# 区块链展览
# 说明书


**上海素图科技有限公司**

电子邮件：liangshuang@sutu.tech　　电话：xxxxxxxxxxx

网站：www.sutu.tech

# 导言

*区块链·数学保证的信任合作*

2008 年，一位自称为中本聪（Satoshi Nakamoto）的计算机专家，在网络上发布了一种点对点的网络货币比特币（Bitcoin）的设想，其中首次提到了区块链这样结构设想。次年，正式发布和运行了比特币节点，这使得越来越多人加入到比特币的网络中来，最终让世人所熟知。

让比特币得以顺利运行的区块链技术，也成为大家所追捧和感兴趣的焦点。区块链技术综合了计算机历史上多种重要的技术成果，要理解区块链技术，需要先理解各个独立的计算机技术。

本展览将区块链按照涉及的技术方面，分为八个方面分别进行展示，并配有一页指导手册让参观者深入思考，希望通过本次展览，让大家了解到区块链的方方面面，为将区块链应用到自己的事业中打好基础。

## 策展人

**梁爽**：上海交大硕士，国产原创区块链数据库"优链数据库"架构师。

**崔璨**：同济大学硕士，文化工作者，长年组织策划各类文化公益普及活动。

# ① 代币机制

## 区块链的价值

代币机制决定了区块链的价值如何体现与流转，通过此装置，可以清晰的理解通胀型代币和通缩型代币，并了解无币区块链。

# 代币机制

## 展示目的

通过此装置，可以清晰的理解通胀型代币和通缩型代币，并了解无币区块链。

## 涉及选项

- 不发币: 也被称为无币区块链，无一般等价物，很难形成价值网络
- 紧缩型代币: 通过挖矿创造初始代币，但代币总量固定
- 膨胀型代币: 通过挖矿创造初始代币，但代币上限不定

## 使用方法

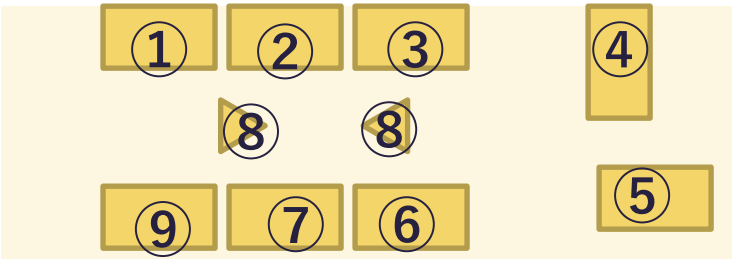
通过展板了解到不发币的无币区块链的特点，通过通缩型代币和通胀型代币的对比，可以了解到这两种形式的区别和应用场景。

# ② 账本模式

## 区块之间的连接方式

区块之间的连接方式决定了区块链的并行性，通过此装置，可以了解两种主流的区块连接方式：区块链和单向无环图。

区块链技术展示空间



# 账本模式

## 展示目的

区块链虽然以“链”命名，但随着技术的发展，已经不仅仅有链状结构这一种，还有类似单向无环图这样的结构，本装置可以让参观者亲自尝试将不同的“区块”连接起来，形成区块链或者单向无环图形状，以此了解和熟悉区块链的两种主要结构。

## 涉及选项

- 区块链: 由比特币创造，将区块链以链状结构相连
- 单向无环图: 有类似于区块链的性质，不过以图的形式使得并行性得到增强

## 使用方法

本展品由一个个“区块”组成，每个区块有一些孔和一个“尾巴”，可以使得区块之间产生连接状态，根据期望连接成区块链结构或者单向无环图结构的选择，可以进行不同的连接实验。

# ③ 数字摘要

## 标识信息唯一性

通过数学方法，可以标识出一个信息的唯一性，通过此装置，可以手动尝试选择不同的算法，选择不同的输入，看到不同的结果。

# 数字摘要

## 展示目的

数字摘要具有以下三个特点：1）输入可以是任意长的字符串；2）输出是固定长度的；3）计算过程是高效的。

通过此装置，我们将形象的向参观者展示数字摘要的三个特点，参观者可以亲手进行操控实验，可以更加深入的理解数字摘要的意义和特点。

## 涉及选项

- SHA2: SHA 算法家族的第二代，在比特币中使用为 SHA256
- Keccak: 也称 SHA3，在以太坊中被使用

## 使用方法

通过此装置，我们可以选择一种数字摘要算法，并且输入不同的字符串，我们可以观察到：

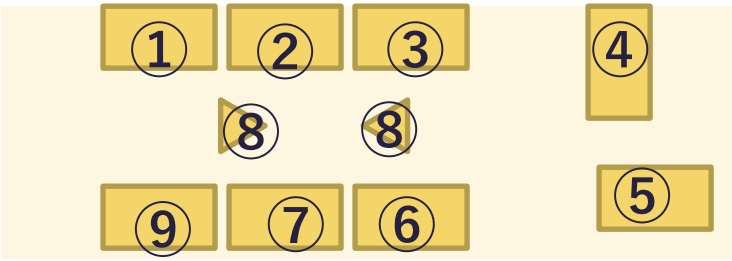
- 输入的字符串不同，则输出的信息也会是不同的；
- 输入不同长度的字符串，输出信息的长度会是固定相同的；
- 输入相同的字符串，输出的信息会是完全相同的；
- 整个过程中可以观察到计算过程是高效的。

# ④ 数字签名

## 安全防伪的基础

基于一个困难的数学问题，使得签名可以安全防伪，通过此装置，两个参与者可以进行攻防比赛，经过游玩，更深刻理解的数字签名。

区块链技术展示空间



# 数字签名

## 展示目的

该装置模拟了数字签名过程和暴力破解数字签名的过程，并且以游玩竞技的形式进行了展现。通过此装置，两个参与者互相进行攻防比赛，经过紧张的游玩后，可以对数字签名有更加深刻的理解。

## 涉及选项

- 椭圆曲线: ECDSA，被大部分区块链所采用
- RSA: 经典的数字签名算法，广泛应用于银行、证书等领域

## 使用方法

开始时，其中一位参与者作为信息的发送方，根据对面墙上的提示，选择要发送的信息，并悄悄地设置一个隐秘的私钥，私钥设置完成时，对应的公钥会被公开的显示在顶上，使得所有人都能看见，参与者继续使用私钥进行签名，完成以上步骤后，点击发送。

一辆载有液晶显示屏的小车，将会从发送者缓缓地驶向对面墙壁，液晶显示屏上会显示发送的信息以及其对应的数字签名，在这个过程中，另外一位参与者作为攻击者，试图去篡改信息，该攻击者可以在小车还没有抵达墙壁以前进行攻击，攻击的方式是选择一个信息，再输入一个两位数字，点击攻击按钮，就会试图暴力破解数字签名，若破解成功，攻击者胜利，若失败，这可以再输入一个两位数字继续尝试，当小车抵达墙壁时，就算作是发送方成功了。

# ⑤ 智能合约

## 扩展的方法

可以执行自定的逻辑，使得区块链具备扩展性，通过此装置，可以清晰的理解虚拟机是否完整的区别，并了解无虚拟机的特点。

# 智能合约

## 展示目的

通过此装置，可以清晰的理解虚拟机是否完整的区别，并了解无虚拟机的特点。

## 涉及选项

- 无法执行: 不能执行任何智能合约，只能进行区块链预定的指定操作
- 受限栈模式: 在比特币中使用，可以执行少量运行的命令
- 图灵完全: 图灵完全的虚拟机，可以执行任何类型的逻辑

## 使用方法

模型中有三个小人，以及三条道路，我们可以先观察到：

- 第一个小人的道路一出发就是尽头了，这表示此路不通，无法执行任何智能合约；
- 第二个小人的道路很窄，只能容纳一辆自行车，这就是受限栈模式，只能执行有限的扩展功能；
- 第三个小人的道路很宽敞，不但能容纳自行车，还能容了小轿车，这就是图灵完全的虚拟机，可以执行丰富的扩展功能，但也因为其丰富性，使得系统里面很容易出现问题，在模型上表现为两个交通工具可能会撞车。

# ⑥ 权限控制

## 新节点的加入

区块链拥有非常多的节点，新节点的加入方式主要分受限和不受限两种，通过此装置，可以亲自实验一下两种不同方式。

# 权限控制

## 展示目的

通过此装置，以实验的方式清晰深入的理解授权接入和公开接入的区别。

## 涉及选项

- 授权接入: 只有获得授权的节点才可以接入区块链网络
- 公开接入: 任意节点均有机会接入到该区块链网络

## 使用方法

我们准备了很多活动的积木（代表节点），参与者可以选择一部分放在世界地图上，并启动对应的按钮，分别表示授权接入和公开接入， 刚启动按钮时，所有已经存在的积木，表示其连接的线都会亮为绿灯，表示其相互连接上了，接下来我们可以把剩下的积木，继续放在空的位置上，我们可以观察到：

- 如果启动的是授权接入，新放入的积木，与已经存在的积木之间的连线，会显示为红灯，表示未获得授权，无法接入；
- 如果启动的是公开接入，新放入的积木，与已经存在的积木之间的连线，会显示为绿灯，表示已经连接成功，顺利接入区块链网络。

# ⑦ 接口设计

## 通用或专用

接口设计决定了区块链对外的展现形式，通过此装置，可以清晰的理解通用接口和专用接口的区别和特点。

# 接口设计

## 展示目的

通过此装置，可以清晰的理解通用接口和专用接口的区别和特点。

## 涉及选项

- 远程过程调用: RPC，一种易扩展升级的接口，广泛用于区块链项目
- 描述性接口: 以 REST 为代表的描述性接口，广泛用在网络应用中

## 使用方法

展示台上有两组插头和插座，一个是一个大圆柱形，即通用型接口，另外一个是一个三角形加一个正方形的接口，这是专用型接口。我们可以进行以下实验：

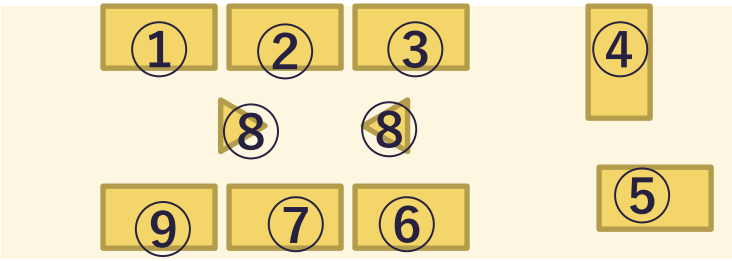
- 专用型接口的插头可以顺利地插入专用型接口的插座，我们拿起插头，可以清晰地看到一个三角形和一个正方形，这个表示的在这个接口上传输的数据类型；
- 通用型接口的插头可以顺利地插入通用型接口的插座，我们拿起插头，只能看到一个大的圆柱形，这只能泛泛的表示在这个接口上传输的数据，并不明确；
- 通用型接口的插头无法顺利的插入专用型接口的插座，因此通用型插头是无法接入专用型插座的；
- 专用型接口的插头可以顺利地插入通用型接口的插座，因此通用型插座是可以接收专用型插头的输入的。

# ⑧ 共识机制

## 记账的策略

共识机制就是多个节点如何获得记账权限的策略机制，通过此装置，可以清晰的理解工作量证明和权利证明两种重要的共识机制。

区块链技术展示空间



# 共识机制

## 展示目的

通过此装置，可以清晰的理解工作量证明和权利证明两种重要的共识机制。并通过旁边的查询机了解和理解更多的共识机制。

## 涉及选项

- 工作量证明: 在比特币中使用，通过大计算量避免女巫攻击
- 新工作量证明: 通过大计算量避免女巫攻击，通过设计新的方法，避免跨链算力攻击
- 权利证明: 根据在区块链上所拥有的权利（股权）来获得记账（并获得收益）的概率
- 委托权利证明: 将拥有的区块链权利委托给部分用户，这部分用户平均分配获得记账概率

## 使用方法

工作量证明实验装置：这是一个三角形的展台，三边分别有一个按钮和一个信号灯，当获得记账权限的时候信号灯会闪烁并变亮，参观者通过快速的点击按钮（即证明工作量），使得自己一方的信号灯可以更多机会和概率闪烁并变亮（即获得记账资格）。

权利证明实验装置：这是一个三角形的站台，三边分别有四个凹槽和一个信号灯，我们可以将代表权力的积木，放入凹槽，即认为该方拥有对应数量的权利，当获得记账权限的时候信号灯会闪烁并变亮，现在信号灯会亮的方向，是根据对应拥有权力的数量所决定的。

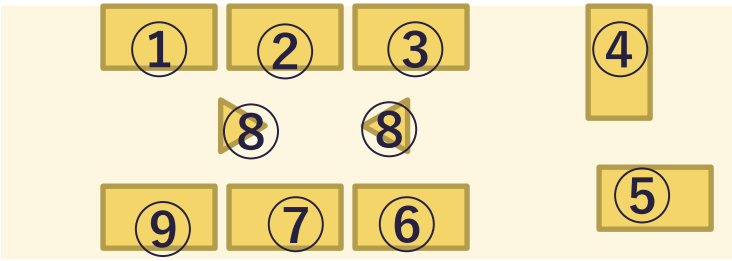
共识机制在区块链领域，有非常丰富的创新和应用，是区块链安全性的重要一环，可以在我们提供的查询机上了解和理解更多的共识机制。

# ⑨ 架构报告

## 创造你的区块链

这是本次展出的综合性装置，通过学习区块链的八个架构和组件，亲自选择自己喜欢的组件，来构建一个你自己的区块链。

区块链技术展示空间



# 架构报告

## 展示目的

这是本次展出的综合性装置，通过学习区块链的八个架构和组件，亲自选择自己喜欢的组件，来构建一个你自己的区块链。

## 使用方法

参观者进入到会场的时候，可以在入口处领取到你常带有指导的空白表单，参观者在展区内游览 8 个不同的区块链技术展示装置时，可以分别将自己所喜欢和选择的方向对应的贴纸，贴至该表单上。

完成所有 8 项表单后，在展出的出口处，使用我们特定的报告装置，扫描你的表单，该装置将会打印出你所设计的区块链的报告，可以将该报告粘贴至该已经完成的表单中。

最终参观者可将此表单带走，作为参观本展示空间的成果。