区块链是一项巧妙的发明，有望使数字世界更加安全和分散。通过允许数字信息的分发而不是复制，区块链技术创建了一种新型互联网。最初是为数字货币比特币而设计的，现在科技界正在寻找该技术的其他潜在用途。在不久的将来，我们将看到区块链被用于各种日常交易，无论是银行交易，还是电子商务网站购物。

技术世界的每个人都了解或至少听说过区块链。但是只有极少数的开发人员知道如何开发区块链代币或应用程序，或者从哪里开始。让我们稍微详细地看看区块链应用程序的开发过程。

区块链开发简介

现在，我假设您已经了解了区块链的基础知识，即区块链是什么，它起源于何处，可以在何处使用。

与其他开发过程一样，区块链应用程序或代币开发也需要我们描述应用程序的范围和用途。它可以是像比特币这样的一枚代币，也可以是一份精明的房地产合同或其他东西。让我们看看这些实际发展的前提步骤

1. 发展的观点

第一步是决定——我想用区块链做什么?

如果你想用区块链来为一个自制的业余应用程序存储用户资料，你可能走错了路。即使你希望使用区块链获得一个中等大小的应用程序，你也需要权衡区块链的利润与成本。您需要为您的应用程序确定用例，并确保您的想法是否需要区块链。需要注意的是，区块链是一种加密数据和验证事务的方法，如果实现不正确，它不能保证交易上的额外安全性。

一旦您得出区块链对您的项目是必不可少的结论，您就需要认识到区块链的开发是昂贵的。有几种开发区块链应用程序的方法，下一节将讨论这些方法，它们的成本和功能各不相同。

区块链使用作为一个有效的例子, 如果您是一个房地产代理，并希望构建一个基于区块链的供应链应用程序，该应用程序可以为您出售的每个属性保留一个分类账，那么您应该了解应用程序的多个用例，以及它将如何为您的业务和消费者带来好处。

2. 确定合适的区块链平台

一旦您认为您的业务需要基于区块链，您就需要确定要使用的合适平台或技术。有几种基本方法可以解决

a. 创建新的区块链——您可以选择创建自己的区块链框架，其中从算法到事务验证，从技术堆栈到代币交易费，一切都由您决定。这是最全面的区块链开发方式，也是最昂贵的。你实际上是在考虑创造另一种比特币，尽管听起来有利可图，但它可能会让你花费数十万美元以上的资金。通常只有在创建自己的加密货币时才会选择此选项。

b. 克隆流行的区块链平台 ——开发基于区块链的应用程序的另一种更有效的方法是使用流行的区块链平台进行开发。这些平台是开源的，因此您可以使用它们的存储库并将代码部署到自己的服务器上。我们要问的主要问题是——为什么这个世界会接受你创建的区块链。请记住，区块链平台与网络中能够验证事务的节点数量一样成功。

流行的平台有以太坊、Hyperledger Fabric和Hyperledger SawTooth。每一个都有特定的特点，可以帮助你做出决定。

最受欢迎的区块链平台是以太坊，它可以保存你的代币发展)。关于以太坊的几点：

.
以太坊是一个开源的、基于公共区块链的分布式计算平台，具有智能合约的功能。

· 以太坊使用了一种名为“Ethash”的工作验证算法，这种算法需要更多内存，因此难以进行挖掘。

· 以太坊中的智能合约是用可靠的编程语言 Solidity 编写的，这是Javascript的一个子集。

c. 在现有的区块链平台上使用代币——这与上一点稍有不同。最后一点，我们克隆了整个区块链平台并将其部署到我们自己的服务器上，假设我们有足够的网络节点，这些节点将通过“挖掘”来验证交易。

但我们也可以“创建代币”，并将其部署到像以太坊这样正在运行的区块链上。这些平台提供了现成的api、算法和挖掘策略，以便在应用程序中轻松实现区块链(区块链即服务)。您不需要为您的交易创建单独的waller，因为以太坊代币可以被各种现有的钱包接受。

这类似于在Shopify上创建自己的电子商务商店。Shopify平台上的所有电子商务功

能都可以随时使用，用户只需填写所需数据，就可以在Shopify上创建自己的商店。类似地，您可以用可靠语言编写自己的令牌，并将其部署在以太坊上(或者为不同的区块链平台使用不同的语言)。现有的平台将为您提供现成的服务，您可以使用代币进行交易。记住，代币可以是代币，也可以是智能合约。

3.原型开发

鉴于区块链的开发成本非常高，建议在将其部署到实时服务器或现有的区块链平台(如以太坊）上之前，首先开发一个原型应用程序，以确保一切正常工作。

在原型开发期间，您还应该决定应用程序的哪些部分是“on-chain”的，哪些是“off-chain”的。简单地说，由于您正在创建一个使用区块链的web应用程序或移动应用程序，因此可以在一般的云托管上运行正常的功能，而不需要区块链。然后是应用程序的交易部分，您可能会将其放在区块链平台上。

您还应该决定应用程序(或其部分)是构建在许可网络中，还是构建在无许可网络中。

· 无许可的网络：在这里，每个人都可以加入并开始验证。最著名的例子是比特币和以太坊网络

· 许可的网络。在这种情况下，网络所有者决定谁可以加入网络，只允许少数成员验证块。协商一致机制可以与无许可网络相同，也可以是完全独特的设计(例如基于权限的)。

尽量将链上api与链外api分开，因为它们将驻留在不同的位置。决定应用程序的一致算法和事务策略。如果您使用的是现有的区块链平台，那么这个阶段将更容易，因为许多东西已经在这些平台中有效地实现了。

4. 技术

. web3.js - Ethereum JavaScript API(文档)

. Dapp浏览器-Desktop Mist, Parity 、 Metamask 和mobile ones Toshi, Cipher 和Trust

. 智能合约的稳固性(文件编制)

. 开放Zepplin -智能合约开发(文档)

. 从事-无服务器分散式应用使用Ethereum,
IPFS和其他平台https://embark.status.im/

. 最流行的Ethereum开发和测试框架http://truffleframework.com

. Metamask -在浏览器中运行Ethereum
dApp而不需要运行完整的Ethereum节点(https://metamask.io/)

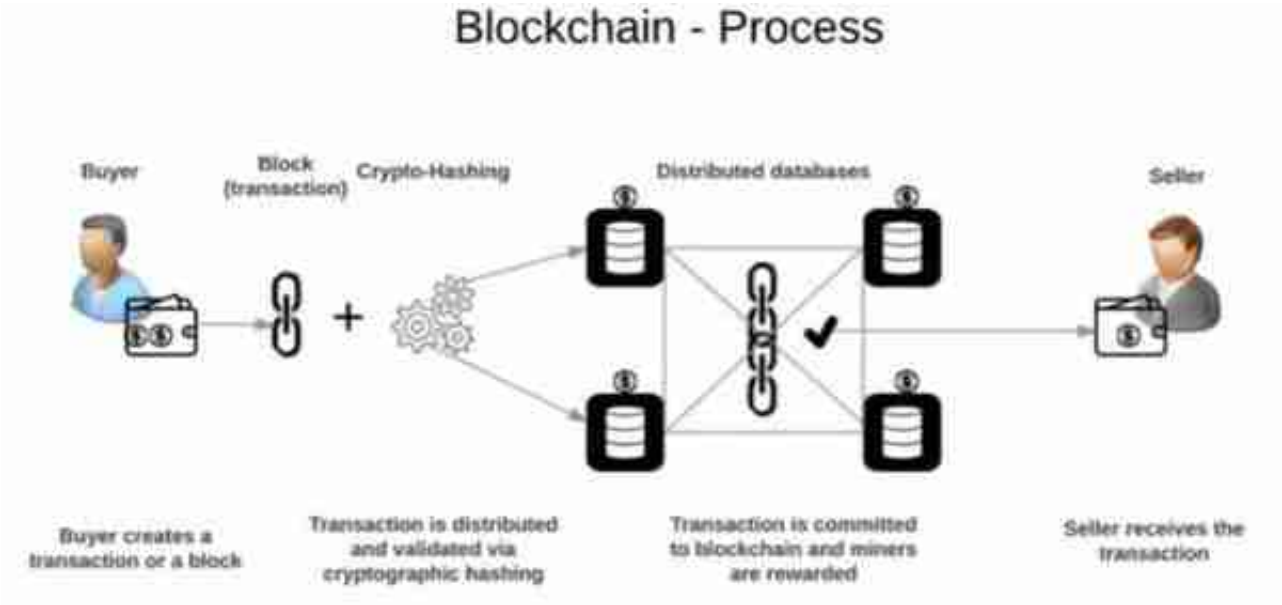
. Parity -最先进的Ethereum部署客户端(https://paritytech.io/)

. Etherscan - Ethereum上的块资源管理器，用于监视(https://etherscan.io/)

除此之外，常规框架还可以用于像react这样的应用程序/服务器开发。用于移动应用的js、nodejs和原生技术。

5. 发展

这是区块链应用程序开发的核心元素。为了简单起见，我们将经历2c点中描述的过程。如上所述，即在现有的区块链平台上使用代币。首先理解事务机制是很重要的。



Token本质上是一个长长的字母数字字符串，充当您智能合约的唯一标识符。区块链钱包上的每个用户都有唯一的公钥和私钥(类似于长密码)。这些键用于识别用户的信用卡/借记卡，或指向智能合约。这是非常类似的，但比添加一个新的受益人在您的银行帐户使用他们的银行帐号等更安全。

您可以为以太坊创建自己的智能合约或代币。您应该首先创建一个测试代币，并在将其部署到真实的区块链上之前验证您的功能。遵循这个官方指南来创建您的第一个以太坊代币，以及这篇博客文章来理解创建您自己代币的细微差别。一旦您创建了代币，您就将其“放在链上”，本质上类似于在服务器上部署代码。

交易开始时，一个用户发送一个发送代币的意图，该意图被网络确认为有效(如果您拥有代币且没有将其发送给任何人)。然后您的代币信息与您的私钥相结合，私钥将吐出一个数字代码，然后使用发送方的公钥由网络确认。这是可能的，因为可以用公钥验证与私钥签署的合约，但是无法发现公钥与私钥之间的相关性，因此一切都是安全的。

总之，整个过程类似于加密和解密。信息的分散化和块的历史包含在加密中，使其安全和篡改证明。

此外，您将为其构建API

-执行审计职能。

-储存和检索数据。

-生成密钥对并将其映射到特定地址。

-利用哈希值和数字签名进行数据认证。

-管理和触发智能合约以运行应用程序的业务功能。

这篇文章是构建区块链应用程序的第一步。让智能合约“更智能”、确保你的代币不可被黑客攻击，或者至少极其难以被黑客入侵，这些都涉及到巨大的复杂性。按照上面的步骤，您可以为您的应用程序制作基于区块链的最小可行产品。