满足和超过这些要求是可能的。

Chromia will also come with a client SDK which supports development of the client side of decentralized applications. SDKs will be offered for JavaScript (to enable browser-based apps), Java and other languages. The SDK will also enable platform-wide single-sign-on and a wallet for key management to spare users the hassle of registering in each app separately.
Chromia 同时会有客户软件开发包用以支持客户端分散应用程序的发展。软件开发包将提供 Java 脚本、Java 和其他语言。软件开发包还支持平台范围内单点登录和钱包钥匙管理，分散用户在每一应用程序单独注册的困扰。

Decentralized applications 分散应用程序

We assume that the reader of this document is already familiar with the concept of a decentralized application. Nevertheless, it makes sense to clarify to what exactly we refer, as it is connected intimately to the goal of the platform.
我们假定阅读此文的读者已熟悉分散应用程序的概念。尽管如此，由于它和我们的平台目标紧密相关，所以还是在此解释阐明我们所真正引用的分散应用程序。

By ‘decentralized application’ we mean a multi-user application which is hosted and provided in a decentralized way. That is, no single entity should have control over functionality of such an application.
所谓“分散应用程序”，是指一个多用户应用程序，以去中心化的方式运行和提供服务。这意味着任何个体都无法对该应用程序有百分百的操控权。

The problem with traditional centralized applications is that the party which controls the underlying services can:
传统中心化应用程序的问题在于，控制基础服务的一方能够：

- Shut down the application 关闭应用程序
- Deny service to certain categories of users 拒绝某些用户群的服务
- Monetize users by violating their privacy 通过侵犯隐私将用户货币化
- Remove functionality which is valued by users 移除对用户来说有价值的功能

Open source and peer-to-peer software addressed the centralized control issue for certain categories of apps, such as office software and file sharing. But software which relies on

server-hosted databases is much harder to tackle, particularly because it's hard to decentralize databases.
开放源代码和点对点软件解决了办公软件、文件共享等应用程序的中心化控制问题。而依靠服务器代管型数据库的软件要更难处理，尤其因为很难将数据库去中心化。

One of the earliest and most important examples of an "application" depending on a centralized and broadly accessible database is digital money. It is essential that every participant in a system of digital money can have certainty about the state of the database, namely, how much money does each participant have. Bitcoin was the first specimen of the new generation of software which combined open source, peer-to-peer tech and consensus algorithms to create money outside of the control of centralized entities.
数字货币是最早期也是最重要的一个依靠中心化被广泛熟知的数据库的"应用程序"例子。数字货币系统里的每个用户能清楚数据库的状态，也就是用户拥有多少货币。比特币作为开创软件新时代的标杆，将开放源代码、点对点技术和共识运算法则相结合，在中心化个体控制以外制造货币。

Using more advanced decentralized database software it is possible to decentralize even more applications and probably to create completely new kinds of applications which were previously inconceivable.
利用更先进的去中心化数据库软件将有可能分散更多的应用程序，也可能创造以前无法企及的全新种类的应用程序。

We can identify that decentralized applications have the following desirable traits:
分散应用程序有以下优点：

- Not controlled by a single entity. 并非单个个体控制
- Ideally, controlled by the community of users. 理想状态下由用户社区控制
- Cannot be shut down 不可被直接关闭
- Censorship-resistant -- service cannot be denied 抗审查-服务不可被否决
- Transparent, users can see what is going on 透明 – 所有进程用户可见
- Privacy -- users have control over their data 隐私 – 用户可控制自己的数据
- Highly available 高效

We do not expect decentralized applications to have *all* of these features. In fact, some features might contradict each other. For example, a dapp may enable the majority of users to restrict access to a minority, in which case the dapp is controlled by users, but it is not censorship-resistant. In practice application developers aim at a reasonable compromise between decentralization and other priorities.
我们不奢求分散应用程序拥有所有这些特征。事实上，有些特征互相矛盾。例如，一个分散应用程序或许会使大部分用户能限制小部分人的权限，而分散应用程序又是由用户控制的，做不到抗审查。在实际操作中，应用程序开发者们会在去中心化和其他特性中寻求平衡。

Transparent apps 透明的应用程序

Some apps are only partially decentralized: only data which is critical for transparency is hosted in the blockchain, while the rest of the app is centralized. Such applications are better described as transparent apps (tapps) than decentralized apps.
有些应用程序仅仅是部分去中心化：只有需要公开透明的数据才会在区块链上代管，其余部分都是中心化的。这样的应用程序称之为透明应用程序更恰当。

Many apps which are marketed as dapps are in fact tapps. For example, CryptoKitties[13] stores kitty ownership information in the Ethereum blockchain. Is it decentralized? No, not really, because a single company can shut it down. In fact, it can shut it down in several different ways:
市场上许多称之为分散应用程序的其实是透明应用程序。例如，CryptoKitties 在以太坊区块链上存储小猫主人信息。这属于去中心化吗？并不是，因为一个单独的公司就能将其关闭。事实上，它可以以多种方式关闭：

- Client code is not open source, if the CryptoKitties website is shut down it will be impossible to play the game.
  客户节点不是开放源代码，如果 CryptoKitties 的网站出现故障，就没办法继续游戏。
- The company behind CryptoKitties can shut down contracts hosted on Ethereum blockchain.
  CryptoKitties 背后的公司可以停止在以太坊区块链上的代管合约。

Thus, in practice, the only thing which differentiates CryptoKitties from a centralized app is transparency.
因此，CryptoKitties 唯一有别于中心化应用程序的就是它的透明性。

Token model 代币模型

Traditional funding and monetization models do not work well for decentralized applications. The value calculation made in a traditional funding model is based on control of centralized 'property' like data, user-base, intellectual property, and patents. A decentralized application ideally belongs to its users, a diverse group of stakeholders who form some kind of mutually beneficial balance. There is no central party to own assets, add value, and profit from that activity. That's why we need a different kind of funding model which is more compatible with distributed ownership. For ownership to be distributed, it is necessary to denote the proportion of ownership or stake in the system with some sort of liquid or semi-liquid asset. This makes it possible to quantify the stake proportion of a given actor, allows them to add value without controlling or submitting to control, and to exchange that value securely. Usually this is achieved with tokens.
传统的资金和货币化模型对分散应用程序并不适用。传统资金的价值计算模式是基于中心财产的控制，像数据，用户基数，知识产权和专利等。分散应用程序理想状态下属于它的用户们，他们一定程度上形成了利益的相互平衡。没有集中的一方占有财产，增值和从此活动中收益。

[13] A popular game that allows players to purchase, collect, breed and sell various types of virtual cats.
一款流行的游戏，玩家可以购买、收集、饲养和销售各种各样的虚拟猫。
https://www.cryptokitties.co/

这就是为什么我们需要一个不一样的资金模式来更好的与分散的所有权相兼容。对于所有权的分布，有必要对所有权的比例做出指示或者用一定的流动或半流动资产来资助系统。这使得量化投资比例成为可能，并且无需控制或提交控制就能增值，也可安全地进行价值交换。通常，这都靠代币来实现。

On Chromia, dapp tokens can go beyond the basic ICO model:
在 Chromia，分散应用程序代币可实现的不只是基本的 ICO 模型：

1. Issue tokens.发行代币
2. Sell tokens to investors. 向投资者出售代币
3. Do whatever you want with the money. 随意支配货币

Instead of that, Chromia will provide mechanisms which balance the interests of developers and users. Dapp tokens can be automatically backed by Chroma tokens which provide liquidity and value independent of speculative investment into a dapp. Dapp investors can be compensated through a profit-sharing contract. For developers, Chromia offers the opportunity to derive income from dapps. This incentivises the creation and maintenance of high quality dapps because better dapps generate more income and create more demand for tokens owned by the developer. The Chromia model is designed to support sustainable circular economies and foster a mutually beneficial relationship between developers, users, and investors.
相反,Chromia 会提供平衡开发者和用户利益的机制。分散应用程序的代币可以用幻彩代币自动背书，幻彩代币为投机性投资提供流动性和价值独立。分散应用程序投资者能通过分红合约得到补偿。对开发者而言，Chromia 提供了从分散应用程序上获得收入的机会。这激励了高质量的分散应用程序的创造和维系，因为越好的分散应用程序产生越多的收入，创造更多的代币需求。设计出 Chromia 模型是为了支持可持续性循环经济，在开发者、用户和投资者之间营造互惠互利的关系。

The role of Chromia Chromia 的角色

Chromia aims to be the decentralized database component of decentralized applications. A combination of a decentralized database and code, which is run on end-user devices (e.g. mobile or browser app), will typically comprise the entire decentralized application. Let's see how Chromia enables dapp features:
Chromia 力求成为分散应用程序的去中心化数据库组件，终端用户设备（如手机或浏览器）上运行的节点和去中心化数据库的结合将组成整个分散应用程序。让我们一起看看 Chromia 是如何赋能这些应用程序的：

Not controlled by a single entity. 非受控于单个个体

We assume that after creating a dapp, developers would make both front-end and back-end (i.e. parts which run in Chromia) code open source. This allows users to use the app without any further involvement of the original developer.
我们假设在开发了一款应用程序后，开发者们会使前端和后端（在 Chromia 上运行的部分）节点成为开放源码，使得用户们可以自主使用应用程序。

The data which belongs to the app will be hosted by Chromia. This is done in two tiers:

属于某应用程序的数据将会通过 Chromia 进行代管。通过两步骤完成：

1. Chromia root system selects nodes which will run application blockchain, manages token conversion, node compensation and so on.
   Chromia 根系统选取节点来运行应用程序的区块链，完成代币兑换，节点补偿等操作。
2. A set of nodes will manage application data.
   一组节点将管理应用程序数据。

Both these tiers are decentralized cryptoeconomic systems, and thus we can say that the application is not controlled by a single entity. Typically users will pay for the resources necessary to host the application.
这两个层级都属于去中心化加密生态系统，因此我们可以说应用程序并非受控于单一个体。用户们通常要为代管应用程序所需的资源付费。

Of course, application code might grant control to some entities. Ideally the users should demand an independent review and use the application only if control structures are reasonable.
当然，应用程序的节点也可能要保证对多个个体的控制。理论上，用户们需要完成独立的审核，并且只有在控制结构合理的情况下使用应用程序。

Controlled by the community of users. 受用户社区控制

Chromia will include optional governance mechanisms which will allow users to control various aspects of application functionality. For example, code upgrades.
Chromia 将搭载选择性管理机制，允许用户们控制应用程序功能的多个方面，如节点升级。

Cannot be shut down. 不可关闭

As mentioned above, Chromia enables decentralized application hosting, thus a single entity cannot shut down an application. But we cannot guarantee that an application cannot be shut down by legal action. Chromia root structures will be dominated by few companies (at least within first few years of its existence) which have to comply with laws. Thus an application might have to be evicted from Chromia.
如上所述，Chromia 实现了分散应用程序代管，因此任何单一的个体都无法关闭应用程序。但是我们无法保证应用程序通过法律途径被关闭。Chromia 根结构将会由一些合法的公司来主导（至少在前期的几年内）。所以，某一应用程序将有可能不得不从 Chromia 中驱逐出去。

We should note, however, that application fundamentally belongs to users. Chromia is a public hosting platform and completely open source. If users disagree with a government decision to shut down the application, they can simply move their data elsewhere, i.e. they can set up a different Polis (similar to a fork in a traditional blockchain) in a different jurisdiction. As long as users have a need for an application and are willing to support it, it cannot be shut down.
然而，需要注意的是，应用程序本质上归属于用户们。Chromia 只是一个公共的代管平台和开放源码。如果用户们对政府关闭应用程序有疑问，可以将自己的数据转移到其他地方。他们可

以在其他管辖区域建立不同的城邦（类似于传统区块链中的叉形指令）。只要用户对应用程序有需求并且愿意支持它，它就不会被关闭。

Censorship-resistant. 抗审查

In the Chromia model, application developers will typically delegate operations to nodes. Nodes process user requests using a consensus mechanism. Thus neither developers nor nodes have the ability to implement censorship on a whim.
在 Chromia 模型中，应用程序开发者将实际操作委托给节点。节点运用共识机制处理用户的请求。因此，不管是开发者还是节点都不可以随机进行审查。

It is theoretically possible that multiple nodes can collude to implement censorship, but then users can demand that the application be moved to other nodes. Of course, it is possible that an application would have some censorship components (anti-spam, anti-abuse, etc.) as features. What is reasonable depends on the particular application. If users believe that censorship is unwarranted, they can fork the application and host an updated version.
理论上来说，多个节点可以联合进行审查，但是用户可以要求将应用程序移至其他节点。当然，应用程序可以有一些审查组件（如反垃圾邮件、反欺凌等）的特性。是否合理取决于特定的应用程序。如果用户认为审查是无保证的，他们可以分叉应用程序并执行更新的版本。

Transparent. 透明的

Application data will be hosted on multiple nodes and blockchain consensus makes it immutable once it's finalized. We believe that many applications will have transparency as the only feature. Chromia is a neutral technology provider, it doesn't by itself enforce decentralization. In many cases transparency is already a huge improvement over the status quo.
应用程序数据在多个节点上代管，区块链共识使得一旦确定后就不可更改。许多应用程序将透明度作为其唯一特性。Chromia 是一个中和技术供应商，它自身不执行去中心化。许多案例中，透明度目前已经得到了巨大改善。

Privacy. 隐私

Privacy is a complex topic. Decentralized application data is typically public, thus the application has to be engineered with that in mind. For example, it might use pseudonymous identities, cryptographic constructs such as hashing, zero-knowledge proofs and so on.
隐私是一个复杂的话题。分散应用程序数据是典型的公共数据，编制应用程序的时候就该考虑到这一点。例如，它可能会使用虚拟身份，加密图形构图，如散列法、零知识证明等。

We believe that this approach is better than a traditional approach based on trust and secrecy of application providers. If a provider's security is breached, privacy is 100% compromised. On the other hand, if data is public in the first place, it cannot be compromised.
我们认为此方法在应用程序供应商信任度和保密性上要优于传统方法。如果供应商的安全被破坏，那么隐私将肯定会被盗取。相反，如果数据原本就是公开的，那就无法被盗取。

Chromia plans to offer privacy-enhancing features (for use in dapps) in future.
Chromia 计划未来推出隐私提升特性。

Highly available.高效

Chromia is designed to withstand node failures. The number of failures it can withstand is a configurable parameter. Minimal number of nodes is four, at that point it can withstand one node failure. If higher availability is desired, a higher number of nodes can be used.
Chromia 设计了节点失效抵挡。可抵挡的节点失效数量是一个可配置参数。最小值是四，到达该值时，可抵挡一个节点失效。如果有更高的需求，可以使用更多的节点。

Decentralization quality 去中心化质量

As we mentioned above, applications can be decentralized to various extents. Chromia aims to be a neutral technical platform rather than as a moral authority, thus it will allow applications to be hosted regardless of their decentralization level.
如上所述，应用程序可去中心化至不同的层级。Chromia 力求成为中和的技术平台，而非道德权威，因此它所代管的应用程序不受分权层级的限制。

However, we believe that decentralization is important, and it's important for users to know features of application they are using. For this reason, we plan to develop guidelines and evaluation criteria. Independent companies will be able to rank applications on these criteria. We also encourage users to demand an independent code audit.
但是我们知道去中心化十分重要，用户们需要了解他们所使用的应用程序特性。为此，我们计划创建指南和评估标准。独立的公司可以对应用程序进行评分。我们同时也鼓励用户们请求独立代码审计。

Platform architecture 平台架构

In this section we describe the platform architecture, expanding on the "Design rationale" section.
这一章节，我们讨论平台架构，是对设计原理章节加以展开。

Postchain 后链

Chromia is based on the Postchain[14] framework. Postchain defines interfaces between the components of a blockchain-based system and provides a number of building blocks for networking, consensus, cryptography, etc.
Chromia 基于后链框架。后链定义了区块链系统组件之间的接口，为网络、共识、加密图形等提供了一系列构建区块。

The main difference between Postchain and other blockchain frameworks is that Postchain is designed to store blockchain data (both raw blockchain contents and application state) in a relational database. Not only that, Postchain allows transaction logic and consensus to be fully aligned with a relational database; e.g. transactions which violate constraints in the database are rejected and excluded from consensus, they do not result in fatal errors of any kind.

[14] Source code can be found at 源代码可访问以下链接 https://bitbucket.org/chromawallet/postchain2/

与其他区块链框架的主要区别在于后链是在关系数据库上存储区块链数据（原始区块链内容和应用程序状态）。不仅如此，后链使得交易逻辑与共识和关系数据库完全统一。例如，在数据库中违反约束条件的交易将会被拒绝，并从共识中剔除，它们不会导致任何的致命错误。

Postchain is implemented largely in Kotlin and runs on the JVM. The JVM is one of the most commonly used virtual machines, it's geared towards server use cases and has a large number of libraries available. The JVM provides inherent protection against vulnerabilities such as buffer overruns/underruns, data leaks and so on -- it controls access to objects, performs array bounds checking and does not expose error-prone features such as raw pointers. Thus apps implemented on the JVM are usually free of problems such as remote code execution even when they contain bugs. This is very important for blockchain software as remote code execution can lead to huge losses.
后链在 Kotlin 上广泛运用并在 JVM 上运行。JVM 是最常用的虚拟机之一，它指向服务器使用案例，且有大量可用的程序库。JVM 对脆弱性起内在保护的作用，如缓冲器超限或欠载，数据流失等情况。它控制访问对象，开展数组界检查，不会暴露像原始指针这样的易错特性。因此，在 JVM 上运行的应用程序通常不会有远程代码执行等这样的问题，即使他们本身带有故障。这对区块链软件至关重要，因为远程代码执行可能导致巨大的损失。

Kotlin further tightens type checks and particularly ensures null safety within the code written in Kotlin. We believe that use of modern programming language designed for safety can reduce number of defects and help to make sure remaining defects do not lead to drastic consequences.
Kotlin 更注重类别检查，尤其是确保代码里的空值安全。现代安全编程语言的使用能够减少缺陷数量并确保现存的缺陷不会酿成严重的后果。

Postchain allows multiple blockchain to be hosted in a single database and allows one blockchain to "see" data belonging to another blockchain when that data is final (committed). This simplifies implementation of inter-blockchain interaction, as blockchains can refer to shared data without any additional overhead or complexity. In particular, this can be used for inter-blockchain asset transfers.
后链允许多个区块链在一个数据库上代管，且一个区块链能够"看到"另一个区块链上的最终数据。这简化了区块链间交互的操作，因为区块链无需另加费用或复杂操作就可参考共享数据。尤其可用在区块链间的资产转移。

Chains 链

Splitting into multiple blockchains helps Chromia to achieve horizontal scalability as each node will only need to work with data corresponding to blockchains it needs to work with, thus increasing the number of nodes and blockchains can increase scalability. This architecture also makes updates simpler, as an update of a single blockchain will have no effect on others.
拆分多个区块链帮助 Chromia 实现了横向扩展，每个节点只要与其工作的区块链相关数据相匹配就行，这样就可增加许多节点和区块链的数量。这样的架构也使更新更加简单，单一区块链的更新不会对其他区块链造成影响。

The overall system consists from a number of “system” blockchains which are essential for Chromia functionality and a number of application blockchains which are specific to particular applications.
整个系统包含了若干 Chromia 功能块所需的“系统”区块链和若干针对特定应用程序的应用程序区块链。

System chains: 系统链

Root chain. 根链

Validators: root nodes. 验证器：根节点

Purpose: keep track of the list of root nodes. 目的：追踪根节点

Description: The root chain is needed for thin clients to be able to validate any data within Chromia without downloading the entire blockchain.
描述：根链是为了使小客户在无需下载整个区块链的情况下验证 Chromia 上的任何数据。

Directory chain. 目录链

Validators: root nodes. 验证器：根节点

Purpose: keep track of all providers, nodes, application blockchains and their validators.
目的：追踪所有的供应商、节点、应用程序区块链和他们的验证器

Description: The directory chain is responsible for keeping track of all critical information and orchestrating the operations of the system.
描述：目录链负责追踪所有重要信息，协调系统的运行。

Token root chain. 代币根链

Validators: as defined in directory. 验证器：如目录中定义

Purpose: keep track of Chroma tokens.目的：追踪幻彩代币

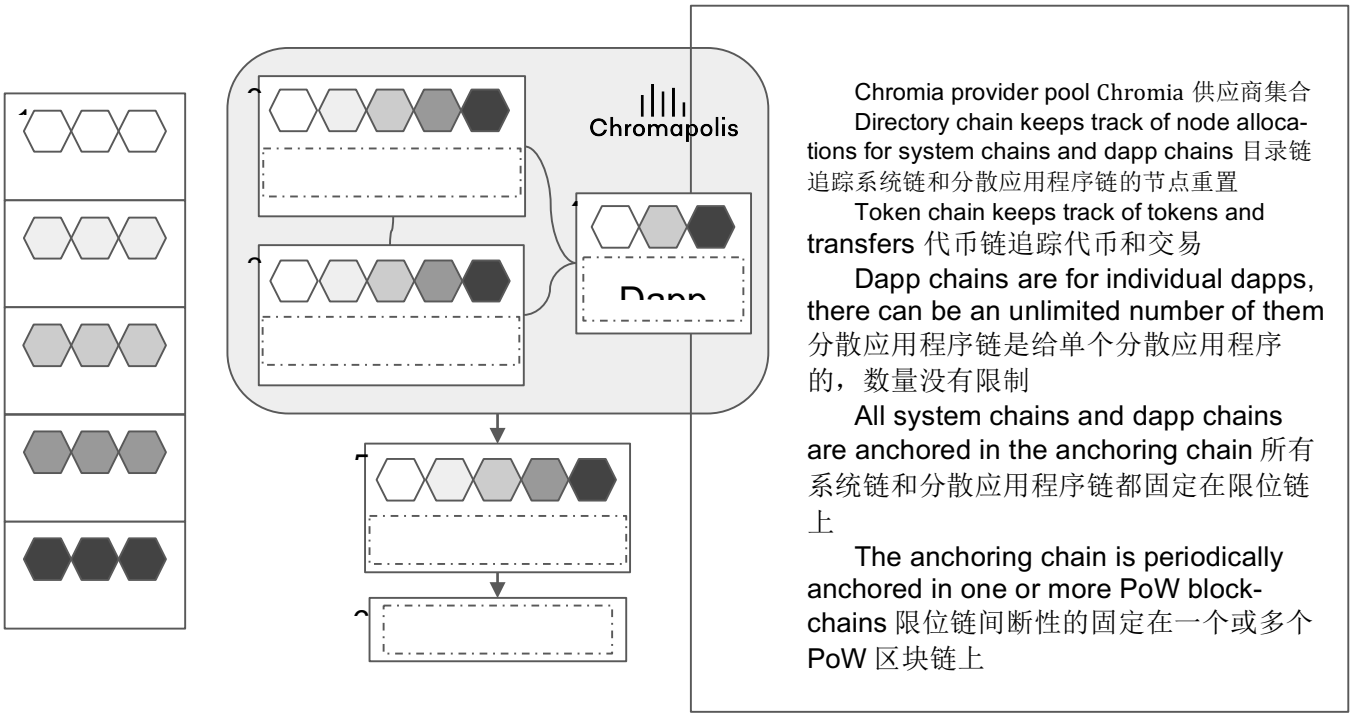
Description: The token root chain keeps track of token distribution between other chains.
描述：代币根链追踪其他链之间代币的分配。

Anchoring chain. 限位链

Validators: as defined in directory. 验证器：如目录中定义

Purpose: Defend against attacks on a subset of nodes. 目的：防卫子节点上的攻击

Description: The anchoring chain records hashes of blocks of other chains. This makes it possible to detect consensus failures. In case of a consensus failure, blocks anchored in the anchoring chain take precedence over other versions of blocks. The anchoring chain is itself anchored in Bitcoin & Ethereum blockchains.
描述：限位链记录其他链上块的散列。这使得监测共识故障成为可能。如果共识故障，在限位链上的区块优先使用其他版本的区块。限位链本身是在比特币和以太坊区块链上。



(Security considerations related to the maintenance of multiple chains are explained in a separate section.)
（有关不同链维护的安全性考虑会有单独的章节做说明）

Node implementation 节点实施

The data model and operations needed for system functionality such as node selection and rewards can be implemented in Rell. Use of a high-level, declarative language can simplify the implementation and reduce the possibility of defects.
数据模型和节点选择与奖励这样的系统功能操作可以在 Rell 上实现。高水平说明性语言的使用可简化其实施并减少出错的概率。

Interaction with other blockchains 与其他区块链的交互

Interaction with the Bitcoin and Ethereum blockchains are needed for anchoring. Ethereum interaction is needed to allow ETH to be used for payments within Chromia and for Chroma as an ERC20 token. This functionality can be implemented via indexers: nodes which have to interact with Ethereum need to run an Ethereum node in parallel to Chromia node and import information from the Ethereum blockchain to the Chromia database.
为了锚定，需要与比特币和以太坊区块链进行交互。与以太坊的交互是为了使 ETH 支付能在 Chromia 上使用，并把幻彩作为 ERC20 代币。这一功能可以通过分度器来实施：与以太坊交互的节点必须运行一个与 Chromia 平行的以太坊节点，从以太坊区块链向 Chromia 数据库输入信息。

Components 组件

The following is a list of software components which we plan to implement for the Chromia MVP release:
以下的软件组件清单是我们计划为 ChromiaMVP 发布所运用的：

1. Rell compiler and runtime environment Rell 编译程序和运行时间环境
2. Rell IDE: tooling which makes development easy Rell IDE: 使开发更容易的工具
3. Client SDK: allows front-end (web or mobile app) to connect and interact with Chromia. 客户 SDK：允许前端（网页或手机 APP）与 Chromia 连接和交互
4. Chromia node, system chains Chromia 节点：系统链
5. Bitcoin & Ethereum support needed for anchoring 为锚定做支持的比特币和以太坊
6. Chroma ERC20 contract, gateway on Chromia side Chromia 方的幻彩 ERC20 合约和网关
7. Auto-conversion smart contract on Ethereum 以太坊上自动兑换智能合约

Governance 管理

There is a need for governance on both the system and application level.
系统和应用程序层面都存在管理需求。

Chromia system governance Chromia 系统管理

System-level governance covers the following topics:
系统层级的管理包括以下方面：

1. System updates, that is, updates to system blockchain structures, their rules and so on.
   系统更新：系统区块链架构、规则等的更新
2. Tuning parameters such as the price of running a dapp according to economic realities.
   协调参数，如根据市场情况确定运行分散应用程序的价格
3. Acceptance of new members into the system.
   系统新成员的加入
4. Exclusion of bad actors.
   不良用户的剔除

Obviously, governance must be decentralized, a single entity shouldn't have control over the system. We believe that providers are in the best position to perform governance duties:
显然，管理必须去中心化，单一的个体不该控制整个系统。供应商是履行管理职责的最佳人选：

- They can professionally review the proposals. 他们能够专业的审核提案。

- They are motivated to keep Chromia interesting both for users and for application developers. A bad governance decision will affect revenues and profits collected by providers. 他们有动力使 Chromia 对用户和应用程序开发者保持吸引力。不良的管理决策会影响供应商的收入和利润。

Thus we can require ⅔ of providers to vote in favor of a governance proposal to approve it.
所以，我们可以要求三分之二的供应商投票赞成管理提案才可通过。

Initial centralization 初始中心化

The initial launch of Chromia MVP will likely not have a sufficient quantity of independent providers. Thus at the initial stage governance will be centralized: all decisions will be made by ChromaWay in consultation with system stakeholders. Transition to proper decentralized governance will happen when the system is ready from a technical perspective and the provider ecosystem is healthy.
ChromiaMVP 发起的初始阶段可能不会有足够多的独立供应商。所以在初期阶段将集中管理：所有决定都由幻彩大道向系统股东咨询后作出。当系统从技术角度已准备就绪并且供应商生态系统健康的状态下将会考虑向去中心化管理转变。

Rejected alternatives 被否决的选择

Stake / coin voting 赌注、钱币投票

A widespread governance model in blockchains which do have on-chain governance is stakeholder vote or “coin voting”. This is particularly common in DPoS blockchains since stakeholder voting is an essential part of Sybil control & consensus mechanisms. We thoroughly considered this model and rejected it for the following reasons:
区块链上大范围的线上管理模型叫做股东投票或“钱币投票”。它在 DPoS 区块链上相当常见，因为股东投票是 Sybil 控制和共识机制的必要组成部分。我们充分考虑了该模型，拒绝理由如下：

1. Usually it is not possible to control stake decentralization, i.e. tokens might be concentrated in a few hands, therefore it cannot guarantee decentralized governance.
   通常没办法控制赌注的去中心化，例如代币有可能会集中在某一部分人手中，因此无法保证去中心化管理。
2. It’s not fair in the sense that rich stakeholders have more power.
   富有的股东拥有更多的权力这不公平。
3. Many users keep their tokens on exchanges, essentially allowing exchanges to vote for them.
   许多用户都拿他们的代币进行兑换，本质上允许了用兑换来投票。
4. DPoS style voting seems to be particularly prone to problems with bribes, cartels and centralization. These problems have been actually observed in the wild.
   DPoS 型的投票似乎更会带来贿赂、垄断、集权等问题。这些问题实际却是在自然环境中比较突出。

5. Even if tokens were more-or-less evenly spread, few users actually go through a hassle of voting, few users can understand the proposals, etc. This was demonstrated in the DAO case.
   即使代币或多或少被平均分布，很少有用户会进行复杂的投票，也很少有用户能理解提案等。DAO 的案例足以说明这点。

No formal governance 没有正式的管理

Some cryptocurrencies, e.g. Bitcoin, take pride in having no formal governance. It might work fine if all they want is “digital gold” -- after all, gold itself has no governance. But Chromia is more complex, and it needs to be able to respond to challenges in a timely and coordinated manner, thus Chromia needs a formal governance system.
像比特币这样的一些加密货币以没有正式的管理引以为傲。如果他们所想要的只是“数字黄金”，那或许能行得通，毕竟黄金本身没有管理。但是 Chromia 更为复杂，它需要及时应对挑战，所以需要有正式的管理体系。

Unique users 独特的用户

It’s tempting to give one vote to each user -- thus making governance fairer than “voting with money”. But it’s impossible to identify unique users in a decentralized setting, and many issues related to stake voting still apply. Particularly, users might be not informed enough to make good decisions.
给每个用户投票权相当有吸引力，比“用钱投票”来的更加公平。但在去中心化的设置中识别独特的用户不太现实，许多股份投票仍会应用。尤其是用户做出好的决策时可能信息未被充分告知。

Still, we plan to experiment with this kind of governance: our plan is to identify a set of users who actively want to participate in governance -- “citizens of Chromia”. Sybil control can be implemented by keeping track of the social graph. We have no immediate plan to give these users any formal governance power, but they can cast advisory votes.
我们仍旧计划尝试这种管理：我们准备选出一部分主动想要参与管理的用户，称其为“Chromia 公民”。Sybil 控制可以通过追踪社交图谱来实现。我们不会立即给这些用户正式管理的权力，但他们可以投建议票。

Application governance 应用程序管理

Different applications have different governance needs:
不同的应用程序有不同的管理需求：

1. Some are designed to be *immutable* and thus would require no governance at all.
   有些应用程序的设计是不可变的，所以根本不需要管理。
2. Other might exercise direct democracy and give each user a right to vote.
   其他可能采取直接民主，给每个用户投票的权利
3. Another option is to implement weighted voting, e.g. proportional to tokens one has.
   另外一种方式是实行权重投票，如按照拥有的代币比例。
4. Dapp developers can also play a role in governance, and either:

分散应用程序开发者也可履行管理的职责：

a. Maintain full control 要么全面控制
b. Work together with users through voting, e.g. developer makes proposals which users can approve or reject 要么和用户通过投票来协作，如开发者制定提案，用户可以通过或否决

We want to give developers and users an ability to decide for themselves and experiment with different forms of governance as they please.However, we want to ensure that users always have certain freedoms:
我们希望能让开发者和用户有自己做决定的权利，也能体验不同模式的管理。期望用户始终享有一定程度的自由：

1. The freedom to access and copy application data. This is an inherent property of a public blockchain. 获取和拷贝应用程序数据的自由。这是公有区块链的固有资产。
2. The freedom to fork the application. This is an inherent property of free and open source software and public data: anyone can make a modified copy of software and run it on a copy of data. 叉形应用程序的自由。这是自由、开放式软件和公共数据的固有资产，任何人都可以修改软件备份并在数据备份上运行。

Thus we do not impose any restrictions which aren't an inherent property of applications running on public blockchains.
我们不在公有区块链的应用程序上强加任何限制。

Chromia will provide tooling which would give users an ability to fork a dapp if they are displeased with its governance or just want to experiment with something different. Our goal is to make sure that this forking can be done in a smooth and civil manner.
如果用户对管理不满或者仅仅是想要有不同的体验，Chromia 提供了可以让用户叉形分散应用程序的工具。我们的目标是确保这样的叉形指令可以平稳地进行。

Uses 使用

Chromia is a general purpose platform suitable for a wide range of applications. But we live in a world with many competing blockchains, thus it makes sense to focus on relative strengths:
Chromia 是一通用的平台，为大多数应用程序所适用。但是我们有许多的竞争对手，这促使我们关注于我们的优势：

- Chromia is database-centric, as such it is particularly suited for applications which are similar to databases in their nature, or deal with complex data schema, complex queries, indexing and so on.
  Chromia 是以数据库为中心的，尤其适合本质上与数据库类似的应用程序或是处理复杂数据架构、复杂查询和检索等的应用程序。

- Chromia has excellent data read-write capacity, thus it's uniquely suitable for applications which require operating on large amounts of data.
  Chromia 有卓越的数据读写能力，适合有大量数据处理需求的应用程序。
- Chromia allows both fast queries and fast confirmations. Thus it is suitable for interactive applications where data needs to be displayed and updated within seconds.
  Chromia 支持快速查询和快速确认，因此适合数据需要在数秒内展示和更新的交互类应用程序。
- Chromia is very flexible in terms of resource use policies, thus it can accommodate different business models which do not work on the previous generation of blockchains.
  Chromia 在资源使用政策上十分灵活，它可以适应不同的商业模式，这在以往的区块链上是做不到的。

Tokens 代 币

Tokens are the bread and butter of blockchains.
代币如同区块链的面包和黄油。

- High capacity: we aim to support 50 million token transfers per day per blockchain in MVP version of software. This isn't a world record, but it should be enough to support large user bases. Token transfer capacity can be further improved in future versions.
  大容量：在 MVP 版软件上，我们计划每一区块链每天能支持 5 千万代币交易。这并非是世界纪录，但足以支持大用户基数。代币交易容量在未来的版本里还可得到进一步提升。
- Low latency: transfers can be confirmed within 2 seconds which should be enough to support in-person payments.
  低延时：交易可在 2 秒内确认，这足以支持个人支付。
- Flexibility: token implementation is fully programmable, any imaginable feature can be implemented.
  灵活性：代币实施是完全可设计的，任何可能的特性都可以被实现。
- Custom fee policies: fee policy is decided on a per-dapp basis. This means that transfers can be free, or subject to a flat fee, or a fee proportional to the trade amount.
  自定义费用政策：费用政策是基于每一个分散应用程序而设置的。这意味着交易可以是免费的

- Native multi-token support and atomic swapping: trustless token exchange is implemented on transaction format level, it doesn't even require any special support in the dapp.
  本地多种代币支持和原子交换：在交易形式层级实行不可靠代币兑换，在分散应用程序中无需任何特殊支持。
- Inter-blockchain transfer: tokens can be moved between different blockchains within Chromia. Non-Chromia blockchains can be supported in future.
  区块链内转移：在 Chromia 上代币可以在不同区块链之间转移。未来也可以支持非 Chromia 区块链。
- Thin wallet support: a thin wallet (e.g. mobile or browser wallet) can validate transfers within seconds, without syncing with a blockchain.
  小钱包支持：小钱包可以在数秒内验证转移，无需与区块链同步。

Games 游戏

Blockchain-based gaming is a fast-growing sector of the crypto economy, but current blockchain technology severely limits what games can offer. Typically a blockchain is used only to host tradable tokens, while the actual gameplay happens outside of blockchain.
基于区块链的游戏是加密经济行业快速发展的区段，但是现在的区块链技术严重限制了游戏。区块链仅仅用来代管可交易的代币，而实际的游戏玩法发生的区块链以外。

Chromia can allow much more advanced kinds of games where the entire game world can be hosted within the blockchain, evolving over time according to predefined rules. Updating the game state every cycle requires a number of read and write operations proportional to the number of units in the game. This means that blockchains which do not have high read/write capacity can support relatively few units/players.
Chromia 可以运行更高级别的游戏，整个游戏世界都可以代管在区块链中，并按照既定的规则顺势向前发展。每个周期更新游戏状态都要根据游戏中单元的数量而进行一系列的读写操作。这意味着没有交钱读写能力的区块链仅能支持相对有限的单元或玩家。

On the EVM, loading and storing a memory cell which is already non-empty costs 5200 gas. The block gas limit at the time of writing is 8,000,000. Thus Ethereum can do at most 1500 read/write operations per block. If the entire Ethereum blockchain was dedicated to a single game, at most 6000 units could be updated (e.g. moved) per minute. A Proof-of-authority public blockchain called GoChain offers 136500000 gas per block and 5 second inter-block interval. This implies 5250 cell updates per second.
在 EVM 上，加载和储存一个非空的存储单元需要消耗 5200 gas。编写区块时设置的 gas 总量为 8000000。以太坊每个区块至多执行 1500 个读写操作。如果整个以太坊上的区块链单独分配给一个游戏，那么每分钟最多可以进行 6000 单元更新。一个叫做 Go 链的共有区块链给每个区块提供 136500000 gas 和 5 秒的块间间隔。这意味着每秒 5250 单元的更新。

For Chromia we target at least 100,000 cell updates per second in the MVP release, offering capacity that is twenty times higher than the best available public EVM-based chains. We plan to increase this number in future with optimized in-memory blockchain state storage.
对 Chromia 而言，我们的目标是在发行的 MVP 上至少完成每秒 100000 单元的更新，比现有最好的公有基于 EVM 的链能力高出 20 倍。我们计划在未来随着内存区块链存储的优化，这一数字能进一步增加。

Here's a list of Chromia benefits for gaming applications:
以下是 Chromia 所能带给游戏应用程序的好处：

- Fast game client load (thanks to advanced query capability the entire game state relevant to the user can be transferred to the client in a matter of seconds)
  快速的游戏客户加载（得益于高级查询能力，跟用户相关的整个游戏状态能在数秒内传递给客户）
- Interactivity: updates can be confirmed within seconds, data can be retrieved from blockchain within seconds
  交互性：更新可以在数秒内确认，数据也可在数秒内从区块链上获取
- High read & write capacity (upwards of 100k updates per second)
  高读写能力（每秒高达 100k 的更新）
- Good support for complex data schemas needed to support game worlds
  为游戏世界提供复杂数据图解的良好支持
- Ability to update code over time
  随时间更新的能力
- Comes with game token pegging contracts which can create automatic liquidity for game tokens. Token use in games will be covered in more detail in the "Token" section.
  拥有游戏代币固定合约，能为游戏代币创造自动流量。游戏中代币的使用将在"代币"章节做详细介绍。

Business uses 商业用途

Based on our experience with enterprise blockchain applications, we believe Chromia can be used in applications where data is either open, or can be openly hosted in encrypted form, or only commitments (hashes) need to be revealed. This can be particularly relevant in applications which are connected to transparency. Indeed, publishing data via a private blockchain hardly makes things more transparent.
根据我们在企业区块链应用程序方面的经验，我们相信 Chromia 可以运用于多种多样的应用程序。不管是数据对外开放的，还是以加密形式公开代管的，更或者是只有承诺需要被披露。这跟应用程序的透明度密切相关。事实上，通过私有区块链来公布数据几乎不可能使事情更透明。

ChromaWay is planning to offer Chromia-based storage option for its Esplix business contract platform, thus allowing businesses to utilize Esplix contracts without a hassle of running their own blockchain nodes.
幻彩大道打算为 Chromia 上的存储选择提供 Esplix 商务合约平台，这样就使企业能在不运行自己区块链节点的情况下使用 Esplix 合约。

Tokens and incentives 代币和激励

Similar to how tokens are used in Ethereum to pay transaction fees and compensate block producers, Chroma tokens are used in Chromia to compensate block-producing nodes.
But there is a difference: in the Ethereum model, fees are paid directly by users who make transactions. In Chromia, fees are paid by dapps, which can in their turn collect fees from users. This is discussed in more detail in the next section.
类似于以太坊上代币用来支付交易费和补偿区块生产者，幻彩代币在 Chromia 上用力补偿区块生产节点。但是不同之处在于：在以太坊模型中，费用是直接由进行交易的用户支付的。而在 Chromia 中是由分散应用程序支付的，他们可以从用户那儿搜集这部分费用。具体情况将在下一章节详细讨论。

Fees 费用

Application fee models 应用程序费用模型

In Chromia, users pay fees indirectly:
在 Chromia，用户间接支付：

1. The dapp pays to nodes hosting fees. Fee is paid from dapp token account on a daily basis and depends on computational resources requested by the application and used data volume.

   分散应用程序支付节点代管费。费用每天从分散应用程序的代币账户中扣除，扣除的依据是应用程序所要求的计算资源和使用的数据量。

2. The dapp itself can collect fees from users according to its own policies

   分散应用程序可根据自己的政策向用户收取这部分费用

This means that there's no system-wide fee policy for users. Dapp developers are free to implement any policy they want. We believe following fee models might be relevant:
这意味着对于用户而言没有系统层面的政策费用。分散应用程序开发者可制定任何他们想要的政策。以下的一些费用模型可能会用到：

1. Classic model: fees are paid for each performed action. Unlike in Bitcoin and Ethereum the price can be fixed, fees do not need to be demand-based.

   传统模型：根据每一操作收取费用。不同于比特币和以太坊，这里的价格可以是固定的，不会按需定价。

2. Subscription model: user pays a subscription and then can perform actions without additional payments, however, these actions should be rate-limited to prevent abuse. For example, on a Twitter-like service a user might be restricted to 50 messages per day.

   订阅模型：用户可以预付一部分费用，然后再操作时就无需额外付费。但为了防止滥用，这些操作应该有限价。例如，一个像推特这样的服务，或许可以限制用户每天最多发送 50 条信息。

3. Freemium model: certain action might be performed for free, but other actions might require paid subscription. The freemium model is very common for internet businesses.

   免费增值模型：设定一些免费的选项，而其他选项则需要预付费用。免费增值模型在互联网行业十分常见。

4. Subsidized model: an application might collect no fees from users, and instead rely on a pre-funded account provided by a sponsor. This can work well when sponsors derive benefit from users outside of blockchain, e.g. the dapp might be available only to users who bought a physical product. This model could work well with manufacturers of IoT devices sponsoring users who bought the device for use of a related dapp.

   补助模型：一个应用程序也许不向用户收取任何费用，而是依靠赞助商提供的预筹账户。如果赞助商可从区块链以外的用户那儿获取利益，比如分散应用程序仅对购买过实物的用户开放，那么这种模型可以运行的很好。这一模型适用于 IoT 设备的制造商，他们可以赞助购买过产品的用户来使用相关的分散应用程序。

5. Donation-based model: wealthy donors might donate tokens to provide services to users for free.

   基于捐赠的模型：富有的捐赠者或许会为用户免费提供代币。

6. Gameplay-connected: user can pay fees indirectly when they perform game actions:

   游戏设置相关联：用户可以在进行游戏操作时间接支付费用：
   a. Buy in-game items, land, etc 购买游戏装备、土地等
   b. Convert tokens to “game gold” 用代币兑换“金币”
   c. Trade items 交易物品
   d. Pay in-game taxes 支付游戏税费

Hosting fees 代管费

In general, Chromia dapp hosting fees depend not on resources *consumed* by an application, but on resources *allocated* for an application. This is similar to how dedicated and “virtual private” server hosting works: the hosting company doesn’t care what server is actually doing, it wants to be compensated for providing a server. This is also the model used by AWS EC2, Google Cloud Compute Engine and similar services. In the blockchain space, a similar model is used by EOS.

总体而言，Chromia 分散应用程序的代管费不是取决于一个应用程序所消耗的资源，而是取决于为应用程序所配置的资源。这类似于虚拟专有服务器的代管模式：代管公司不考虑服务器实际在做什么，它只是为提供服务器而收取补偿。这一模型也用于 AWS EC2、谷歌云计算引擎以及类似的服务。在区块链空间内，EOS 使用相似的模型。

Applications' needs can be very different. Some applications require a lot of computational resources, some need to process a large number of transactions, some need more storage space, some need a small amount of very fast storage. The kind of hardware which is optimal for an application depends on its requirements.
应用程序的需求千差万别。一些需要大量的计算资源，一些需要处理大量的交易，还有一些需要更多的存储空间，而另一些需要快速存储。应用程序最佳的硬件种类取决于它的要求。

For this reason, we introduce different node classes. Class requirements will likely evolve over time depending on needs of applications, provider capacity, hardware availability, etc. Provisionally, at MVP launch we want to introduce three classes:
为此，我们引入了不同的节点等级。等级需求可能会随着应用程序的需求、服务能力、硬件有效性的变化而随时间发展。暂时来讲，随 MVP 启动的有三个层级：

A. The fastest class for applications which require high transaction rate or expensive processing. Specs: 3+ GHz CPU, two hardware threads per application, NVMe storage.

   给高交易率或昂贵处理的应用程序提供的最快等级。规格：3+ GHz CPU，每个应用程序两条硬件螺纹，NVMe 存储。

B. Medium class. Specs: 2+ GHz CPU, 1.5 hardware threads per application, SSD storage.

   中间等级。规格：2+ GHz CPU，每个应用程序 1.5 条硬件螺纹，SSD 存储。

C. Economy class. Specs: 1+ GHz CPU, equivalent of a single 1 GHz hardware thread per application, SSD storage.

   经济等级。规格：1+ GHz CPU， 每个应用程序 1 条硬件螺纹，SSD 存储。

Application hosting fee paid on daily basis is split into several components:
每日支付的应用程序代管费分成几个部分：

1. Percentage of processing time.处理时间的比例
2. Number of transactions. 交易数量
3. Storage. 存储

Chromia doesn't have the means to precisely measure computational resources "consumed" by an application as this depends on a variety of complex factors which are outside of control of Chromia code (CPU caches, CPU pipelining, OS context switch overhead, DB engine optimizations etc.), instead it will simply measure median time used to process a block as reported by block producer nodes.

Chromia 并没有方法来准确衡量被应用程序所消耗的计算资源，因为这取决于 Chromia 节点控制以外一系列的复杂因素（CPU 缓存、CPU 流水线、OS 上下文转接、DB 引擎优化等）。取而代之的，Chromia 仅仅根据区块生产节点所报告的计算处理区块的中位时间。

When a thread allocated for an application never goes idle (i.e. it continuously builds or applies blocks), the application is using 100% of processing time. In that case it pays a full price for one day of hosting for a particular class.
当应用程序的线路被重新分配，它永远不会闲置（即：它会持续创建或运用区块），应用程序将充分利用处理时间。在该情况下，将全价支付一天的该等级代管费用。

When an application uses less than 100% of processing time, it's eligible for a discount. For class A and B nodes, the discount is limited to 50%. Even if the application is completely idle it still has to pay half of the day hosting price. This is necessary because actual physical resources are allocated to an application whether it uses them or not. A limited discount is provided because we want to encourage applications to be as efficient as possible. Idle time might increase capacity available to other applications, decrease energy consumption and hardware wear.
当应用程序没有百分百使用处理时间时，会有适当的折扣。对于 A 类和 B 类节点，折扣上限是 50%。即使应用程序完全处于闲置状态，还是会收取半天的代管费用。这是合理的，因为不管应用程序使用与否，实际的物理资源都已分配给它。只提供有限的折扣是因为我们想要鼓励应用程序尽可能有效被使用。闲置时间可能会增加其他应用程序可用的容量，降低能量消耗和硬件磨损。

For class C node hosting there is no limit to discount and applications which build no blocks will pay nothing in hosting costs. Additionally, class C allows applications to specify throttling. An application that doesn't want to pay more than 50% of the daily hosting fee can be throttled to use no more than 50% of processing time. Class C nodes will use special algorithms which allow efficient co-hosting of a large number of blockchains. As a result of this, class C nodes target rather than guarantee their posted capacity.
对于 C 类节点的折扣没有限制，没有建立区块的应用程序不需要支付任何代管费用。另外，C 类节点允许应用程序实行指定限流。如果应用程序不愿支付高于 50%的代管费，它可将处理时间限制在 50%以内。C 类节点会使用特殊的运算法则使大批量的区块链有效的完成联合代管。因此，C 类节点是努力完成他们公布的容量目标，而不是保证。

Storage costs and per-transaction costs also depend on the class of nodes used by an application. Hosting 1GB of data on class C nodes will be much cheaper than hosting the same amount of data on class A nodes.
存储费用和每笔交易的费用也取决于应用程序的节点等级。C 类节点上代管 1GB 的数据要比 A 类节点便宜的多。

The hosting price is standardised by selecting the median of prices submitted by all providers. A more sophisticated market which allows providers to auction spare capacity will be developed in the future once the number of providers exceed decentralization needs.
代管价格的标准是选取所有供应商所提交的中间价。一旦供应商的数量超过了去中心化的需求，未来将发展允许供应商拍卖剩余容量的更成熟的市场。

Node incentives 节点奖励

The block building process should be properly incentivized. That is to say, it should not be profitable for nodes to neglect their duties e.g. by making only empty blocks or no blocks at all.
区块的创建流程应适当予以激励。也就是说，节点不应该为了收益而忽略了它们的职责，不该只提供空的区块或压根没有区块。

In theory the collective of providers has an interest in offering a great service to all applications. If applications move to other blockchain platforms, providers cease to make any money. However, we also need to consider providers who might try to cheat the system for individual gain. Beyond the basic incentive to not create invalid blocks or conflicting histories (which can be automatically detected and punished by automatically excluding a node, and possibly its provider, from the system), the system can track the following data:
理论上，供应商团体致力于为所有应用程序提供更好的服务。如果应用程序转移至其他区块链平台，那供应商将没有收入。然而，我们同样要考虑有些供应商为了私人利益会尝试在系统中作弊。为了不创建无效区块和与历史记录相冲突（冲突可以自动检测到并通过从系统中剔除节点或其供应商进行惩罚），系统可以追踪以下数据：

1. Number of blocks built by a node for a particular blockchain as a primary (the role of primary is rotated over time).
   节点为特定区块链所创建的主要区块数量（主要的角色会随时间而循环）
2. Number of transactions in blocks built by a node as a primary.
   节点所创建的主要交易数量
3. Number of commit messages submitted.
   所提交错误信息的数量

This data can be used to detect nodes which neglect their duty as a primary or are not fast enough to submit commit signatures. Nodes which systematically underperform can be excluded automatically or through a providers' vote.
这些数据可以用来监测节点是否忽略了它们最初的职责或提交错误签名速度不够快。总体表现不佳的节点将自动被剔除或通过供应商投票剔除。

Note that nodes of as a whole have an interest in accepting as many transactions as possible and storing as much data as possible as they are paid by number of transactions and storage used.
总的来说节点会接受尽可能多的交易和储存尽可能多的数据，因为他们是按照交易数量和存储空间来收费的。

Another resource which other blockchain systems typically neglect is a node's capability to reply to queries. Indeed, if nodes are compensated only for the amount of data processed, they are incentivized to ignore queries and only process transactions. But if users run light clients, queries are absolutely crucial. We have developed a mechanism which creates an incentive for nodes to reply to queries. It is explained in detail in the Appendix. Simply put,

upon receiving a response from a node a client can discover that this response is “lucky” via a mechanism similar to PoW. Only a fraction of all responses (e.g. 1 in a million) is “lucky”. A lucky response is published in a certain blockchain and yields a small reward both to user and to the node which produced the response. Special provisions (covered in the Appendix) are made to discourage nodes from farming lucky responses on their own.
其他区块链系统所忽略的另一个资源是节点回复查询的能力。事实上，如果节点只是根据处理的数据量来获得补偿，那它们会忽略查询而只处理交易。但如果用户运行的是小客户，那查询就极其重要。我们创建了一个激励节点回复查询的机制。在附录中有详细的介绍。简单来说，当客户收到一个来自节点的回复时，他能通过类似 PoW 的机制来发现该回复是否是“幸运回复”。所有回复中仅有一小部分（如百万分之一）是“幸运回复”。幸运回复会在区块链上公布，并同时给予用户和提供该回复的节点小小的奖励。我们制订特殊条款来制约节点自创幸运回复。
（详见附录）

Node stakes 节点股份

To encourage providers to secure their nodes they will be required to put Chroma tokens into a separate account which represents the provider’s stake in the Chromia economy and is used as collateral which is forfeited when nodes owned by a provider misbehave.
为了鼓励供应商保护他们的节点，他们会要求将幻彩代币存入一个单独账户，作为供应商在 Chromia 经济体中的股份，也是供应商的节点作弊时用做抵押的。

Providers can group nodes into units with different levels of stake: high, medium, low. High-stake nodes should be more thoroughly secured as they can be used for applications highly sensitive to security, such as running system blockchains and high-volume financial dapps. Low-stake nodes can be used for less sensitive dapps such as simple games. Each dapp can specify a minimal stake which is required for nodes which run it. The stake level necessary for system blockchains is set by a council of providers.
供应商可以将节点组成单元，设置不同的股份层级：高、中、低。高股份节点应该被完全保护，它们可以被对安全高度敏感的应用程序使用，例如运行系统区块链和大容量的金融分散应用程序。低股份的节点可以被用到简易游戏之类的低敏感度分散应用程序。节点要求每一个分散应用程序都指定一份最小额度的股份。系统区块链所需要的股份层级由供应商委员会来设定。

Token use in games 游戏中使用的代币

The current generation of blockchain games are based on collectible items and do not offer rich gameplay. We envision a new generation of massive multiplayer online games with rich game worlds hosted within Chromia blockchains, and rich market economies based on tokens and tradeable game items.
目前这一代区块链游戏是基于可收藏的项目，并没有很高的游戏配置。我们预想了一个在 Chromia 区块链上拥有丰富多彩游戏的大型多玩家在线游戏新时代，还拥有基于代币和可交易游戏物品的富有市场经济。

For this kind of game Chromia can offer a set of smart contracts which make game tokens liquid and valuable. This would allow game developers to quickly bootstrap game economies.

For game users, pre-made smart contracts offer a certain degree of stability: they can be sure that game tokens they earn won't lose all of their value overnight due to a poorly coded token structure.
对于这一类的游戏，Chromia 可提供智能合约，使游戏代币能够流通并具有价值。这将使游戏开发者迅速引导游戏经济。对于游戏用户而言，预先制定好的智能合约提供了一定程度的稳定性，他们可以肯定所赚得的游戏代币不会因为差劲的代币架构而一夜之间失去其所有的价值。

At the heart of Chromia game smart contracts, is a market making/token conversion algorithm similar to a widely known "Bancor algorithm" (a similar algorithm was discovered by Chromia team members before Bancor). When Chroma tokens are converted to game tokens (e.g game "gold" tokens), new game tokens are created. Chroma tokens are put into the smart contract reserves and the price is adjusted. Price adjustments work in such a way that higher demand (more people buying game tokens than selling) results in a higher price. When game tokens are converted back to Chroma, the price is reduced. The algorithm can be configured to enable smooth price movement, so the game token price against Chroma cannot drop significantly unless the vast majority of users abandon the game and convert their tokens to Chroma.
Chromia 游戏智能合约的核心是一个代币交换运算法则的市场，该运算法则类似于广为人知的"班克尔运算法则"。（在班克尔之前，Chromia 团队发掘了一种相似的运算法则。）当幻彩代币转换为游戏代币时，新的游戏代币诞生了。幻彩代币被放入智能合约，价格也做了调整。价格调整遵循的是需求越大（买游戏代币的人多于出售的人）价格越高。当游戏代币转换回幻彩代币时，价格被降低了。这样的运算法则能够保证平稳的价格波动，所以游戏代币的价格相较于幻彩代币不会有明显降幅，除非大量用户放弃游戏，将游戏代币转换为幻彩代币。

A fee can be collected upon conversion by adjusting the buy/sell price. For example, a 1% fee can be taken out of the Chroma amount and used to:
通过调整买卖价格来收取一定的兑换手续费。比如，可以从幻彩代币内收取 1%的手续费，用来：

- Pay for game dapp hosting fees (i.e. it's transferred to dapp's hosting account)
  支付游戏分散应用程序代管费（即被转入分散应用程序代管账户）
- Pay the game developer and, possibly, investors
  支付给游戏开发者或是投资者

Game token price increasing with demand means that players have an incentive to invest into game gold. In fact, they have an incentive to discover new interesting games which are going to grow in popularity over time. Indirectly they also have incentive to promote and share the games they play. This set of incentives can result in healthy game community dynamics.
游戏代币随需求增加而增值意味着能刺激玩家投资游戏币。事实上，他们有动力去发掘新的有趣的游戏，这些游戏将来会增加热度。间接的，他们也有动力宣传和分享他们所玩的游戏。这样的激励方式有助于营造健康的游戏社区生态。

The full list of Chromia features developed specifically for use in game applications will be published in a separate paper.
Chromia 为游戏应用程序专门开发的所有特性清单会在单独的文章中发布。

Chroma token economics 幻彩代币经济

To summarize, the Chroma token has the following roles in Chromia:
总而言之，幻彩代币在 Chromia 担任以下角色：

- It is used by dapps to pay hosting fees, thus compensating the nodes.
  用来给分散应用程序支付代管费，从而补偿节点
- It is used as a “standard” currency within the Chromia economy, as dapps can collect it as fees, or use as reserves to peg their own tokens, etc.
  在 Chromia 经济体中被视为“标准”货币，分散应用程序可以将它作为费用，或者作为存储固定他们自己的代币等
- It is used to make sure that providers have a stake in Chromia ecosystem thus offsetting incentives to collude.
  确保供应商在 Chromia 生态系统中有股份

Since Chroma tokens are used for stake and reserve purposes we expect a significant amount to be taken out of circulation and “locked” for this kind of use.
既然幻彩代币是当作股份和储备目的的，我们期望能从流通的当中拿出一定比例的金额，“锁定”这种类型的使用。

System accounts 系统账户

Chromia has several special Chroma token accounts which are used for system-wide purposes:
Chromia 在系统范围内有几个特别的幻彩代币账户：

- ERC20 token pegging: Chroma tokens on this account belong to owners of Chroma ERC20 tokens which enable some interoperability with the Ethereum blockchain. This account is managed by the Ethereum gateway blockchain.

  ERC20 代币追溯：在此账户上的幻彩代币属于幻彩 ERC20 代币的拥有者，这些代币使得和以太坊区块链有互操作性。这一账户由以太坊网关区块链管理。

- System node compensation pool: Nodes which run dapp blockchains are compensated by dapps. But nodes running system blockchains also need to earn money. For this reason a certain percentage (decided by the council of providers) is taken out of hosting fees and sent to the system node compensation pool, which is then used to compensate nodes for hosting system blockchains. In other words, Chromia itself can be seen as a dapp which orchestrates and taxes other dapps.

  系统节点补偿资金：运行分散应用程序区块链的节点可得到分散应用程序的补偿。但是运行系统区块链的节点同样需要挣取资金。为此，一定比例（由供应商委员会决定该比例）的代管费将拿来放入系统节点补偿资金，这部分资金将用来补偿代管系统区

块链的节点。换言之，Chromia 本身可视为一个分散应用程序，它协调其他分散应用程序并像他们征税。

- Future development pool: Initially ChromaWay and its subsidiaries will develop Chromia, but eventually this role should be decentralized. Once the economy is sufficiently decentralized the “future development pool” can be unlocked and used according to providers’ vote to improve Chromia as a whole.

  未来发展资金：最初幻彩大道和其附属机构会开发 Chromia，但最终这一角色应该被去中心化。一旦该经济体足以去中心化，未来发展资金将会被解锁，并根据供应商的投票用作 Chromia 整体发展。

- Charity pool: in certain situations where tokens are sacrificed (explained below) a fraction of such tokens can be diverted into a charity pool. Funds from this account can be used to donate to charities according to users’ votes. This can promote Chromia as an ethical and socially-conscious blockchain.

  慈善资金：在某些情况下，将牺牲一部分代币转化为慈善资金。这一账户的资金可以通过用户的投票来用于捐献慈善。这有助于宣扬 Chromia 是一个有道德和社会意识的区块链。

Public good account 公共优良账户

In certain situations tokens need to be “sacrificed” (irreparably destroyed or burned) to avoid a conflict of interest or the possibility of abuse. These situations include Sybil control mechanisms, punishment of misbehaving parties or a “neutral action” in a case of a disagreement between two or more parties.
在有些情况下，代币会为了避免利益冲突或滥用的可能而做出“牺牲”（不可挽回的损毁或烧毁）。这些情况包括 Sybil 控制机制、作弊方的惩罚或者双方或多方意见不统一时的“中立举措”。

Chromia offers an alternative to irreparable destruction in the form of a public good account. This is a virtual account which automatically distributes received tokens into 4 different accounts:
Chromia 以公共优良账户的形式给不可挽回的破坏一个选择。这是一个虚拟账户，会将收到的代币自动分至四个不同的账户：

- 25% of tokens are burned; burning tokens indirectly benefits all Chroma token holders as tokens are permanently removed from circulation
  25%的代币被烧毁，烧毁的代币间接给幻彩代币持有者带来利益，因为代币永久不再流通
- 25% of tokens are put into the “System node compensation pool”
  25%的代币放进“系统节点补偿资金”
- 25% of tokens are put into the “Future development pool”
  25%的代币放进“未来发展资金”
- 25% of tokens are put into the “Charity pool”

25%的代币放进“慈善基金”

Thus all Chromia users indirectly benefit from the public good account in the long term. It's very unlikely for the public good account to be abused as control funds in it are collectively controlled and aren't easily accessible. It is therefore a viable and productive alternative to simple “burning”.
从长远角度看，所有 Chromia 用户都间接获益于公共优良账户。该账户被滥用的可能性极小，因为资金是共同控制的，也并非易于获取。因此对于简单的“烧毁”来说是一个可行的选择。

Funds will be sent to the public good account in following cases:
以下情况资金会被放进公共优良账户：

- A user would need to send 10 Chroma tokens to the public good account to become a “Chromia citizen”. This confirms the user's commitment to Chromia and gives certain perks such as the ability to vote, priority services, the ability to participate in “lucky request” reward program, etc. (Details about this program are covered in the Appendix.)
  用户需要往公共优良账户中充值 10 幻彩代币才可称为“Chromia 公民”。这是作为用户对 Chromia 的承诺，同时也获得了投票权、优先服务、参加“幸运要求”奖励项目的权利等。（该项目的细节详见附录）
- The lost stake of misbehaving nodes is sent to the public good account.
  作弊节点丢失的股份将进入公共优良账户
- 0.1% of application hosting fees are sent to the public good account
  应用程序代管费的 0.1%将计入公共优良账户

Additionally, we encourage dapps to use the public good account when the destination of tokens is unclear for some reason, or if tokens need to be destroyed for game-theoretic reasons. For example, “Burnable Payments” is a simple game-theoretic mechanism which makes sure that that neither buyer nor seller have an incentive to cheat: if the buyer disagrees with the seller he can burn escrowed funds.
另外，如果分散应用程序因为某些原因而导致代币目的地不清晰时或者由于博弈而导致代币需要被损毁时，我们鼓励他们使用公共优良账户。“可燃支付”是一种简单的博弈机制，它能保证不管是买家还是卖家都不可以作弊。如果买家不同意卖家，他可以烧毁代管基金。

Token distribution 代币分配

One billion tokens will be created upon launch of the system. That constitutes the token supply limit, no tokens will be created in the future. Initial distribution of tokens:
系统上线时会发布十亿代币。这形成了代币的供应限额，未来不再发行更多代币。原始代币分配如下：

- 65% owned by ChromaWay through its subsidiary Chromia Devcenter Oü to be sold, awarded to team members, invested or used in any other way
  65%归幻彩大道所有，通过它的子公司 Chromia 开发中心进行销售、奖励员工、投资或用于其他地方

- 3% put into an automatic conversion contract on Ethereum blockchain to enable Chroma<->ETH conversion
  3%放入以太坊区块链上的一个自动兑换合约，使得幻彩代币和以太坊代币实现兑换
- 2% put into system node compensation pool
  2%放入系统节点补偿资金
- 30% is allocated for promotional use: to be given to users to try applications hosted on Chromia
  30%用作促销宣传：用来给在 Chromia 上尝试应用程序的用户

Within the ChromaWay allocation, 15% (of all tokens) will be sold initially to select partners. The rest will be locked and released slowly over time. Up to 22% will be unlocked during the first year after launch, then up to 12% per year. ChromaWay and its subsidiaries will hold tokens for at least three years. This creates long-term incentive for Chromia development. After three years Chromia development and governance must transition to a decentralized model.
在幻彩大道的配额中，有 15%是用来发售选择合伙人的。其余部分会被锁定，日后逐渐释放。有 22%将在发行的一年内被释放，之后最多 12%一年。幻彩大道及其子公司占有代币至少 3 年，这样能长期促进 Chromia 的发展。3 年后 Chromia 的发展和管理必须转变为去中心化模式。

Promotional tokens will also be initially locked, and unlocked at a rate of 1% per month.
促销代币最初也会被锁定，随后以每月 1%的比例释放。

Thus percentage of tokens in circulation changes over time:
因此在流通的代币比例会随时间发生变化：

1. At start: up to 22%
   最初：22%
2. After 1 year: up to 54%
   1 年后：54%
3. After 2 years: up to 78%
   2 年后：78%
4. After 3 years: up to 96%
   3 年后：96%
5. After 4 years: 100%
   4 年后：100%

Promotional token fund 促销代币资金

The use of the promotional token fund will be initially controlled by Chromia Devcenter. Its purpose is to encourage use of Chromia platform and dapps hosted on Chromia. Tokens from this fund should be given only to end users, they shouldn't be used to fund development of projects.
促销代币资金的使用最初由 Chromia 开发中心控制。目的是为了鼓励只用 Chromia 平台和其代管的分散应用程序。此资金中的代币只可给终端用户，它们不可用作发展项目。

The rationale for this fund is that it's hard for an average internet user to acquire tokens: they need to register on crypto exchanges, which is a lot of hassle. Also people are generally reluctant to spend money just to try out a new app (which might be not-so-great).
使用这一资金的根本原因在于一般的网络用户很难获得代币。他们需要通过繁琐的步骤在加密交易所上注册。而且人们一般也不愿意花钱去尝试一个新应用程序（有可能还不怎么样）。

Thus it is necessary to give away tokens for free to build a mainstream user base.
所以有必要免费发放代币，以此建立主流用户基础。

However, this needs to be done with caution. Obviously, Sybil control measures should be used -- it is certainly possible that somebody will try to impersonate multiple users to acquire a large number of tokens for free. One possible way to mitigate abuse is to require some form of identification (e.g. Facebook account).
然而，这也需要小心处理。极有可能有人会冒充多个用户来获取大量的免费代币，所以应该使用 Sybil 控制。一种可行的减少滥用的方法是要求提供验证表（如脸书账号）。

Tokens might also be given out for use within a specific app or game.
代币可能也用于某个特定的应用程序或游戏。

Tokens from promotional fund are released gradually to:
促销资金里的代币逐渐释放到：

- Onboard users as the system grows 随系统发展而加入的用户
- Monitor the situation and experiment with different ways to distribute tokens 监测情形，测试用不同的方式发放代币
- Avoid disrupting the value of Chroma 避免破坏幻彩的价值

1% per month is a *maximum* distribution rate. If promotional use is deemed inefficient tokens might be reserved for later use or sent to the public good account.
每月 1%是最大的发放比例。如果促销没有效果，代币可能会预留给后期使用或转至公共优良账户。

Decentralization 去中心化

Centralization necessary at start 以中心化开始

Chromia shall be a true decentralized platform for decentralized applications: not controlled by anyone, open for permissionless innovation.
Chromia 必须是为分散应用程序创立的真正的去中心化平台，不受任何个人控制，拥抱任何创新。

But decentralization is not a starting point, but a goal. Proper decentralization requires a strong community with a large number of independent participants who are committed to Chromia. But building a community takes time. The platform needs to prove itself before it's deemed interesting enough to contribute to it.

但是去中心化不是起点而是目标。适当的去中心化需要有一个拥有忠于 Chromia 的大量独立参与者的强大社区。但是创建一个社区需要时间，平台在获得认可前首先要证明自己。

Thus Chromia will be centralized at start; we believe it's better to embrace this and use a centralized development and governance model to speed up development than to play pre-tend-decentralization.
所以 Chromia 刚开始会中心化，我们认为比起急于实行所谓的去中心化，用集权的方式发展和集权管理模式来加快发展更加切实有效。

For this reason, ChromaWay opened a for-profit company called Chromia Devcenter Oü which will act as Chromia development center at the initial stages. As the largest holder of Chroma tokens which are locked for 3+ years, Chromia Devcenter is motivated to increase the value of Chromia as a system, as that will likely also increase the value of its holdings.
出于此因，幻彩大道成立了一个叫做 Chromia Devcenter Oü的营利性公司，它在初级阶段会是 Chromia 的发展中心。作为幻彩代币 3 年以上最大的持有者，Chromia 发展中心有动力增加 Chromia 作为一个系统的价值，因为同时也能增加其持有股份的价值。
After observing the cryptocurrency ecosystem for 7 years, we believe that a for-profit model is the optimal way to scale the development in the initial stages. Here are some examples of failures of more decentralized community-based models:
在关注了加密货币生态系统七年后，我们认为最初的营利模式是取得规模发展的最佳方式。以下是更基于去中心化模式的失败案例：

- The colored coins project suffered from slow development and fragmentation. Even monetary bounties didn't help to attract a persistent developer base[15]. Developers who joined the project temporarily produced low-quality code and then hopped to something else.
  彩色币项目受困于缓慢发展和分裂。即使货币补贴也无法吸引稳固的开发者基础。开发者临时性的加入此项目，创造些低质量的节点，然后又跳向别处。
- The Mastercoin project (now known as Omni) bounty-driven process produced three incompatible implementations. Eventually they switched to a centralized process and achieved better results.
  万事达币项目（现在叫做欧姆尼）补贴驱动型的流程创造了三个不兼容的实施。最终他们还是转变成了一个中心化的流程并取得了更好的结果。
- Ethereum Foundation failed to create a working light wallet for three years. As a result, users had to rely on unsafe web wallets, or struggle with keeping their full node wallet in sync.
  以太坊基金会花了三年都没能创建个可用的轻钱包。最终用户只能依靠网页钱包或将他们的全节点钱包放在合成器上。

As a for-profit company, Chromia Devcenter will be able to set concrete goals and focus on them; particularly, focus on features which are essential for Chromia platform adoption and user base growth.

[15] See interview with ChromaWay CTO, at the time leading the colored-coins project, on Coindesk in 2013|请在 Coindesk 上浏览 2013 年对幻彩大道 CTO 的采访，当时他领导了彩色币项目：https://www.coindesk.com/colored-coins-paint-sophisticated-future-for-bitcoin/

作为一个营利公司，Chromia 发展中心建立具体目标并关注于此，尤其关注能帮助 Chromia 平台采用和用户群壮大的特性。

Beyond development, Chromia Devcenter can also
除了发展，Chromia 发展中心也能够

- Organize promotional events 组织促销活动
- Help companies to build dapps on Chromia 帮助企业在 Chromia 建立分散应用程序
- Collaborate on projects with other companies 与其他公司合作项目
- Invest into the dapp ecosystem 投资分散应用程序生态系统

We believe that these activities are better done on a for-profit, commercial basis. Non-profit foundation models can result in inefficient use of funds, abuse, corruption, etc.
我们相信这些活动以营利和商业为目的能更好地开展。非营利模式将导致资金的无效使用、滥用、腐败等问题。

It's important to highlight that Chromia Devcenter is **not** Chromia. Once launched, Chromia as a network will have a certain degree of autonomy. Chromia Devcenter cannot force people to run a particular version of software. It also cannot modify any blockchain records or state beyond what it was explicitly granted access to. Thus it cannot be held responsible for what happens within the network.
特此强调一下 Chromia 发展中心不是 Chromia。一旦启用，Chromia 作为一个网络将有一定的自治权。Chromia 发展中心不可强求他人运行特定版本的软件，也不可更改权限以外的任何区块链记录或状态。因此它对网络里所发生的事情不具备任何责任。

With respect to Chromia network, the role of Chromia Devcenter is the following:
关于 Chromia 网络，Chromia 发展中心扮演以下角色：

- Produce free and open source node software, which can be independently inspected and modified as needed.

  创造免费开放的节点软件，可根据需要单独被检查和修改

- Control certain parameters such as the pricing of resources and selection of providers until the network is big and decentralized enough to control these parameters on its own.

  控制某些参数，如资源的价格、供应商的选择等，直到网络足够大，足够去中心化，能够自己控制这些参数。

There are two risks associated with this role:
这一角色有两大风险：

- Node software (or other relevant software) will have a backdoor or other security threat. *Mitigation*: We encourage providers and users to review software before running it.

节点软件（或其他相关软件）会有后门或其他安全威胁。解决方案：我们鼓励供应商和用户在运行软件前进行检查。

- System parameters or provider selection can be set to values which disrupts the system. *Mitigation*: We will limit the rate of change via blockchain rules enforced by nodes. In the worst case providers/users can fork the network to avoid disruptive settings.
  系统参数或供应商选择会形成破坏系统的值，解决方案：我们会通过区块链规则限制变动率。最糟糕的情况下供应商或用户可以拆分网络来避免分裂性的设置。

Decentralization through a diverse set of providers 通过多样化的供应商去中心化

Once the provider ecosystem is mature enough, governance can transition to a group of providers.
一旦供应商生态体系足够成熟，管理就可以下放给一组供应商。

How does this compare to the quality of decentralization seen in other blockchains?
它的去中心化质量与其他区块链上的如何做对比呢？

Bitcoin 比特币

Satoshi originally described Bitcoin as “1 CPU = 1 vote” kind of a system. The original user base mostly consisted of ordinary internet users interested in P2P systems, and originally block production was extremely decentralized. Still, Satoshi was essentially the dictator and could change code as he wants. He could, in principle, make an update which would steal coins from other users.
Satoshi 最初将比特币描述为一个“一 CPU 一票”的系统。最初的客户群大多是对 P2P 系统感兴趣的网络用户，而最初的区块链制造极其分权。Satoshi 本质上仍旧是独裁者，他可随他意愿更改节点。他原则上还能制造更新，从其他用户那儿窃取比特币。

Eventually the situation with code updates became better: all code which goes into Bitcoin node software is reviewed, Bitcoin node binaries are built using a Gitian process which allows multiple parties to verify that code in the repository corresponds to binaries, this means that end users can rely on a decentralized group of developers to control for possible backdoors and other issues.
最终情况随着节点的更新而越来越好，所有比特币节点软件里的节点都会接受检查。用 Gitian 流程建立了比特币节点二进制，允许多方审核知识库中的节点。这意味着终端用户可以依靠一群分散的开发者来控制可能的后门和其他问题。

On the other hand, the situation with block production became worse over time. First, users joined “mining pools” to make rewards more predictable. As a result, they are no longer producing blocks, but instead rent their hashpower to a pool, which actually produces blocks. This means that a mining pool can, in principle, produce a malicious chain of blocks. In theory, users should notice this and switch to a different pool, but it will take some time. At a certain point of time, a single pool (GHASH.io) had >50% of total hashpower, and users did nothing.
另一方面，区块的生产情况随时间逐渐变糟。首先，用户加入“矿池”中使得奖励更加可预测。导致他们不再制造区块，而是将他们 hash 计算力租给实际生产区块的池。这意味着本质上矿

池可以制造一系列不良的区块。理论上，用户应该察觉到这一点并转向其他池，但会花费一定时间。在某一特定时期，一个单独的池拥有 50%以上的 hash 计算力，用户却无能为力。

Another problem came with the advent of ASIC mining: ASIC manufacturing companies started mining on their own. Companies which had more efficient chips got higher profits and could reinvest it into expansion. Economies of scale create a positive feedback loop where production of mining chips and mining itself becomes more and more centralized.
随着 ASIC 挖矿出现所带来的另一问题是 ASIC 制造公司开始他们自己的挖矿。有更高效芯片的公司获得更高的利润，继而他们能扩大投资。规模经济创造了一个积极的反馈环，矿芯片的生产和挖矿本身变得越来越集中。

This culminated in Bitmain shipping more than 70% of all mining equipment, and Bitmain-affiliated mining pools having more than 50% of total hashrate. Bitmain doesn't report any statistics, but we have every reason to believe that warehouses with the Bitmain logo on them full of Bitmain miners actually belong to Bitmain and are the source of an enormous hashrate. In any case, the currently biggest three mining pools can control the network, and two of them are affiliated with Bitmain.
这占据了比特大陆运输中 70%以上的挖矿工具，比特大陆附属的矿池拥有 50%的总算力。比特大陆不报告任何数据，但我们足以相信标有比特大陆商标的仓库实际满是属于比特大陆的矿工，并且是大量算力的来源。任何情况下，现今三大矿池能够控制网络，而其中两个附属于比特大陆。

It is also undeniable that the majority of hashpower is hosted inside China, thanks to cheap power, cheap facilities and so on. This gives the Chinese government the possibility to control Bitcoin. It could potentially seize facilities and execute a 51% attack, or a soft fork to introduce censorship.
不可否认大多数 hash 计算力都在中国代管，得益于优惠的电价、设施等。这给了中国政府控制比特币的可能性。它可能抢占设施并执行 51%攻击，或是引进审查制度。

PoW centralization resulted in delayed network updates and Bitcoin become practically unusable for payments due to extremely high fees. Summary: while Bitcoin development is decentralized, block production is heavily centralized.
PoW 集权导致网络更新的延迟，比特币由于极其高昂的费用而变得没那么实用。总结：当比特币发展去中心化时，区块制造变得尤为集中。

DPoS DPoS

It was observed that DPoS-based blockchains -- BitShares, Lisk, ARK, STEEM, EOS -- have a large degree of stake centralization, which means that few large token holders can effectively control the network. Problems with DPoS centralization are thoroughly explained by Vitalik Buterin[16].
据了解，像比特股、Lisk、ARK、STEEM、EOS 等基于 DPoS 的区块链有很大程度上的资金中心化，这意味着没有代币持有者能有效控制网络。DPoS 中心化的问题 Vitalik Buterin 有做充分地解释。

[16] https://vitalik.ca/general/2018/03/28/plutocracy.html

Ethereum 以太坊

Ethereum block production is currently PoW-based and thus has roughly same problems as Bitcoin (the three biggest pools can control block production).
以太坊区块生产现在是基于 PoW 的，因此几乎和比特币有同样的问题（三个最大矿池能控制区块生产）。

It is meant to eventually to transition to proof-of-stake. That doesn't mean that every stakeholder has a chance to produce a block. Instead, the number of block producers will be restricted to about 1000 entities, thus smaller token owners have to delegate block production to pools in order to participate.
这最终将转变为权益证明。并不意味着每个股东有机会生产区块。而是区块生产者会限制在大约 1000 家，所以小型代币拥有者若想参与只能将区块生产委托给矿池。

Chromia Chromia

It appears that no existing projects give control of the network to a very large set of people. Neither does this appear to be a particularly useful approach, most people do not have enough technical knowledge and motivation to keep the network safe. A person who runs software he was told to run is essentially just a proxy for the entity which decided what software to release.
现在看来，似乎没有哪个项目会将网络控制权下放给许多人。这不仅看来不是个有效的方法，而且大多数人也没有足够的技术知识和驱动力来维持网络安全。运行软件的仅仅是个代理，他们的主体会决定该释放哪一软件。

For this reason we believe that the Chromia model where the network is controlled by a limited group of providers is not an impediment to decentralization. As long as these providers are truly independent, pursue their own goals (i.e. profit from hosting dapps), and operate in many different countries, the system can be considered decentralized.
出于此原因，Chromia 模式由有限的供应商群组来控制网络，这并不阻碍去中心化。只要这些供应商真正独立，追寻他们的目标（如：从代管分散应用程序中收益）并在多个国家操作，那么系统就可视为是去中心化的。

Initially we plan to get at least twelve providers. In the long run the number can reach thousands, on par with the PoS scheme proposed for Ethereum.
最初我们计划招募至少 12 家供应商。长远看，这一数字可达数千，将于以太坊的 PoS 计划势均力敌。

Another way to look at it is a barrier to entry. A Bitcoin ASIC miner can be purchased for several thousand dollars, but a user won't be able to generate any blocks on his own. To become a significant player one needs hundreds of millions of dollars in capital to acquire hardware and build facilities.
从另一个角度看，这也是准入的屏障。一个比特币 ASIC 矿工花几千美元能买到，但用户不能自己创建任何区块。要想成为一个重要玩家，需要准备数亿美元的资金来获取硬件和建立设施。

On the other hand, any professional hosting company can become a Chromia provider and participate in building blocks. Thus we believe that the barrier for entry is actually lower than that seen in other blockchains.
另一方面，任何专业的代管公司可以成为 Chromia 的供应商并参与区块建立。所以我们认为这样的准入门槛其实要比其他区块链来的更低。

Number of full nodes 全节点数量

Public blockchains such as Bitcoin and Ethereum boast a large number of full nodes -- estimated to be in the 5000-10000 range. While a large number of full nodes potentially increases network resilience, it also has downsides: the network can't be faster than its slowest node. Thus both Bitcoin and Ethereum severely limit number of transactions, as well as computational resources required to process transactions.
比特币和以太坊这样的公有区块链鼓吹大量的全节点，估计有 5000 到 10000. 虽然大量的全节点潜在的提升了网络恢复力，但它也有缺点：网络无法比最慢的节点来的更快。因此比特币和以太坊对交易数量和处理交易所需的资源都严格控制。

Chromia takes a different trade-off: number of full nodes might be limited to number of block producers, which will be typically on the scale of 10-100 nodes per blockchain. Does this result in lower network resilience? Let's analyze different threats:
Chromia 执行不一样的交易：全节点的数量受限于区块生产者的数量，每个区块链搭载在 10~100 节点。这会带来低网络恢复力吗？让我们来分析不同的挑战：

1. **Node hardware failures**: Assuming failures are random, it's extremely unlikely that 10 nodes will fail at the same time, before new replicas can be made.
   节点硬件故障：假设故障是随机的，在新的副本完成前，极其不可能发生 10 个节点同时出故障。
2. **Network DoS**: While in certain scenarios a bigger number of nodes is helpful, a network can be effectively disabled by specifically targeting block producers, and the number of independent node producers might be actually higher in case of Chromia.
   网络 DoS：在某些特定情形下，更多数量的节点是有帮助的，只要找准目标区块生产者，网络就可以有效切断，在 Chromia 独立节点生产者的数量可能更高。
3. **Network partitions**: Networks based on PoW consensus typically do nothing to detect network partitions, thus they can simply work through minor disruptions. But in case of a major disruption it might result in double-spends on the different sides of the partition. The fact that a Chromia-style network stops in case of a partition is actually a feature, not a bug.
   网络分区：基于 PoW 共识的网络对于检测网络分区无任何操作，因此他们能够轻松解决轻微的破坏。但如果有重大破坏，将会导致分区两侧双重损失。如果分区实际是个病毒而不是故障，Chromia 式的网络就会切断。

It should be noted that Chromia does not discourage users from running full nodes. Every blockchain running on Chromia should be public, Therefore any user who wishes to run a full node for a particular blockchain should be able to do so, as long as he has access to modern hardware.

值得注意的是，Chromia 并非不鼓励用户运行全节点。每一个在 Chromia 上运行的区块链都应该公开。因此，只要能够进入现代硬件，任何想要在特定区块链上运行全节点的用户都需要做到这一点。

In fact, if we compare Chromia to Ethereum, it can be said that Chromia architecture makes it easier to run a full node: an Ethereum user is forced to download data of all dapps and all users. Chromia user can choose what dapps he is interested in and sync only the corresponding blockchain data.
事实上，如果我们拿 Chromia 和以太坊作对比，可以说 Chromia 的架构运行全节点要更容易。以太坊用户必须下载所有分散应用程序和所有用户的数据。而 Chromia 的用户可以选择感兴趣的分散应用程序然后同步相关区块链数据。

The number of Chromia full nodes might be lower not because it's harder to run a node, but because with a properly working light client it's just not necessary, and we expect that fewer hobbyists care about specific dapps than about "the world computer".
Chromia 上的全节点数量或许比较少，并不是因为它难以运行，而是因为没有必要。我们期望较少的业余爱好者关注"世界计算机"多过特别的分散应用程序。

Security 安全

Blockchain 区块链

The role of the blockchain is to make sure that there is a single application state seen by all users, and that double-spend and replay attacks are not possible.
区块链的任务是确保所有用户看到的都是唯一的应用程序，不会有双重支付和重放攻击。

In a light client security model, blockchain nodes also take responsibility for validating state transitions and transactions. We will discuss light client security in a separate section; in this section we will focus solely on the security aspects of the "full node" model.
在轻客户安全模型中，区块链节点也负责验证状态的转移和交易。我们将用单独的章节来讨论轻客户安全，本章节我们只关注全节点模型的安全。

The most basic threat we are protecting against is a single node wilfully violating the rules of the system. This can occur because whoever controls it has become corrupt for some reason[17], or because it has been compromised by an external attacker. Centralized systems built using a traditional software architecture have no protection against that -- a single compromised server can result in arbitrary data modification, which in case of financial data can lead to arbitrary losses. Particularly this might happen in the following scenarios:

[17] Corruption here encompasses a range of possible scenarios in which the node provider has incentives to act in a way which is detrimental to the goals of the collective in which it participates. Financial gain, coercion, deception, mental instability; there are many reasons why a node operator might become corrupt.
这儿所说的腐败包含一系列可能的情况，节点供应商有动机使行为趋向于对自己参与的集体目标有害的方向。经济获益、强制型转、欺诈、精神不稳定等，有诸多原因促使节点操作者开始腐化。

我们所保护的最大最基本的威胁是单个节点故意违反系统规则。这种情况会发生是因为无论谁去控制，都出于某些原因变得腐化，或者被外来侵袭者盗用。利用传统软件架构建立的集权系统对此没有保护，单一的被破解服务器就可导致任意数据被更改，如果是财务数据就可能造成损失。这一事件尤其可能在以下情形下发生：

- External intrusion through exploitation of a software or hardware vulnerability.
  通过软件的开发或硬件的脆弱性而遭受外部入侵
- Rogue employee -- system administrator or other person who has access to the server can exploit it for personal gain.
  违规员工 – 系统管理员或者其他有权限进入服务器的员工会因为个人利益而利用它
- Hosting provider's tampering -- physical access to server allows provider to modify data.
  代管供应商的篡改 – 供应商的物理权限使得他们能够篡改数据
- The company itself can arbitrarily change data or rules to its own gain.
  公司自身可以为了收益而随意修改数据或规则

The first layer of protection against these scenarios is application logic which requires both cryptographic authorization and a deterministic computation model. When a user's nodes have complete data they can detect cases where rules are violated and thus reject a false application state. In Chromia this is accomplished by requiring applications to be developed in Rell: Rell has a deterministic computation model and makes it easy to implement cryptographic authorization for all data mutations. The overall architecture also makes it possible for user nodes to receive full input data (blocks and transactions) and independently compute the application state.
针对这些情形的第一层保护是应用程序逻辑，可以要求加密授权和确定性计算模型。当用户的节点具有完整数据时，它们就能检测出违反规则的案例，然后拒绝错误的应用程序状态。在 Chromia，这要靠要求应用程序在 Rell 上发展才可完成。Rell 有确定的计算模型，能使为所有的数据突变实行加密授权更加容易。总的架构也使用户节点接收完整输入数据和独立计算应用程序状态成为可能。

A more sophisticated attacker can exploit situations where multiple valid application states can exist at the same time. This attack is usually described as double-spending, for example:
更有经验的攻击者会开拓局面，多个有效的应用程序状态能同时共存。这种攻击通常被形容为重复支付。例如：

1. An attacker produces an application state in which a merchant was paid to ship some goods.
   某个攻击者创造一个应用程序状态让商家发货
2. The merchant ships the goods.
   商家将货物发出
3. The attacker replaces the application state with another where the merchant is not paid, instead the funds are directed back to the attacker's account.

攻击者会将应用程序状态用另一个未付款的来替代，实际上所有资金都进入了攻击者的账户

4. Now the attacker has both the goods and the money.
   那么攻击者就实现了货款双收

Many variations of this attack exist. For example, it can be done using different kinds of tokens and merchant as part of an exchange.To protect against this attack a system must be designed to ensure that mutually incompatible application states aren't allowed to exist.This can be done using a Byzantine Fault Tolerant (BFT) consensus algorithm which "confirms" a single application state and rejects all incompatible states after that.
许多这类攻击的变形都可发生。例如，它可以利用不同种类的代币和商户作为交换的一部分来完成。为了防护此攻击，系统必须设计成互不兼容的应用程序状态不许存在。这可以靠 BFT 共识运算法则来实现，它可确认唯一的应用程序状态，拒绝所有的不兼容状态。

It has been demonstrated that in an asynchronous network (i.e. without confirmation of packet delivery) a BFT consensus algorithm can tolerate up to 33% of node failures. Strictly speaking, ⅔ plus one node must remain honest. For example, a system with 10 nodes can tolerate up to 3 failures, i.e. it will keep working when 3 nodes are compromised.
根据证明，在不同步的网络（即包发送没有确认）环境下，BFT共识运算法则最多可以容忍高达 33%的节点故障。严格来讲，至少三分之二的节点要保持可靠。例如，一个拥有 10 个节点的系统可以容许 3 个故障，也就是当 3 个节点被破解时它仍可保持工作。

Chromia uses a PBFT-style consensus algorithm to build the blockchain. When the number of blockchain's validator nodes is 3f+1, a block must receive 2f+1 "votes" to be confirmed (i.e. more than ⅔ of all votes). Users' nodes only deal with blocks which are confirmed.
Chromia 运用 PBFT 式的共识运算法则来建立区块链。当区块链验证器节点数量为 3f+1 时，区块必须获得 2f+1 的投票才能被确认（超过三分之二的投票）。用户节点只可处理确认过的区块。

Thus Chromia can tolerate arbitrary corruption of a minority (less than ⅓) of blockchain's validators nodes with no drastic consequences except a possible slowdown. Chromia will attempt to ensure that any blockchain will be allocated nodes from different providers so that a single failure cannot result in blockchain corruption. Requirements will be especially stringent for system chains.
因此 Chromia 可以容忍少数区块链验证器节点的任意损坏，除了可能的降速，没有严重的后果。Chromia 会试图确保任何区块链会从不同供应商那儿被分配节点，这样一个故障不会导致区块链的破坏。对于系统链的要求必须非常严格。

This is the fundamental assumption of Chromia -- individual nodes (as well as individual providers) can and will fail, but it should have no effect on Chromia users.
这是 Chromia 的基本假设 – 单个节点（以及单个供应商）都能也都会发生故障，但是不应该对 Chromia 上的用户造成任何影响。

But we also need to consider situations when more than 33% of validators for a particular blockchain fail. We consider this unlikely, but possible. While we cannot guarantee smooth

operation in case of a “34% attack”, we can try to minimize the damage and enable speedy recovery . Particularly, Chromia needs features to:
但我们同样要考虑某一区块链上多余 33%验证器出现故障的情况，即使可能性很小。我们无法保证 34%攻击时还能平稳运行，但我们可以努力使损害降至最小，且能迅速恢复。特别地，Chromia 需要这些特征：

- Make it difficult for attackers to profit from the attack.
  使攻击者难以从攻击中获利
- Make it possible for the Chromia system to detect the attack as early as possible, so that recovery steps can be taken.
  使 Chromia 系统能尽早检测到攻击，从而可采取恢复措施
- Make it possible for Chromia users to detect the attack as early as possible, so they can abstain from operations which might result in financial loss.
  使 Chromia 的用户能尽早检测到攻击，这样他们能避免财务损失
- Allow Chromia users to wait for stronger confirmations for high-value transactions if desired.
  允许 Chromia 用户有等待时间，如果他们想要对高值交易做更多的确认

The most powerful tool at our disposal is anchoring -- a way of boosting the confirmation strength of one blockchain using another. Let’s consider the simplest anchoring scheme. Suppose we want to anchor blocks of blockchain X in blockchain Y. To do that:
我们所处理的最强大的工具是锚定，它是一种用一个区块链加强另一个区块链确认优势的方式。让我们看看最简单的锚定方案。假定我们想要在 Y 区块链上锚 X 区块链的区块。要采取以下步骤：

1. When block **X_i** is confirmed in blockchain X, one of the block producers will publish a tuple **(X, i , hash(X_i))** in blockchain Y
   当区块 X_i 在区块链 X 上确认后，就有区块生产者在区块链 Y 上发布一个元组
2. Once that publication is confirmed in blockchain Y, a user’s node (which follows both blockchain X and blockchain Y) can find the first tuple of form **(X, i, *)** which is published in blockchain Y
   一旦该发布在区块链 Y 上确认，用户的节点（同时遵循区块链 X 和区块链 Y）能在区块链 Y 上找到第一个元组形式（X，i，*）
3. Block X_i is said to be anchored when **(X, i , hash(X_i))** is the first such tuple.
   当**(X, i , hash(X_i)**成为第一个这样的元组，区块 X_i 就可被锚
4. If consensus on blockchain X fails and a different block **X’_i** is produced, the anchored block **X_i** should take precedence. That is, in case of a recovery the blockchain should include the last anchored block, and blocks incompatible with it must be deleted.
   如果区块链 X 共识失败，另一个不同的区块 X’_i 会产生，锚的区块 X_i 应该获得优先。也就是如果要恢复，区块链应该包含最后锚的区块，其他不兼容的区块必须删除。

It’s easy to see how merchant can use anchoring to boost confirmation strength. Suppose merchant will wait until block **X_i** which contains a payment to him is both confirmed and anchored before he ships the goods. In In this case if consensus of blockchain X fails (e.g. X’s nodes are compromised and produce several incompatible histories), but blockchain Y

stays correct, merchant does not suffer a loss -- once blockchain X is restarted (e.g. with new validators) the block X_i will be included and thus merchant will receive the money.
不难见到商人如何用锚定来加强确认优势。假设商人会直到包含付款的区块 X_i 确认并锚好后才发货。这种情况下如果区块链 X 的共识失败（X 的节点被盗用并产生数个不兼容历史），但区块链 Y 是正确的，那么商人不会有损失 – 一旦区块链 X 被重启（伴随新的验证器），区块 X_i 会被包含在内，这样商人就能收到他的款项。

Technical implementations of anchoring might differ in:
锚定的技术实行可能有以下不同：

1. What is being published (e.g. just a commitment)
   发布什么内容
2. Who can publish information
   谁可以发布信息
3. Whether light-client proofs are possible
   是否轻客户验证有可能
4. How easy it is for a node to detect anchoring failure
   节点检测锚定错误的难易程度如何

Chromia will make use of multi-level anchoring, that is, blocks from a dapp blockchain will be anchored in a special anchoring-chain maintained by another set of nodes.
Chromia 将确保不同层级的锚定，分散应用程序区块链的区块会在由另一组节点维护的特殊锚定链上被锚。

Let's consider an example. First we consider the situation without anchoring. Suppose dapp blockchain A is run by 10 validator nodes all of which are compromised. If tokens from this dappchain are traded on a centralized exchange, compromised nodes might be used to perform an attack:
让我们来看一个例子。首先，我们考虑没有锚定的情况。假定分散应用程序区块链 A 由 10 个被盗用的验证器节点运行。如果这个分散应用程序链上的代币在一个中心化的交易所交易，那被破解的节点可能被用来形成一次攻击：

1. Nodes will prepare two versions of a block at the same height: block **X_i** contains a payment from the attacker to the exchange, and block **X'_i** doesn't
   节点会在同一高度准备两个版本的区块：区块 X_i 包含攻击者给交易所的付款，区块 X'_i 不包括
2. The exchange sees block **X_i** and credits tokens to the attacker's account.
   交易所看到 X_i 会将代币归于攻击者账户
3. The attacker sells his tokens for bitcoins and withdraws bitcoins from the exchange.
   攻击者售出代币换取比特币，然后从交易所收回比特币
4. Block **X'_i** is revealed to all other nodes and subsequent blocks are built on top of it.
   区块 X'_i 向所有其他节点显露，然后随后的区块在此之上建立
5. It's not possible to tell whether block **X_i** or block **X'_i** should take precedence. Obviously, block **X_i** is better for the exchange, but block **X'_i** might include other important payments.

无法确定区块 X_i 还是区块 X'_i 应该占先。显然，区块 X_i 用来交易更好，但 X'_i 可能包含其他重要的付款

6. Thus the exchange might suffer a loss even after faulty nodes are replaced, as the blockchain might be built on block **X'_i.**
因此交易可能带来损失，即使错误的节点被替代，因为区块链可能是在区块 X'_i 上建立的

In a situation with anchoring, the exchange can protect itself from this risk. It should wait until the payment is anchored in block **X_i** before crediting the money. In this case even if nodes try to build an alternate block **X'_i**, that block won't be included into a blockchain after nodes are replaced as it is not anchored.
在锚定的情况下，交易能从风险中保护自己。它应该一直等到付款在区块 X_i 上锚好后在支付款项。这种情况下，即使节点尝试建立备选区块 X'_i，该区块在节点被替代后不会包含在区块链中，因为没有被锚。

The merchant can suffer a loss only when the anchoring chain itself is compromised. However, the Chromia anchoring chain will include a larger number of validator nodes from different providers, say, a hundred. It might be enough to compromise 4 nodes to compromise the dapp blockchain, however, it will take at least 34 nodes/providers to be compromised to anchor two incompatible blocks. That is, it requires a collusion on a large scale.
只有当锚定链本身被破解时商人才会蒙受损失。然而，Chromia 锚定链会包含不同供应商大量验证器节点。可能破解 4 个节点就足以破解分散应用程序区块链，然而将至少破解 34 个节点或供应商来锚两个不兼容的区块。也就是它要求大范围的合谋。

However, we cannot completely rule this situation out. For this reason, the anchoring chain will itself be anchored in PoW blockchains -- Bitcoin and Ethereum. An exchange wallet in high-security mode can wait until block **X_i** is anchored in block **A_j**, and block **A_j** is itself anchored in Bitcoin's block **B_k.** In this case to revert a payment one would need to compromise a significant number of Chromia nodes, and, on top of that, perform a Bitcoin blockchain reorganization. We believe that this situation is exceptionally unlikely.
但是我们不能完全排除此情况。为此，锚定链本身会在比特币和以太坊这样的 PoW 区块链上锚。在高度安全模式中的交换钱包可以一直等到区块 X_i 被锚在区块 A_i 中，然后区块 A_i 自己锚在比特币区块 B_k 中。这种情况下，要想回复付款，需要破解一定数量的 Chromia 节点，另外还要进行比特币区块链重组。这类情况极其罕见。

Confirmation strength can be further boosted by anchoring to multiple blockchains. Particularly, we consider establishing a network of notaries and highly reputable institutions in multiple countries. If we anchor the Chromia anchoring chain in this notary chain then we have extreme security. It will be impossible to revert Chromia blocks without a worldwide conspiracy.
如果锚在多个区块链上，那么确认度可以拉的更长。我们特别考虑在不同国家建立公证人和具有高度信用的机构的网络。如果我们将 Chromia 锚定链锚在这一公证链上，那就将非常安全。没有世界范围内的共谋，是不可能复原 Chromia 区块的。

Node security 节点安全

We believe that a collusion among Chromia providers is unlikely as loss of stake, profits and, possible legal action serves as a deterrent. However, if a software exploit which allows an attacker to execute arbitrary code on a Chromia node were to be discovered, multiple Chromia nodes could be compromised at the same time.
我们认为 Chromia 供应商之间的勾结不会造成资金和收入的损失，因为有适用的法律诉讼作为威慑手段。但是，如果某款软件的开发使得攻击者能够在被发现的 Chromia 节点上执行任一节点，那么多个 Chromia 节点将同时被破解。

The most common causes of remotely exploitable vulnerabilities are memory corruption bugs within the application code. For this reason, Chromia is implemented using a safe language which protects against memory corruption (Kotlin) and is executed on the JVM which provides memory safety.
远程可利用的脆弱性最主要的原因是应用程序节点中的内存损坏故障。出于此因，Chromia 使用了保护内存损坏的安全语言并在 JVM 上执行以保证内存安全。

Another possible source of vulnerabilities is dapp code. Chromia dapps will be implemented in Rell which is itself a memory-safe language; on top of that the Rell execution environment is implemented in Kotlin and runs within the JVM, thus for an application to break out of the sandbox it will need to defeat both Rell and JVM safety mechanisms, which we believe is practically impossible.
另一个脆弱性的可能来源是分散应用程序节点。Chromia 分散应用程序将在 Rell 上运行，它本身就是内存安全语言，另外，Rell 执行环境在 Kotlin 上实施，在 JVM 中运行，所以一个应用程序要想打破沙盒，它需要同时击退 Rell 和 JVM 的安全防线，这在实际操作中不太可能。

The remaining source of vulnerability is code written in C, that is the host OS (e.g. Linux) and DBMS (e.g. PostgreSQL). Exploitable vulnerabilities in the Linux kernel itself seem to be extremely rare, and access to PostgreSQL will be mediated by Rell which limits the possibility of attacks.
其余的脆弱根源是写在 C 中的节点，即主机 OS（比如 Linux）和 DBMS（比如 PostgreSQL）。Linux 内核本身的可利用脆弱性看起来极其少见，进入 PostgreSQL 的权限也会由 Rell 进行调解，这样也限制了攻击的可能性。

Nevertheless, we will research further options to reduce the possible attack surface:
虽然如此，我们还是会进一步探索减少可能攻击界面的方案：

- Run security-oriented Linux distribution with all non-essential components disabled
  运行以安全为中心的 Linux 分配，禁用所有不必要的组件
- Consider using an OS which further reduces the footprint or attack surface (e.g. OSv[18])
  考虑使用 OS，进一步减少足迹或攻击界面（比如 OSv[18]）
- Consider switching to a JVM-based database engine, or implement a new database engine specifically for Chromia
  考虑转换到基于 JVM 的数据库引擎或者专为 Chromia 执行一个新的数据库引擎

[18] http://osv.io/

Another possible attack vector is hardware and firmware. For example, the Intel Management Engine is present in the vast majority of Intel's products, and effectively runs a separate OS which can potentially be compromised. This could provide a vector to compromise the node running on the same CPU. To mitigate this attack vector we will recommend providers to diversify and use hardware from different vendors. We will also advise providers to limit their exposure to cloud providers. If the bulk of Chromia nodes run on, for example, AWS, Amazon has a power to fork or shut down the network.
另一个可能的攻击载体是硬件和固件。例如，因特尔管理引擎出现在绝大多数因特尔产品中，并有效运行着一个可以潜在被破解的单独 OS。为了减缓这攻击载体，我们建议供应商使用不同的硬件。我们也同样会建议供应商限制在云供应商前的曝光。如果大量 Chromia 节点在 AWS 上运行，亚马逊可以叉形或停止整个网络。

Governance security 管理安全

Governance can be a source of security problems. We can take an example from the corporate world: while the CEO herself might not be able to tamper with servers directly, she can replace the system administrator with one who will, for example, delete some crucial data.
管理有可能成为安全问题的根源。我们可以举一个企业界的例子：虽然 CEO 自己可能无法直接篡改服务器，但她能把一个可以删除重要数据的人更换成系统管理员。

Chromia governance mechanisms must therefore also be designed with security in mind. Particularly:
因此 Chromia 管理机制设计时必要考虑安全因素，尤其是：

1. It should not be possible to introduce changes which can be used to fork or destroy blockchains.
   不应该有可以用来叉形或损坏区块链的变化
2. All changes must be applied with a delay so that they can be reviewed and, if necessary, mitigating measures can be taken, in the most severe cases this might be an emergency hard fork.
   所有的变化都必须延时，这样可以对变化进行审核，如有需要可以采取缓减措施，最严重的情况下，可能会是个紧急硬叉形
3. The rate of changes should be limited.
   变化率应该有限制

Light client security 轻客户安全

Most Chromia users will use light clients which do not process the entirety of blockchain data. They will have to rely on Chromia nodes to query data from the blockchain state, and supply the confirmation status of transactions and payments. How can light client users authenticate this data? In short, they have to trust validator nodes. Each block is signed by a BFT majority[19] of all validator nodes. Thus, to confirm an invalid transaction, more than two thirds of validator nodes would need to be compromised.

[19] ⅔+1 of total validator nodes 总验证器节点的⅔+1

大多数的 Chromia 用户会使用轻客户，他们不运行整个区块链数据。他们必须依靠 Chromia 节点来从区块链查询数据，提供交易和付款的确认状态。轻客户用户该如何认证这数据？简单来说，他们不得不信任验证器节点。每个区块有所有验证器节点中的大多数签名。因此，要确认无效交易，三分之二以上的验证器节点需要被破解。

Light client security isn't significantly worse than full node security. Just over one third of nodes need to be compromised to produce a fork, but more than two thirds need to be compromised to produce an invalid block. The first scenario is far more likely, and light clients are protected against it to the same extent as full nodes.
轻客户安全并不比全节点安全糟糕。形成一个叉形指令只要破解三分之一以上的节点，但形成一个无效区块需要破解三分之二以上。第一种情形更有可能，轻客户与全节点被同等程度受保护。

Light clients can also take advantage of anchoring, including anchoring into PoW blockchains. Anchoring methods used in Chromia can produce compact proofs, this means that a user can benefit from anchoring without needing to run a full node.
轻客户也可利用锚定的优势，包括锚到 PoW 区块链。Chromia 所运用的锚定方法可以制造紧密证据，这意味着用户不需要运行全节点就可从锚定中获益。

In some cases the data retrieved from nodes is not important and does not need to be authenticated. In scenarios where the data does need to be authenticated, different data structures can be used depending on the nature of the data:
一些情况下，从节点上检索的数据并不十分重要，不用认证。在一些数据需要认证的情况下，不同数据架构可以根据数据本质进行使用：

1. Transaction Merkle tree: can be used to check that a transaction is confirmed and is valid. E.g. this can be used to verify a payment. The transaction Merkle tree root is present in the block header and is signed by nodes as a part of the consensus algorithm.
   交易默克尔树：可以用来核实交易被确认且有效。如它可用来验证付款。交易默克尔树根在块头呈现，由节点签名，作为共识运算法则的一部分。
2. State commitment Merkle tree: Typically a block header will commit to the set of rows which represent the blockchain state. This allows a light client to make sure that a certain row returned in response to a query is present in the latest blockchain state. State commitments can be disabled in high-performance blockchains as they increase blockchain overhead. A state commitment Merkle root is present in the block header and thus signed in same way as the Transaction Merkle root.
   声明承诺默克尔树：一个块头会投入于代表区块链状态的行中。这允许轻客户确认回复查询的某一特定行在最新的区块链声明中展示。在一些高效的区块链中声明承诺可以关闭，因为他们会增加区块链的开销。声明承诺默克尔树根在块头呈现，和交易默克尔树根一样的签名方式。
3. Assertions and indexers: Special data structures can be used to prove that the entire query response is correct and doesn't omit any data. If present, they are signed in the same way in the block header.

认定和索引器：特殊的数据结构可以用来证明整个查询回复时正确的且没有数据遗漏。如果出现，他们同样会在块头签名。

4. Signed query responses: When a query response is important but cannot be proven through indexers, a light client can submit requests to multiple nodes and receive signed responses.
   已签名的查询响应：当一个查询响应很重要但是不能通过索引器来证明时，轻客户可以向多节点提交请求并获得签名的回复。

A light client can authenticate data via validator node signatures only when it knows validator node public keys. Validator node pubkeys can be obtained from the directory chain. The directory chain itself can be validated using the root chain. The resolution process is as follows:
轻客户只有在知道验证器节点公共钥匙的时候才可以通过验证器节点签名进行数据验证。验证器节点公共钥匙可以从目录链中获得。目录链自身可以使用根链来验证。解析流程如下：

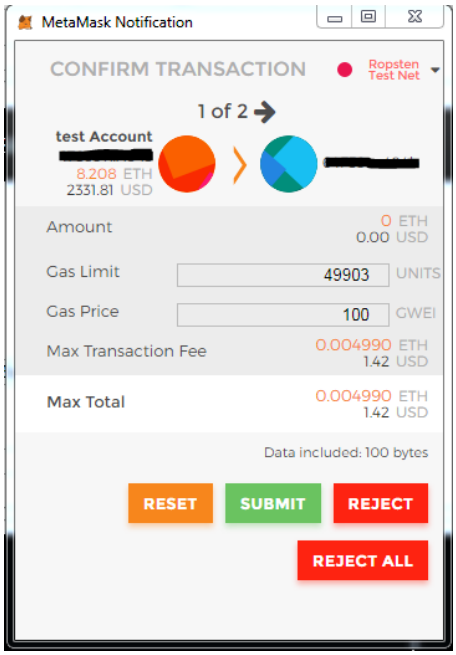
1. A light client comes with a built-in, hard-coded hash of the genesis block of the root blockchain as well as an initial list of root node public keys.
   伴随着轻客户的有内置，根区块链的创始区块的硬编码，还有根节点公共钥匙的初始清单。
2. A light client downloads the entire root blockchain to get an up-to-date list of root nodes. Root chain is extremely sparse with only one block per day, and thus this operation is not a lot of burden even to a light client.
   轻客户下载整个根区块链来获得最新的根节点。根链极其稀少，一天只有一个区块，所以这样的操作即使对轻客户来说也不是负担。
3. A light client can query any directory chain replica to retrieve a list of validators for the blockchain it is interested in and validate them with a state commitment mechanism, i.e. checking the signatures of root nodes.
   轻客户可以查询任一根链复制品来获取感兴趣的区块链验证器清单，用声明承诺机制来验证他们，即核实根节点的签名。
4. Results of query to the directory chain should also be confirmed via the anchoring chain and PoW anchoring.[20]
   目录链的查询结果也可以通过锚定链和 PoW 锚定来确认。

Dapp client and wallet security 分散应用程序客户和钱包安全

The Chromia team will develop ChromaWallet -- a wallet which can be used to hold Chroma tokens as well as any tokens on any Chromia blockchain which follows the FlexibleTokens standard. It will also provide an ability to interact with dapps using a simple form-based interface and to manage dapp accounts. ChromaWallet will be provided in desktop, mobile, and web app formats and will target hardware wallet integration.
Chromia 团队会开发幻彩钱包，一个可以用来存储幻彩代币以及任何遵循灵活代币标准的 Chromia 区块链上代币的钱包。它也可以用简单的基于表单的界面来与分散应用程序互动，管理分散应用程序账户。幻彩钱包将提供电脑版，手机版和网页版，目标实现硬件钱包整合。

[20] Step #4 is necessary to makes sure that a collusion of root nodes cannot compromise any other blockchain. 第四步可以确保根节点的共谋无法破解其他区块链。

In a future version ChromaWallet will be able to function as a general-purpose dapp browser, sandboxing dapp UI code execution and offering graphical interface rendering on a web technology stack. The dapp browser will be able to download dapp UI code from a Chromia blockchain. Of course, it won't be able to guarantee that this code is free of bugs or security defects, but it will be able to ensure that code can only be updated together with the dapp itself and that all users run identical code (i.e. code cannot be bugged specifically for one user). Note that the dapp browser functionality won't be present in the MVP version.
在以后的版本中，幻彩钱包能够作为一个多用途的分散应用程序浏览器，沙盒化分散应用程序 UI 代码执行，提供网页技术堆栈上的图像界面。分散应用程序浏览器将能够从 Chromia 区块链上下载分散应用程序 UI 代码。当然，没有办法保证代码没有故障或安全问题，但它可保证代码只可与分散应用程序本身一起更新，所有的用户都使用同样的代码（代码故障不会发生在单一用户的身上）。值得注意的是分散应用程序浏览器功能不会在 MVP 版本中呈现。



Instead, dapps which require complex UI, such as games, can be implemented using a separate client delivered as a web or mobile application. In this case security can be controlled through the use of sub-accounts. The dapp client will receive a private key of a sub-account which belongs to a user and will be able to sign transaction on behalf of the user. This means that the user can perform game actions in a natural way, similar to how "normal" games work. There will be no confirmation dialogs bugging users for each action he takes in a game, as seen in Ethereum MetaMask and EOS Scatter.
相反，像游戏这样要求复杂 UI 的分散应用程序可以通过单独的网页或手机应用程序来运行。这种情况下，可以通过附属账户的使用来控制安全。分散应用程序客户会收到用户附属账户的一个密钥，并可以代表用户来签署交易。这意味着用户能够像常规游戏一样，以自然的方式开展游戏活动。用户不再会被游戏中每一操作的确认对话而烦扰，这在以太坊 MetaMask 和 EOS Scatter 上经常遇见。

However, actions which are sensitive, such as a transfer of a large sum of tokens, might require confirmation using a different sub-account which is managed by ChromaWallet. This means that malicious dapp code won't be able to do significant harm. This also means that large-value transactions can benefit from 2FA or hardware wallet integration implemented in ChromaWallet.
但是，像转移大量代币这些敏感的动作需要幻彩钱包上不同的附属账户进行确认。这就意味着恶意分散应用程序代码无法造成重大伤害。也意味着高值交易能从幻彩钱包上的 2FA 或硬件钱包整合中获益。