ArchSummit

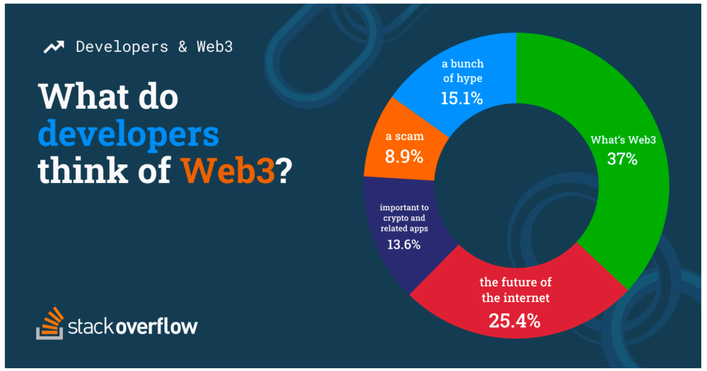
全 球 架 构 师 峰 会

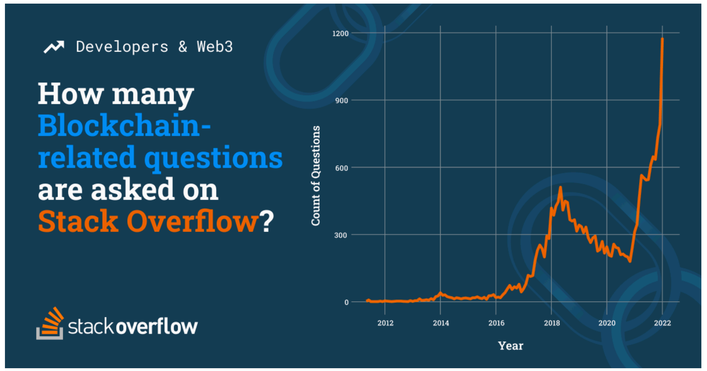
全球架构师峰会·杭州站

主办方：InfoQ

Web3.0去中心化预言机网络技术剖析

Wally Yu - Solutions Architect
Sep. 2022

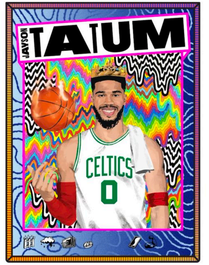


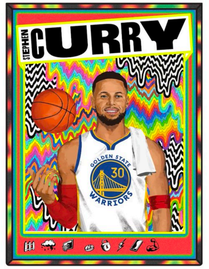


Demand Growth for Engineering Roles

Role	Percentage Growth
Blockchain engineer	+517%
Security engineer	132%
Embedded engineer	76%
Data engineer	38%
Backend engineer	33%
ML engineer	27%
Mobile engineer	15%
Full-stack engineer	7%
Frontend engineer	4%

All growth data has been normalized to account for Hired's overall marketplace growth.





Agenda

1.区块链与智能合约

2.预言机问题

3.数据上链

4.链上随机数问题

5.从Web2到Web3

6.Ideas?

小测试

发明区块链技术的人的名字是什么：

A. 上本聪

B. 中本聪

C. 下本聪

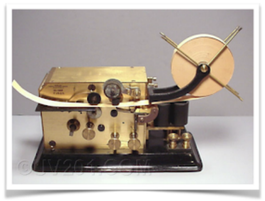
What is a blockchain?

区块链是啥

A blockchain is highly **secure**, **reliable**, and **decentralized network** that stores data, exchange values, and record transaction activity in a **shared ledger** that is **not controlled by any central authority**,
but instead maintained by computers all around the world.

技术驱动
合约的演变

The Next Stage: Technologically Enforced Contracts



Telegraph Agreements
(Electronically Signed)
1869

Telex Machines
(Telecom Based)
1930s

Digital Agreements
(Internet Based)
1980s to Present

Smart Contracts
(Blockchain Based)
2009 to Present

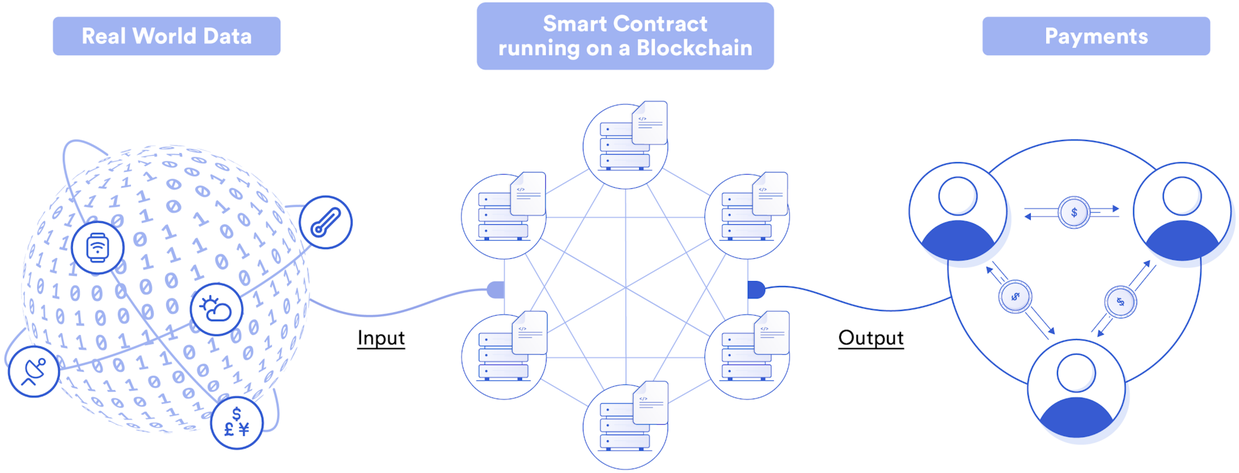
Chainlink

Smart Contracts
智能合约

- A Smart Contract is **a self-executing contract** with the terms of the agreement being **directly written into computer code**
- Programmatically implement **a series of if-then rules** without the need for third-party human interaction

Smart Contracts Run on the blockchain

运行在区块链之上的智能合约



Truth > Trust

Truth > Trust

Truth > Trust

Truth > Trust

Truth > Trust

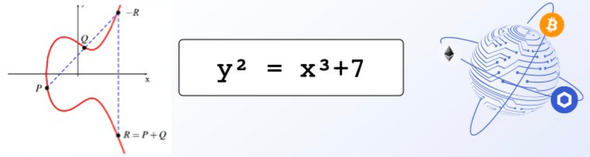
Cryptographic Truth is Strictly Better than “Just Trust Us”

“Just Trust Us” Paper Promises

- **Control is completely given away**
- Counterparty risk is high and opaque
- Transparency is purposefully removed

https://hackernoon.com/what-is-the-math-behind-elliptic-curve-cryptography-f61b25253da3

Cryptographic Truth Guarantees

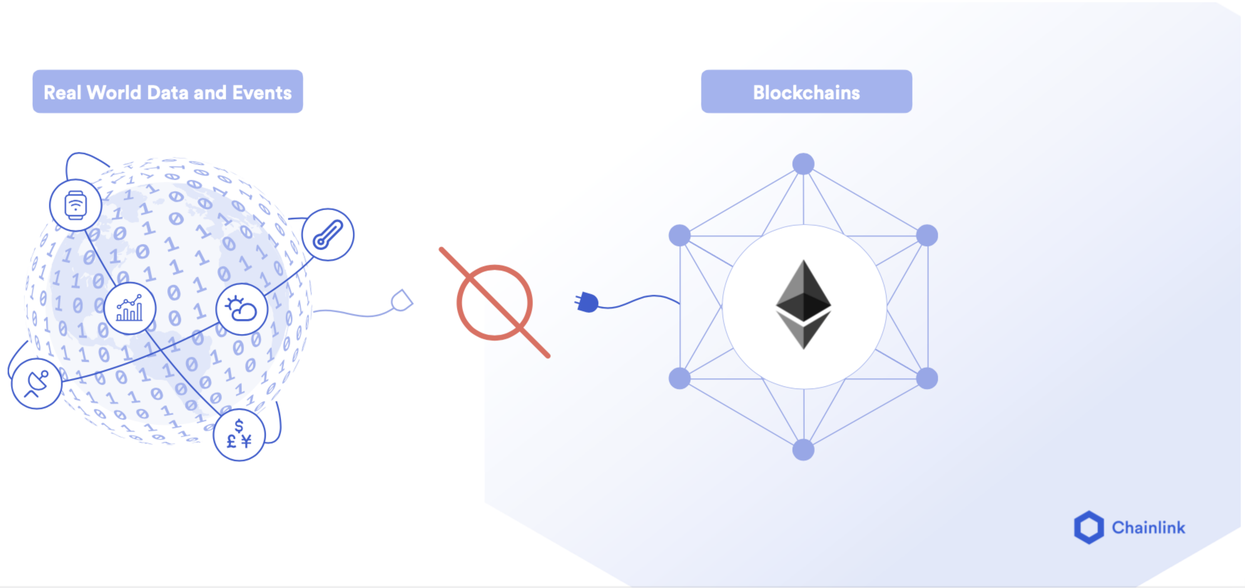


- **Control is in the user’s hands**
- Counterparty risk is low and transparent
- Transparency is unavoidably built-in

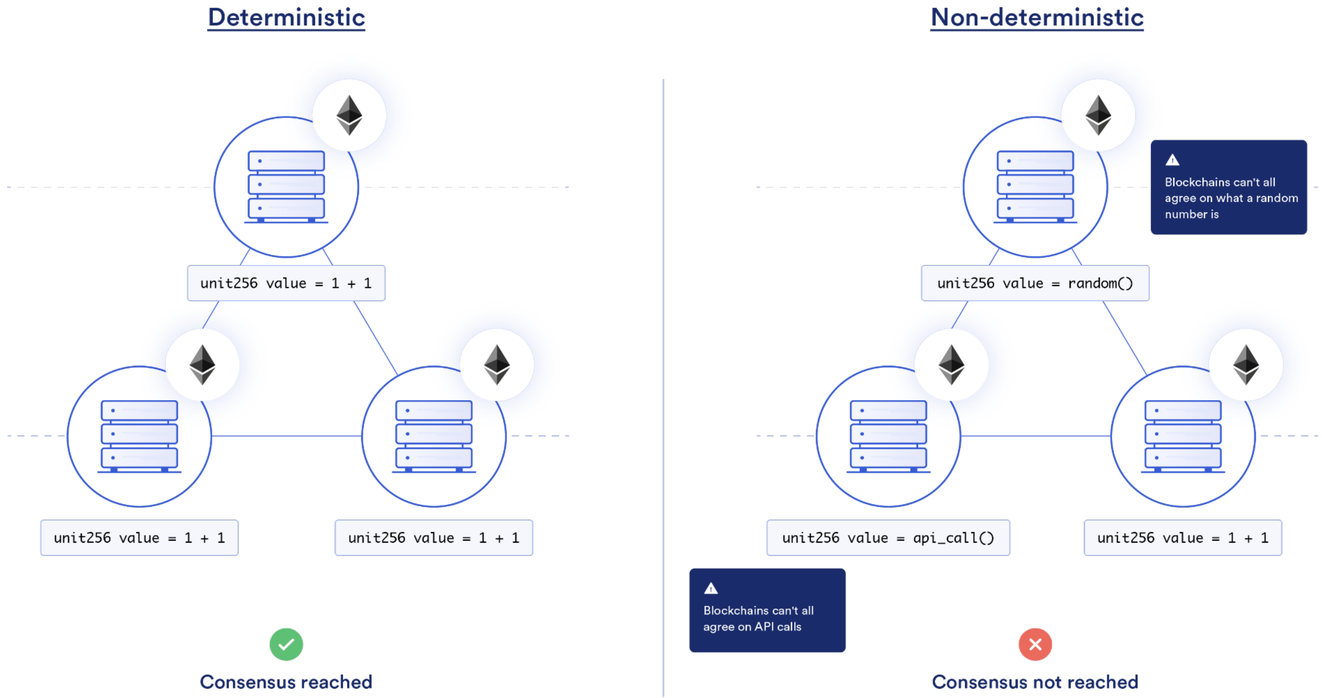
Chainlink

The Oracle Problem
预言机问题

Smart Contracts are unable to connect with external systems, data feeds, APIs, existing payment systems or any other off-chain resources on their own.



区块链的确定性


Deterministic
unit256 value = 1 + 1
unit256 value = 1 + 1
unit256 value = 1 + 1
Consensus reached
Non-deterministic
Blockchains can't all agree on what a random number is
unit256 value = random()
unit256 value = api_call()
unit256 value = 1 + 1
Blockchains can't all agree on API calls
Consensus not reached

The Smart Contract Connectivity Problem

智能合约的局限性

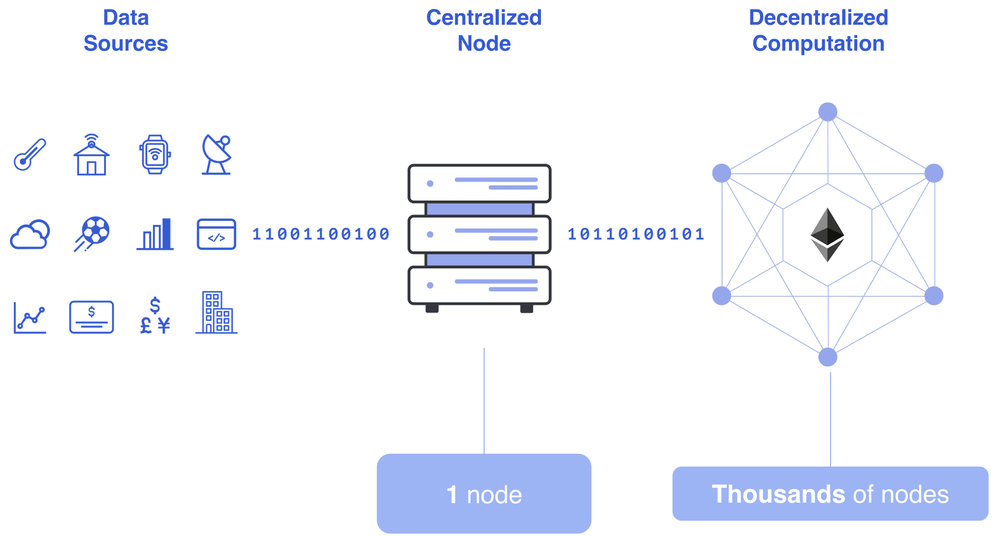
The Smart Contract Connectivity Problem

智能合约的局限性

Blockchain Oracle: Any device that interacts with the off-chain world to provide external data or computation to smart contracts.

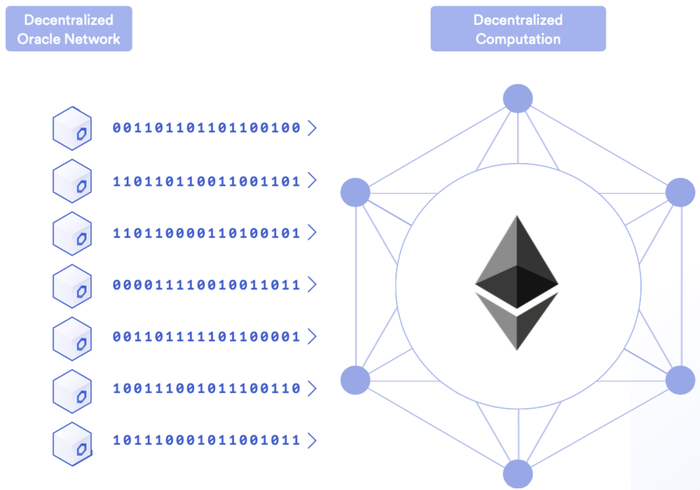
Centralized Oracles are a Point of Failure

中心化预言机的单节点故障



去中心化
预言机网络

A Decentralized Oracle Network



Decentralization

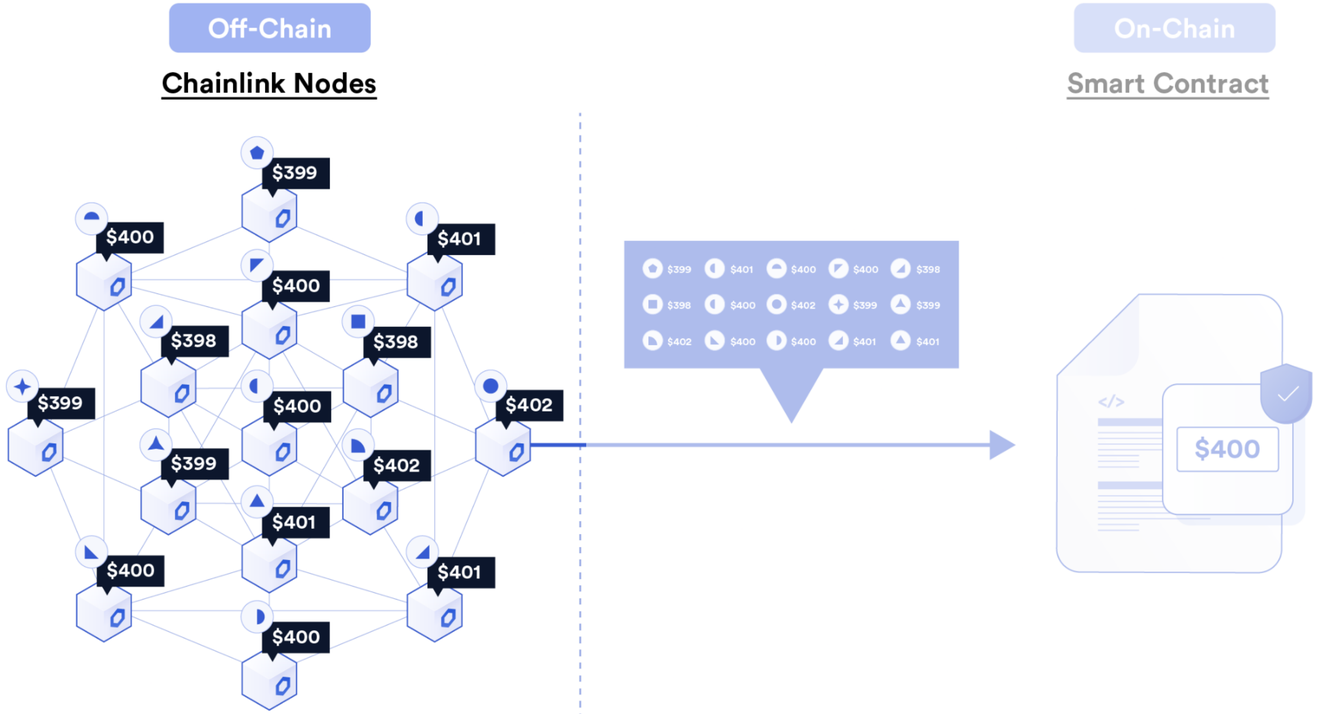
Full replicas being run by independent and sybil resistant node operators, coming to consensus about a computation.

Focused on data validation and consensus about individual off-chain values to make them reliable enough to trigger contracts.

Node Operators are security reviewed, can provide a proven performance history and are high quality and highly sybil resistant.

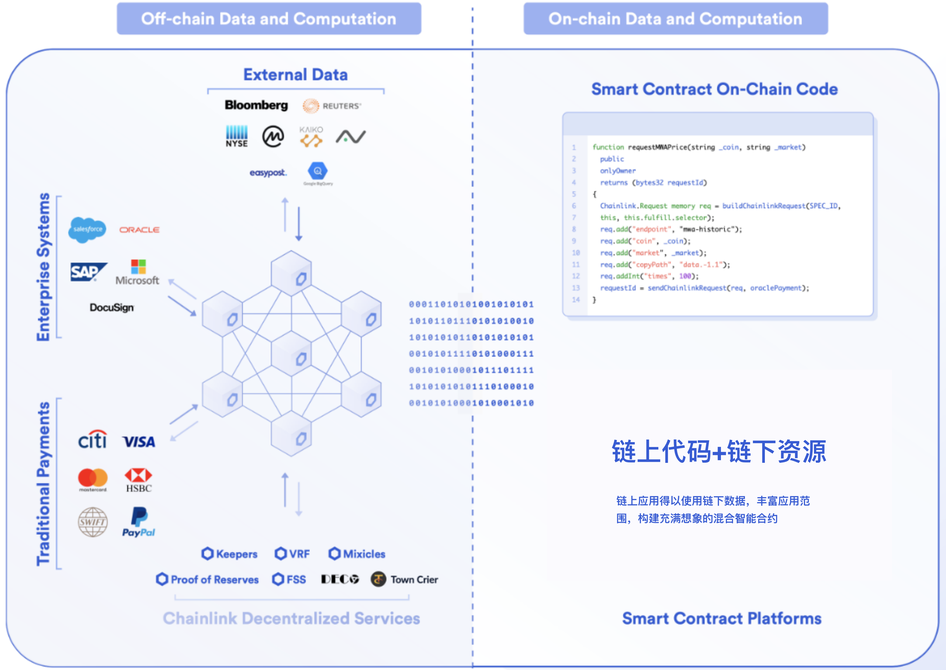
Chainlink

去中心化预言机网络共识

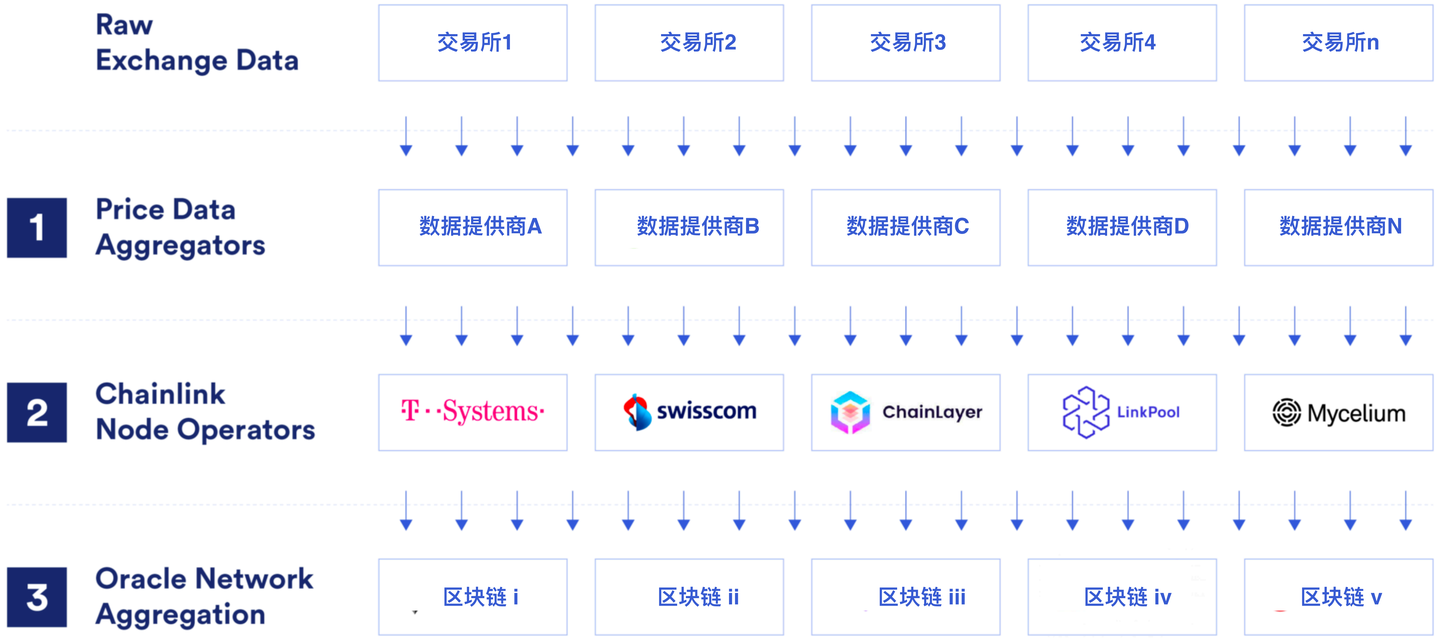


Hybrid Smart Contracts Combine On-chain & Off-chain Systems

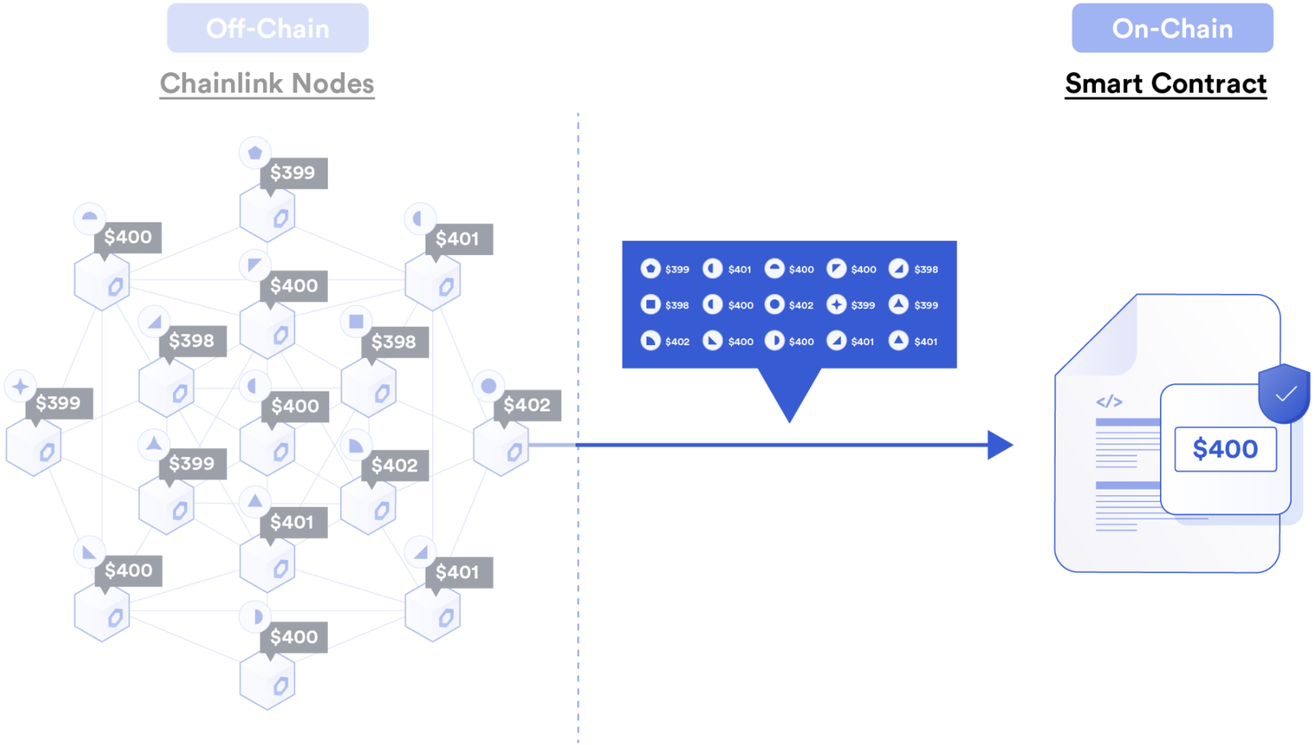
混合智能合约



预言机数据安全
&
上链机制



去中心化
预言机网络
共识
&
上链



丰富的链上数据

https://data.chain.link/

Foreign Exchange

A complete list of Chainlink Data Feeds tracking forex pairs.

Ethereum Mainnet 12

Feed	Contract address	Network	Users	Added
AUD / USD	0x77f9...f022	Ethereum Mainnet		December 11, 2019
BRL / USD	0x971e...ee0f	Ethereum Mainnet		April 13, 2021
CAD / USD	0xa343...1c8e	Ethereum Mainnet		December 17, 2020
CHF / USD	0x449d...b13a	Ethereum Mainnet		December 11, 2019
CNY / USD	0xef8a...759a	Ethereum Mainnet		February 11, 2021
EUR / USD	0xb49f...34c1	Ethereum Mainnet		December 11, 2019
GBP / USD	0x5c0a...d4b5	Ethereum Mainnet		December 11, 2019
JPY / USD	0xbce2...beb3	Ethereum Mainnet		December 11, 2019
KRW / USD	0x0143...d0f3	Ethereum Mainnet		February 16, 2021
NZD / USD	0x3977...5f3e	Ethereum Mainnet		May 5, 2021

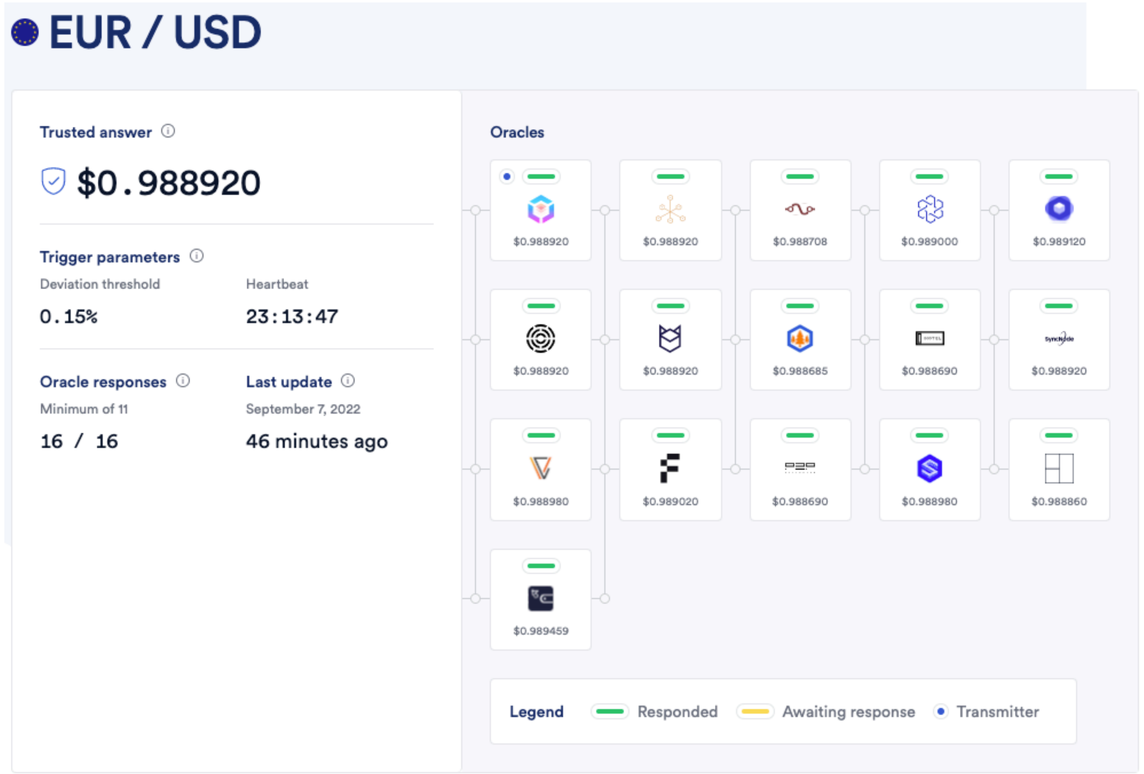
Commodities

A complete list of Chainlink Data Feeds tracking commodities pairs.

All networks 13

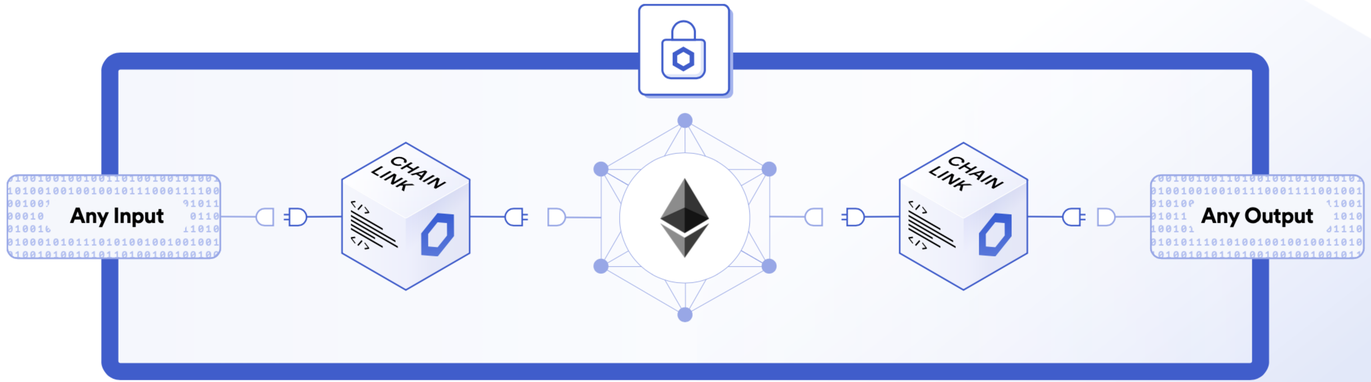
Feed	Contract address	Network
WTI / USD	0xf358...185c	Ethereum Mainnet
WTI / USD	0xe9d0...c4d1	Heco Mainnet
XAG / USD	0x3795...5235	Ethereum Mainnet
XAG / USD	0x8173...16ad	BNB Chain Mainnet
XAG / USD	0x290d...ee49	Optimistic Ethereum
XAU / USD	0x214e...a0d6	Ethereum Mainnet
XAU / USD	0x41e7...9b0b	Heco Mainnet
XAU / USD	0x8689...1cd0	BNB Chain Mainnet
XAU / USD	0x4a5a...b94c	Gnosis Chain Mainnet
XAU / USD	0x0c46...e410	Polygon Mainnet

数据更新触发机制


EUR / USD
Trusted answer
$0.988920
Trigger parameters
Deviation threshold
0.15%
Heartbeat
23:13:47
Oracle responses
Minimum of 11
16 / 16
Last update
September 7, 2022
46 minutes ago
Oracles
$0.988920
$0.988920
$0.988708
$0.989000
$0.989120
$0.988920
$0.988920
$0.988685
$0.988690
$0.988920
$0.988980
$0.989020
$0.988690
$0.988980
$0.988860
$0.989459
Legend
Responded
Awaiting response
Transmitter

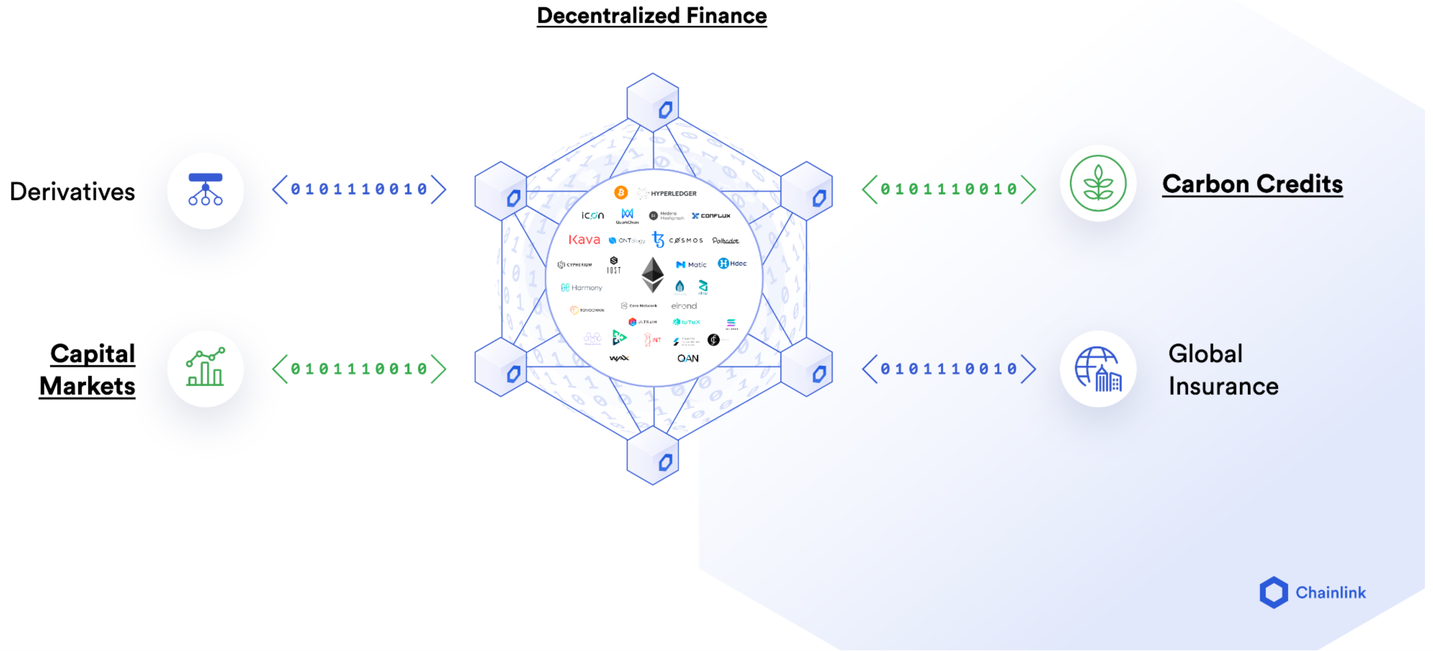
可靠的将数据上链

End-to-end Reliability Is The Promise of Smart Contracts



更多链上
数据与应用

A Global Market for Carbon Sequestration and Reforestation

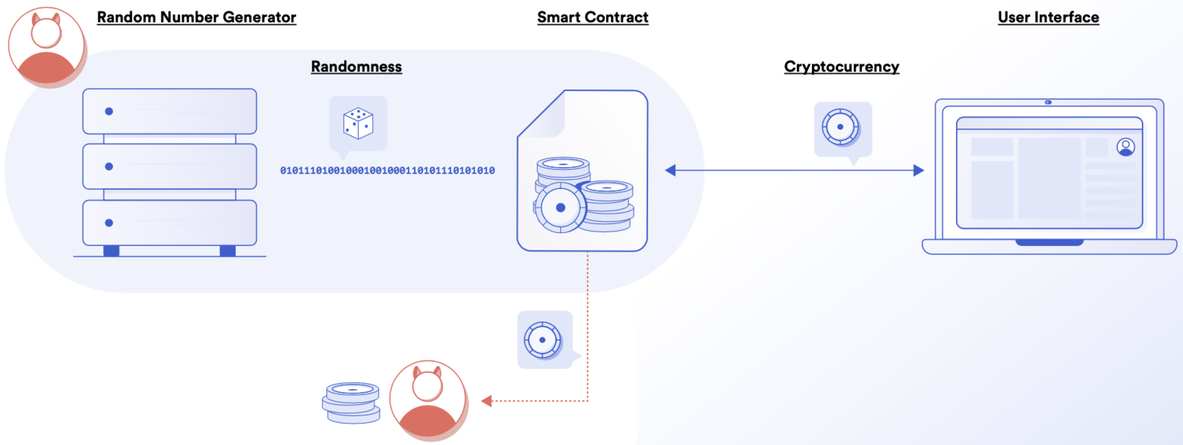


Verifiable Randomness Function

链上可验证随机数

链上产生随机数的弊端

Malicious RNG Operators are a Risk



使用VRF生成

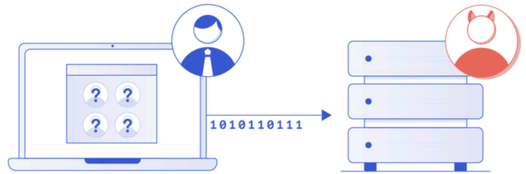
无法被预测
Unpredictability

公平无偏见
Fair/Unbiased

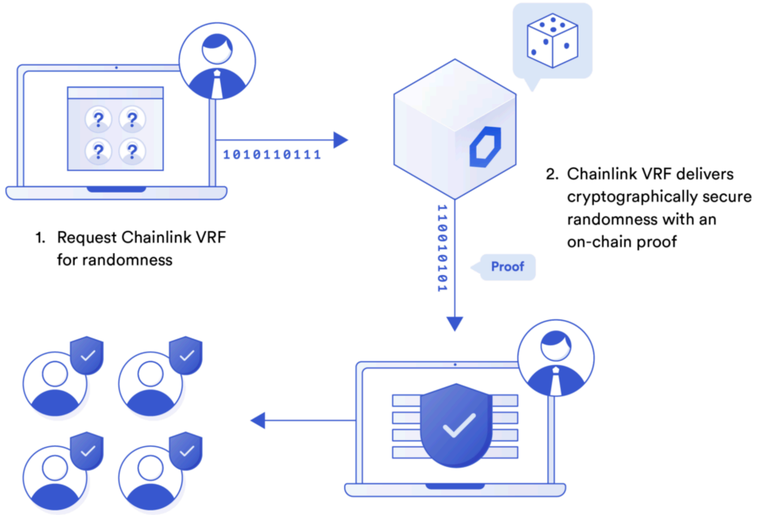
可被验证
Provably Random

防篡改
Tamper Proof

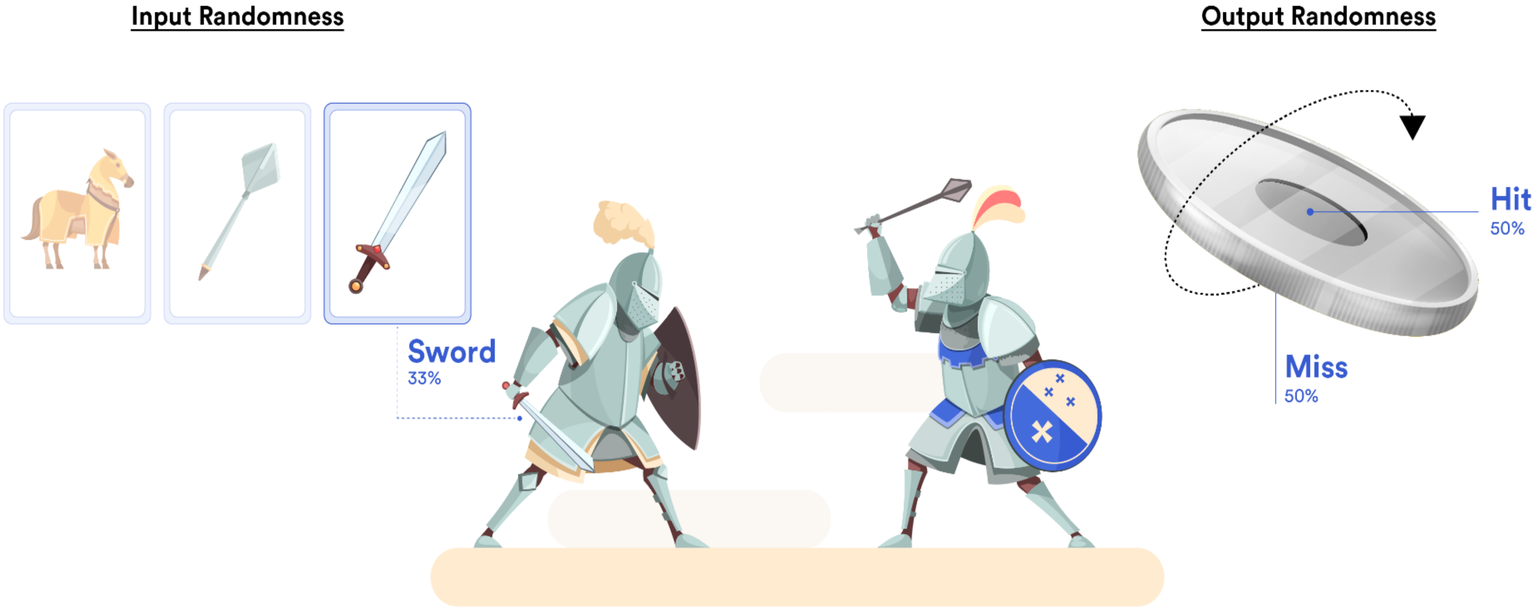
的随机数



Traditional randomness solutions are opaque and can be exploited by malicious actors

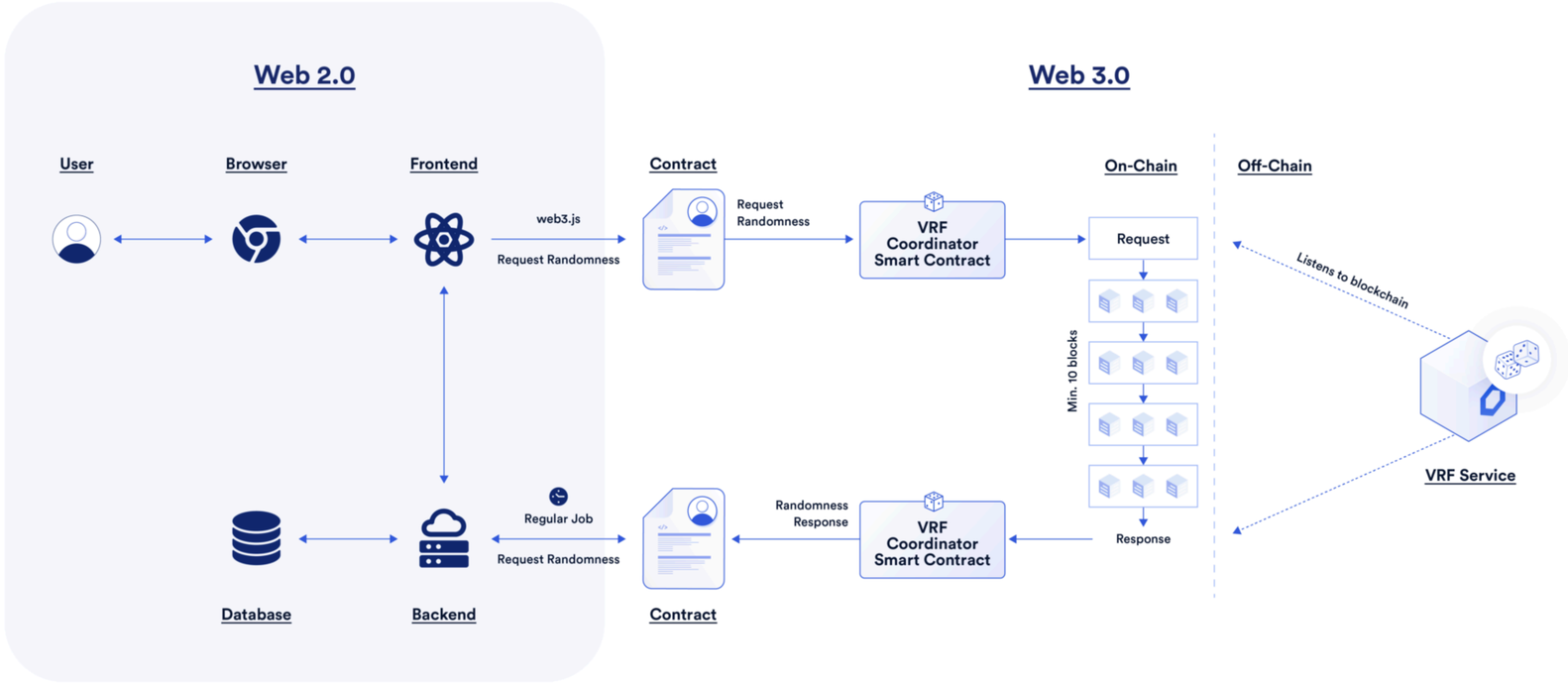


案例 / 场景



Web2架构集成链上VRF

扫码见详细技术架构



具有前瞻性的Web2企业应该抓住机会

VRF | 链下VRF调用的3个典型场景

1 在线游戏

VRF 帮助在游戏等场景中获得可证明的公平结果，如卡牌的随机发放、打斗类游戏中一定几率的命中等都可以非常便捷的集成VRF，以最低的成本保证最大的透明度，使得随机数的产生过程不再是个黑盒子

2 赠送活动

对于随机赠送等随机场景，VRF是您最好的一站式技术解决方案，使用基于区块链的公开透明、不可篡改的随机数生成器（RNG）算法帮助市场营销过程中的随机选取过程公平、没有偏见并且可验证

3 随机抽奖

如果怀疑受到操纵、篡改或不诚实的影响，抽奖等营销活动可能会给公司带来品牌风险。VRF 通过赋予可验证的随机性，从一开始就消除了这些风险，帮助确保参与者被公平选择，从而保护品牌公信力

在线游戏

- 为受到监管的iGaming应用提供可验证的RNG
- 在格斗冒险类游戏中实现不可预测的结果
- 在元宇宙中随机生成玩家出生地和物品放置地点
- 在PvP对战中配对玩家
- 发放宝箱内罕见物品
- 向玩家发牌
- 纯概率类游戏

营销活动

- 免费礼物
- 创新的产品特性
- 选择活动地点
- 游戏化激励

抽奖

- 公平地分发演唱会门票
- 选出中奖者

数据分析

- 公正地甄别欺诈行为
- 为机器学习算法提供熵值足够高的seed

从 Web2.0 到 Web3.0

？ Web5 ？

Web3.0

下一个互联网时代

华尔街见闻 首页 资讯 快讯 行情 日历 APP | VIP会员 大师课

姚前：Web3.0 渐行渐近的新一代互联网

中国财富管理50人论坛 03-18 21:43

378

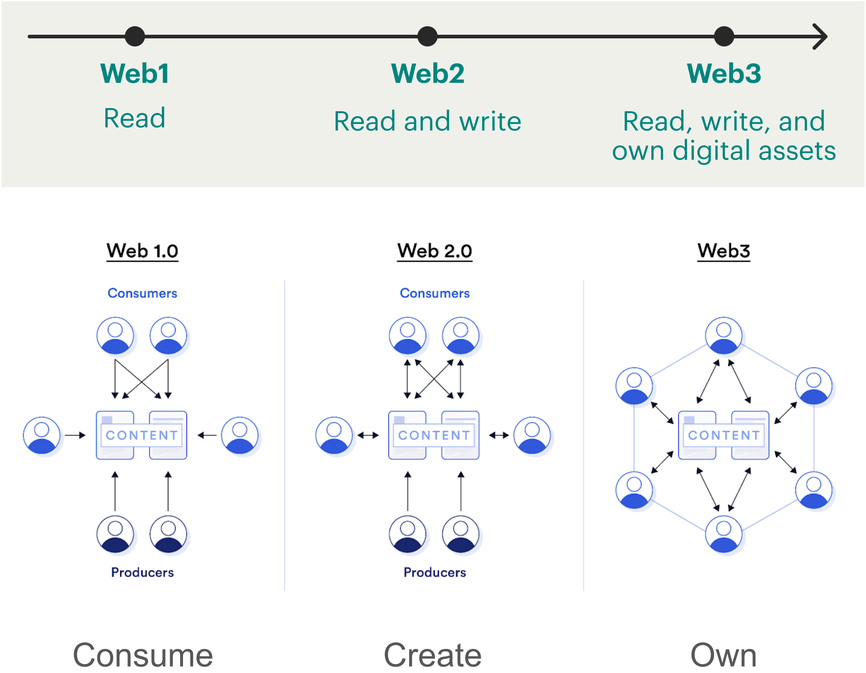
收藏

摘要：

中国证监会科技监管局局长姚前认为，Web3.0有望大幅改进现有的互联网生态系统，有效解决Web2.0时代存在的垄断、隐私保护缺失、算法作恶等问题，使互联网更加开放、普惠和安全，向更高阶发展。

中国证监会科技监管局局长姚前在《中国金融》撰文，结合国内外互联网发展实践和技术演变趋势，分析Web3.0的可能形态并进行相关思考。文章表示，Web3.0有望大幅改进现有的互联网生态系统，有效解决Web2.0时代存在的垄断、隐私保护缺失、算法作恶等问题，使互联网更加开放、普惠和安全，向更高阶的可信互联网、价值互联网、智能互联网、全息互联网创新发展。

Web3.0的建设不仅需要发挥私人部门创新精神，通过大众创新，竞争择优，更需要国家顶层设计以及宽严相济的治理框架给予规范和引导。一是建设高质量的分布式基础设施；二是推动治理良好的技术创新；三是建立通用标准，增进互操作性；四是建立清晰、公平的税收规则；五是建立针对DAO的法律框架。



==想法==

基于Web3技术的创新？idea?

Q&A

wally.yu@smartcontract.com

Web5 is a Decentralized Web Platform that enables developers to leverage Decentralized Identifiers, Verifiable Credentials, and Decentralized Web Nodes to write Decentralized Web Apps, returning ownership and control over identity and data to individuals.

InfoQ 企业会员

企业数字化传播一站式服务

InfoQ 企业会员是为满足企业在中国开发者群体中的品牌曝光需求而推出的一款矩阵化资源包。可为企业提供包括“企业号服务”、“企业动态宣发”、“品牌展示通道”在内的多项专属权益与服务，助力企业高效触达开发者群体，提升数字化时代影响力。

企业号服务

深度触达 300 万中高端开发者

企业动态宣发

新媒体矩阵覆盖百万粉丝

品牌展示通道

线上平台 10 万+ 流量曝光

想一想，我该如何把这些技术应用在工作实践中？

THANKS

主办方：InfoQ