Polkadot 跨链技术演进

孙凯超
Parity 工程师
@kaichaosun

Overview

- Polkadot 技术路线回顾
- XCM
- RFCs
  - Agile Coretime
  - Coreplay
  - Corejam
- Asynchronous Backing

Polkadot 起源

Idea

- Polkadot 的多链愿景
- 2017 年底从 Polkadot 代码库分离出 Substrate

POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK

DRAFT 1

DR. GAVIN WOOD
FOUNDER, ETHEREUM & PARITY
GAVIN@PARITY.IO

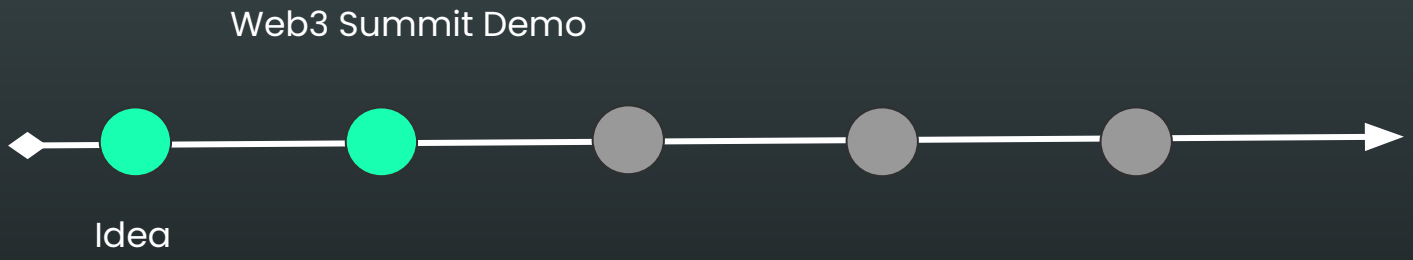
ABSTRACT. Present-day blockchain architectures all suffer from a number of issues not least practical means of extensibility and scalability. We believe this stems from tying two very important parts of the consensus architecture, namely *canonicality* and *validity*, too closely together. This paper introduces an architecture, the *heterogeneous multi-chain*, which fundamentally sets the two apart.

In compartmentalising these two parts, and by keeping the overall functionality provided to an absolute minimum of *security* and *transport*, we introduce practical means of core extensibility in situ. Scalability is addressed through a divide-and-conquer approach to these two functions, scaling out of its bonded core through the incentivisation of untrusted public nodes.

The heterogeneous nature of this architecture enables many highly divergent types of consensus systems interoperating in a trustless, fully decentralised "federation", allowing open and closed networks to have trust-free access to each other.

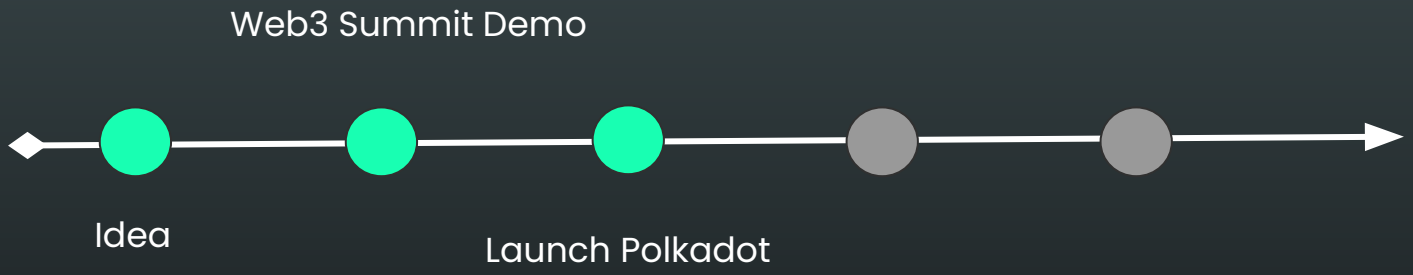
We put forward a means of providing backwards compatibility with one or more pre-existing networks such as Ethereum. We believe that such a system provides a useful base-level component in the overall search for a practically implementable system capable of achieving global-commerce levels of scalability and privacy.

Polkadot 逐步完善



- 2018 年 Web3 Summit 展示 15分钟搭建一条区块链
- Substrate 从此正式成为一个通用的区块链开发框架
- 共识算法 GRANDPA 和 WASM 智能合约研究

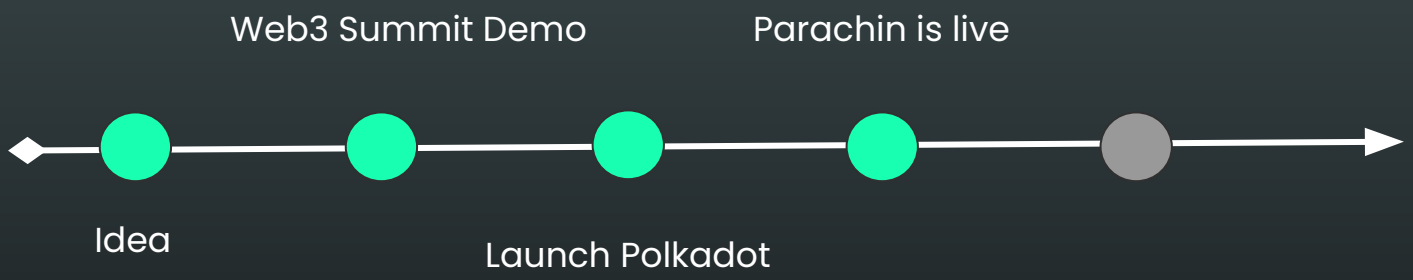
Polkadot Launch



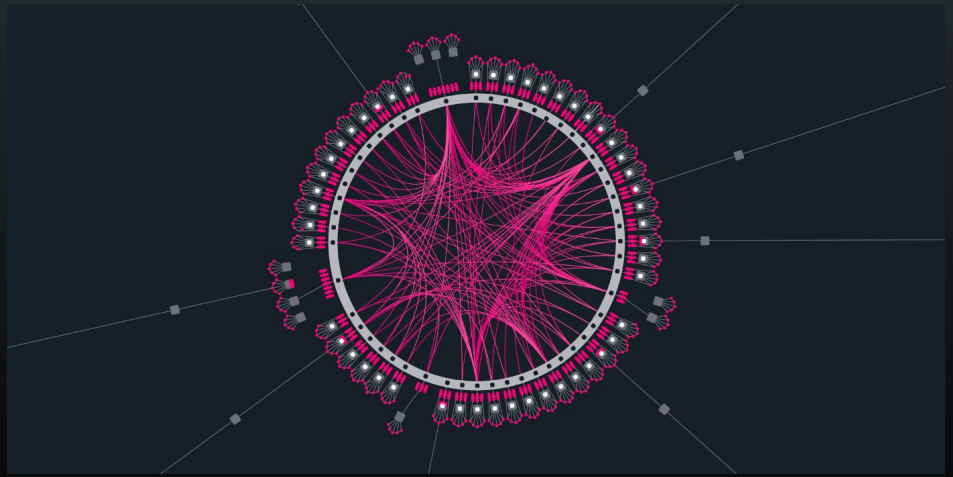
- PoS, Governance, benchmark
- 2019年4月更新至 v1.0 版
- 2019年9月 Kusama CC1 部署
- 发布 Substrate FRAME 模块化架构
- 2020年5月 Polkadot CC1 部署

POLKADOT
IS LIVE.

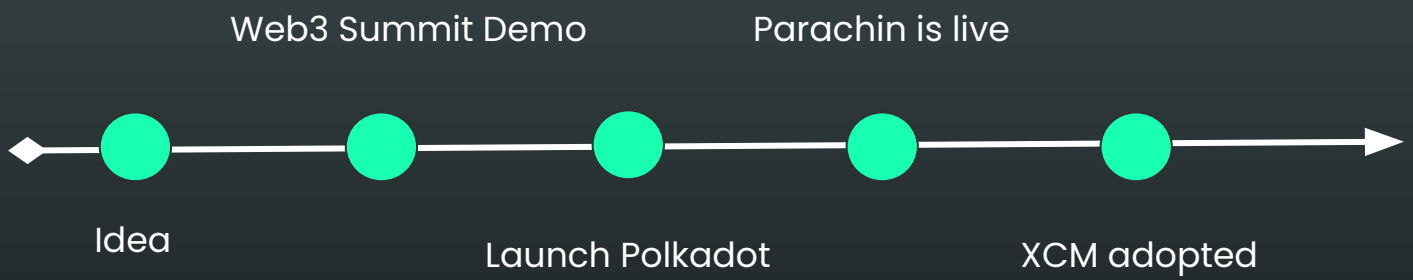
Enter Parachain



- FRAME v2 语法，数据迁移，pallet版本管理
- 2021年6月平行链正式部署在 Kusama 网络
- 2021年12月部署在Polkadot



XCM 升级



- XCM v1 ~ v3 的部署和升级，成为平行链之间通信的主要方式
- 2023年6月部署OpenGov

XCM

- XCM-format (Cross Consensus Message format)，跨链消息格式
  - 标准如 RESTful
  - MultiLocation, MultiAsset, Instruction
  - 共识无关，确保执行，非对称，异步
- 通信层，like TCP
  - VMP (UMP, DMP)
  - XCMP-lite (HRMP)
- XCVM (xcm-executor)，执行指令

https://wiki.polkadot.network/docs/learn/xcm
https://github.com/paritytech/xcm-format

XCM

```
// In this case, we know exactly how much fees we need for each step of the process
let message: Xcm<parachain::RuntimeCall> = Xcm(vec![
    WithdrawAsset((Parent, withdraw_amount).into()), // Fees are paid in the relay's token
    BuyExecution {
        fees: (Parent, fee_in_source).into(),
        weight_limit: WeightLimit::Unlimited,
    },
    InitiateReserveWithdraw {
        assets: All.into(),
        reserve: Parent.into(),
        xcm: Xcm(vec![
            BuyExecution {
                fees: (Here, fee_in_relay).into(),
                weight_limit: WeightLimit::Unlimited,
            },
            DepositReserveAsset {
                assets: All.into(),
                dest: Parachain(2).into(),
                xcm: Xcm(vec![
                    BuyExecution {
                        fees: (Parent, fee_in_destination).into(),
                        weight_limit: WeightLimit::Unlimited,
                    },
                    DepositAsset {
                        assets: All.into(),
                        beneficiary: Junction::AccountId32 {
                            id: ALICE.into(),
                            network: None,
                        }
                        .into(),
                    },
                ]),
            },
        ]),
    },
]);
```

Terms

- RFCs (Request for Comment)，Polkadot相关的技术设计和实现，包括
  - node implementation, cryptography, consensus
  - XCM/XCMP, business, i.e. runtime, system chains
- on-chain，由所有relay chain的验证人去执行
- in-core，由验证人的子集(Validator Group)执行，分配给parachain
- PVF (Parachain Validation Function)，parachain's runtime wasm stored on relay chain
- PoV (Proof of Validity)，parachain blocks with witness data and messages

What's the problem

上线parachain，需要

- 通过auction，需要团队有较强的筹集资金能力
- core长期分配给某一条链，资源得不到优化分配
- 续租core的花费无法预估，缺少确定性

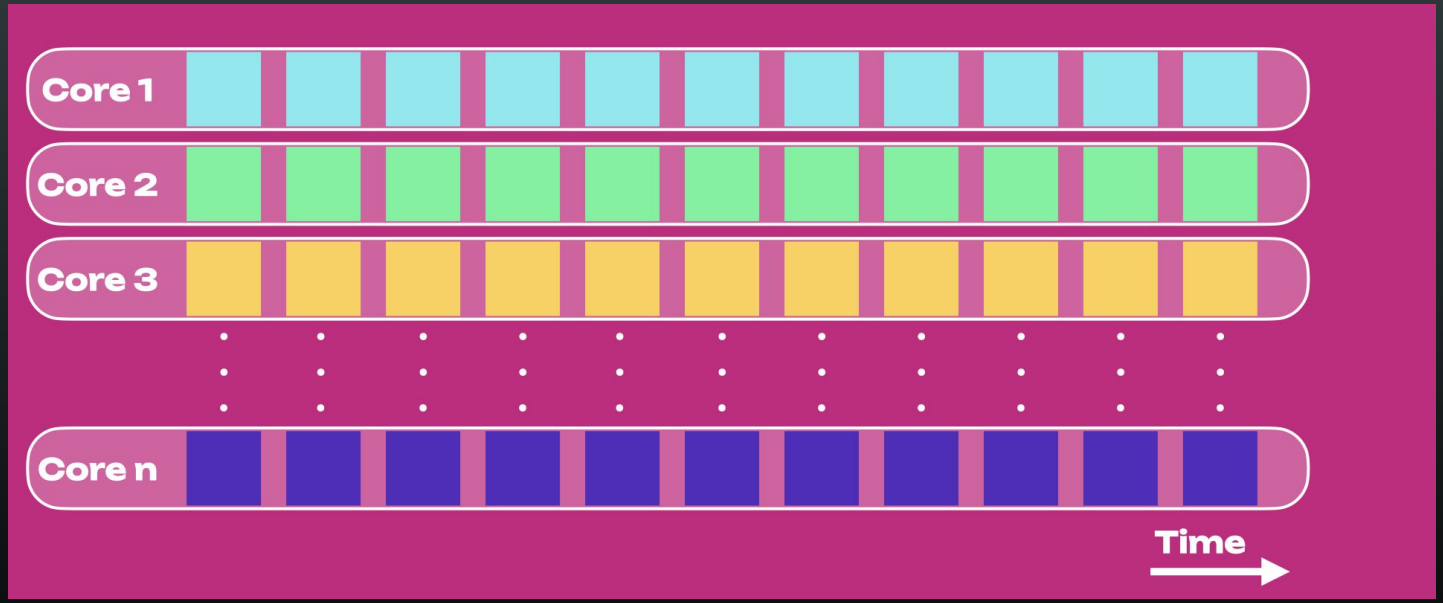
Agile Coretime

灵活的、基于周期性购买的分配 Polkadot coretime的模型 (Agile periodic-sale-based model for assigning coretime of Polkadot)。

- 无需 slot auction
- 销售 coretime 的系统平行链
- coretime 可以以 non-fungible asset 的形式转移、出售，分配给某个任务或者存入即时 coretime pool
- 通过xcm传递消息
  - coretime -> relay, core 应该分配给谁
  - relay -> coretime, core 是否被使用
- 以可预测的价格 renew region（Bulk Coretime）的使用权
- coretime 按需即时付费

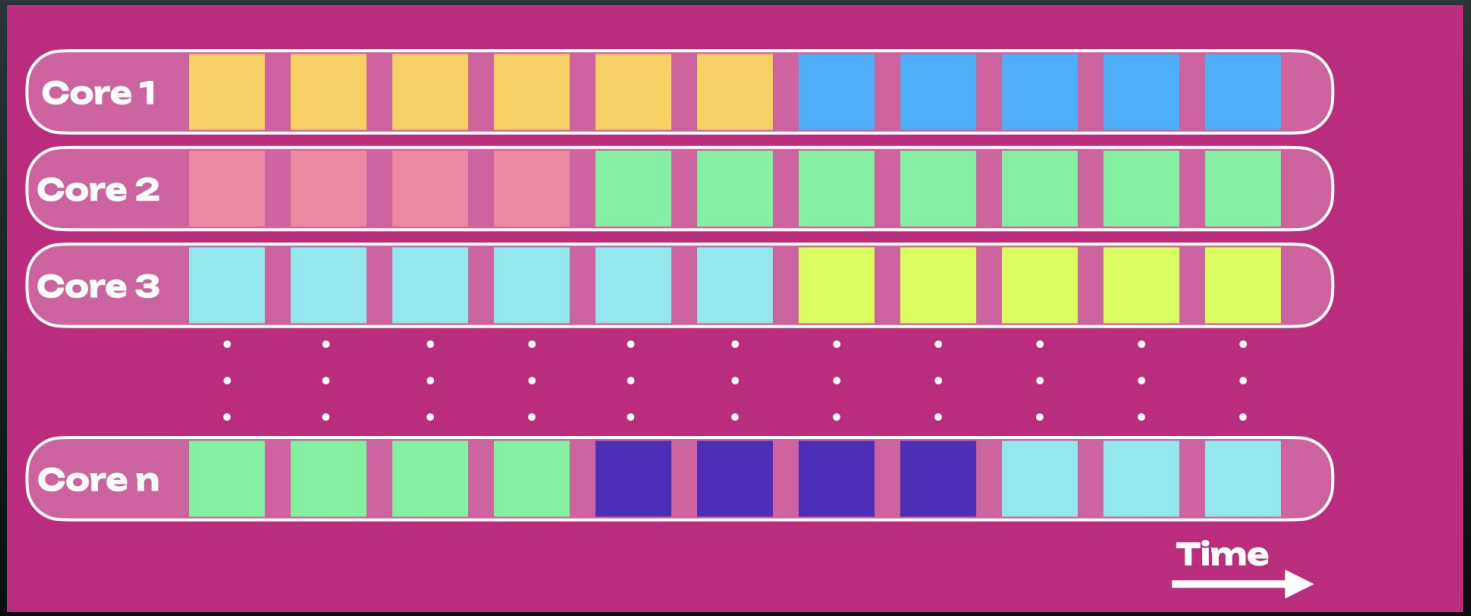
Agile Coretime

Polkadot 1.0对core的使用：



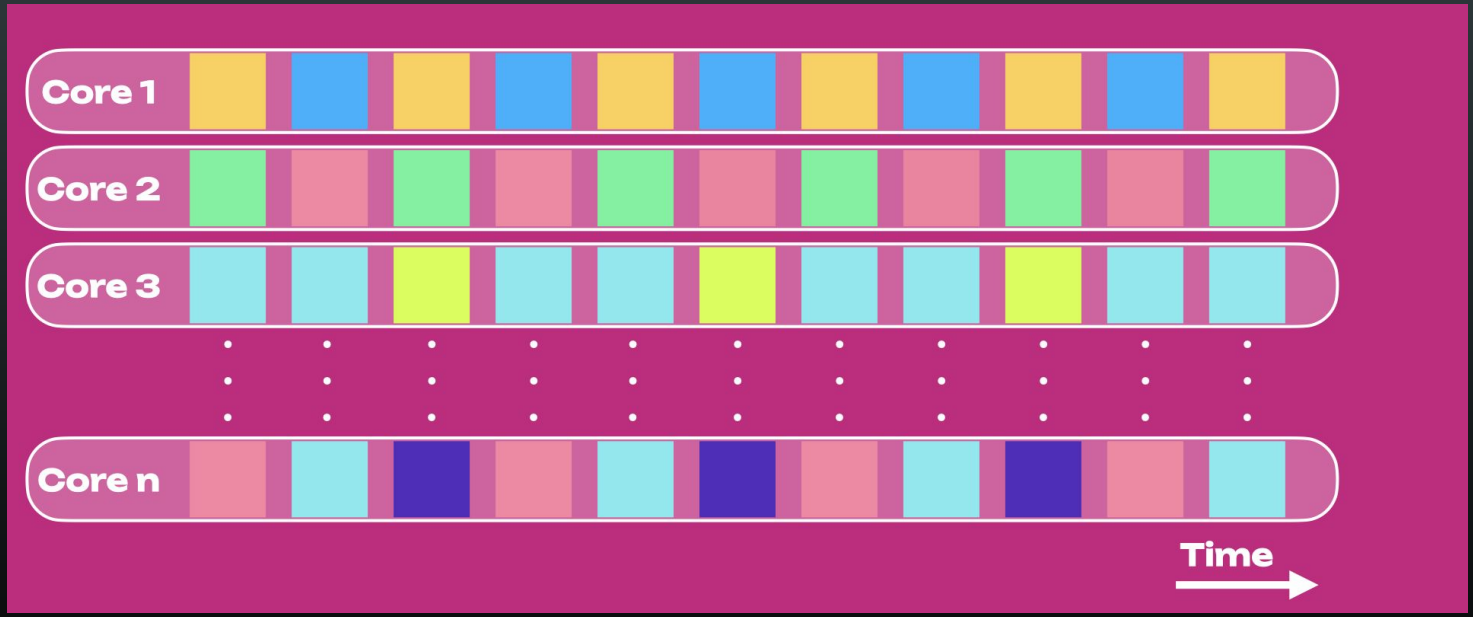
Agile Coretime

Split Coretime, core的使用权可以分割、交易。



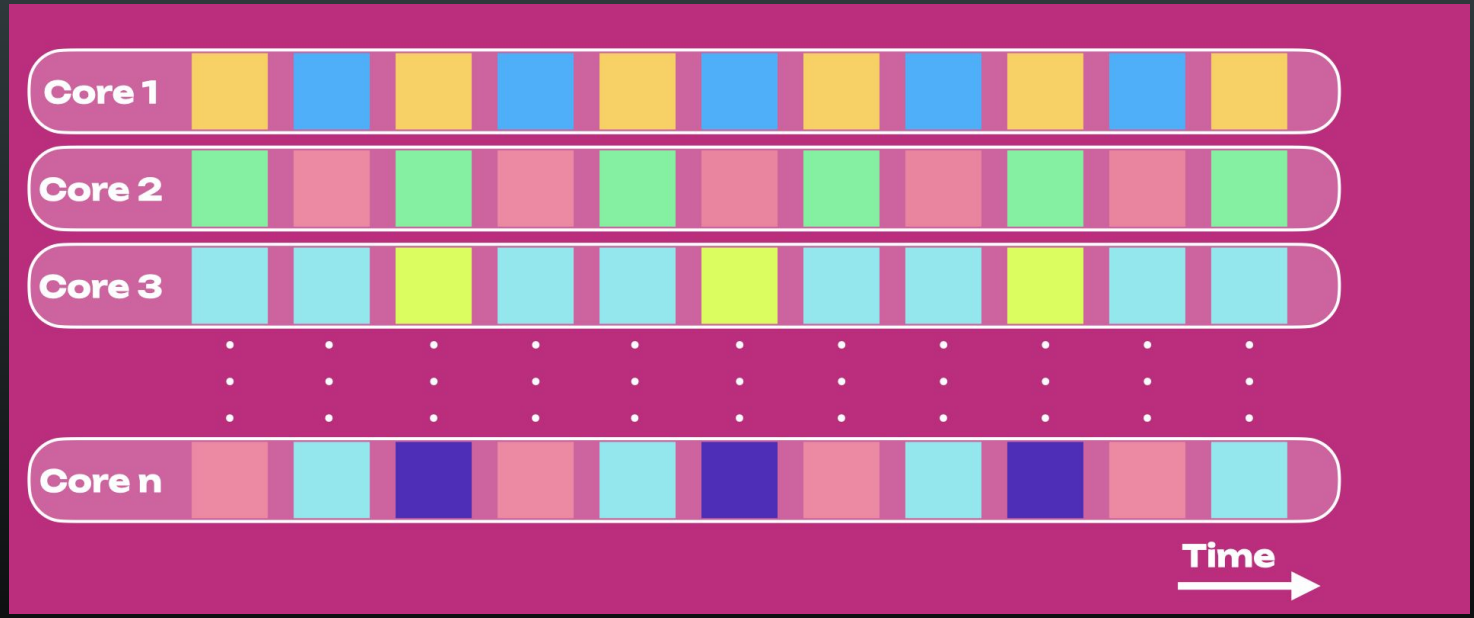
Agile Coretime

Strided Coretime，apps 轮流使用core



Agile Coretime

Combined Coretime，应对峰值 blockspace 的需求。



https://wiki.polkadot.network/docs/polkadot-direction

Agile Coretime

目标，

- Polkadot合理的价值捕获机制
- 生态团队的长期花费可预期
- 降低进入门槛
- 支持 1000 个core，可动态变化
- 促进任务在动态间隔和不同跨度下使用core

Agile Coretime

目标，

- Polkadot合理的价值捕获机制
- 生态团队的长期花费可预期
- 降低进入门槛
- 支持 1000 个core，可动态变化
- 促进任务在动态间隔和不同跨度下使用core

待确定的，

- 初始价格，以及价格变动的算法
- 如何使用销售coretime的revenue，销毁 / treasury
- 可销售core的百分比

Agile Coretime

- Coretime Chain PR:
  - https://github.com/paritytech/polkadot-sdk/pull/1479
- Coretime roadmap:
  - https://github.com/paritytech/roadmap/issues/41
  - https://github.com/paritytech/roadmap/issues/52
  - https://github.com/paritytech/devops/issues/2725
- broker pallet
  - https://github.com/paritytech/substrate/pull/14568

Coreplay

使用 core 执行智能合约（aka Actor），Why，

- 开发者所熟知的开发模式
- 无需单独部署一条链
- 无需过多考虑执行期的资源消耗 (weight)
- 促进core的并行执行
- 适用紧急应用场景

Coreplay

处于idea阶段，

- PolkaVM，基于 RISC-V 的虚拟机，用于执行智能合约
- System disk chains，存储 actor 的临时状态
- 允许actor之间的同步和异步交互

https://github.com/polkadot-fellows/RFCs/blob/gav-coreplay/text/coreplay.md

https://forum.polkadot.network/t/announcing-polkavm-a-new-risc-v-based-vm-for-smart-contracts-and-possibly-more/3811

Corejam

用于并行、去中心状态机的分阶段 收集-提炼-聚合-累加 模型
Parallelised, decentralised, permissionless state-machine based on a multistage Collect-Refine-Join-Accumulate model

- Polkadot之前设计用于长期运行的parachain，随着Agile Coretime和Coreplay的引入，需要更通用模型，满足未来的扩展性要求
- 通用模型的自由度带来
  - 潜在的用户使用场景
  - 降低开发者负担和进入门槛
- 对core的使用策略开放给核心开发之外的社区成员
- 即如何使用 core 资源的通用模型
  - in-core，工作包（Work Package）的传输、生产、计算、验证
  - on-chain，结果的收集、聚合、累加进入relay chain链上状态

Corejam

- Work Package, 包括验证逻辑，一组Work Item，上下文（header hash, root hash, dependencies, etc）
- Work Item, 由一个 Service 和 payload 组成
- Service, 包括代码和链上状态，
  - 和智能合约类似，可以使用链上逻辑修改状态，
    动态测量资源的使用，
    可以持有资产并同步调用其他Service
  - 不同的是，链上的逻辑（Accumulate function）不能直接被外部调用，即它不接收交易；
    所有依赖的输入来源于 Work Item 的计算结果
    相同Service的多个计算结果聚合叠加最终修改链上状态。

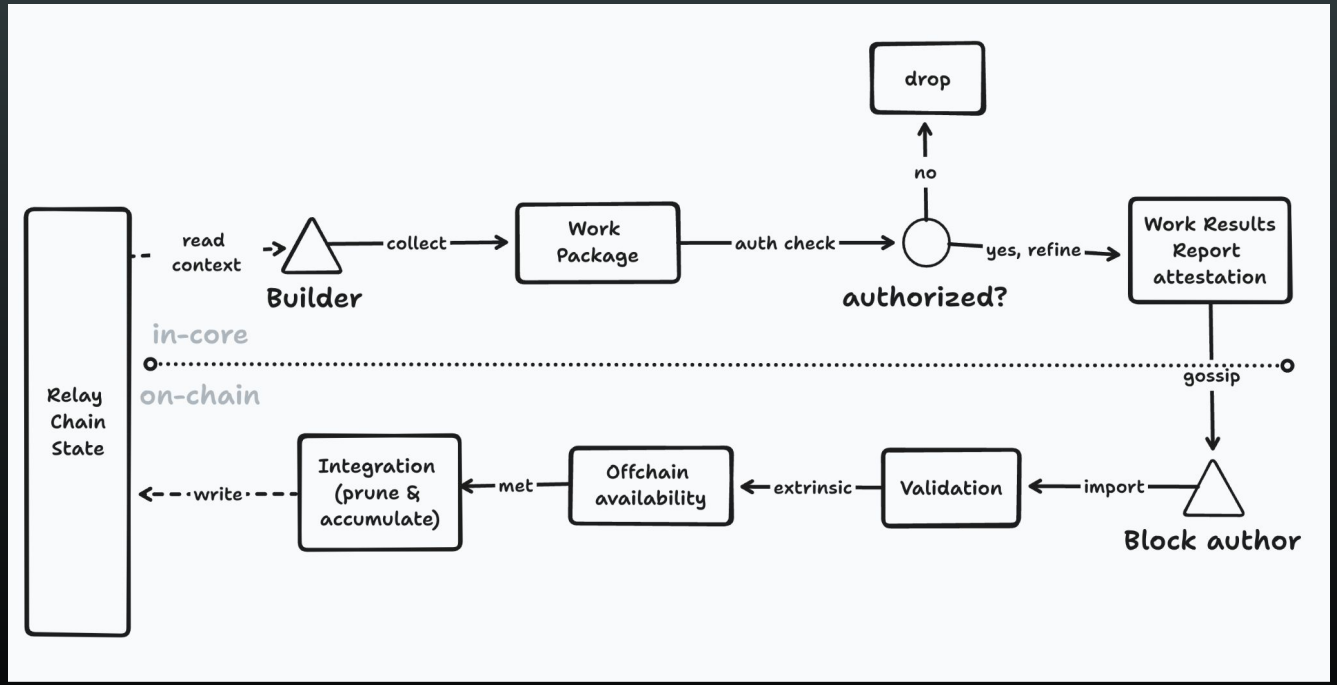
Corejam

- 和之前流程的类比

CoreJam model	Legacy model	Context
Core Chain	Relay-chain	Primary block-chain
Work Package	Proof-of-Validity	Untrusted data provided to RcBG
Work Item	Proof-of-Validity	State-transition inputs and witness
Work Output	Candidate	State-transition consequence
Work Report	Candidate	Target of attestation
(Work Package) Attestation	Attestation	Output signed in attestation
Reporting	Attestation	Placement of Attestation on-chain
Integration	Inclusion	Irreversible transition of state
Builder	Collator	Creator of data worthy of Attestation

Corejam

- Work Package 处理流程



Corejam

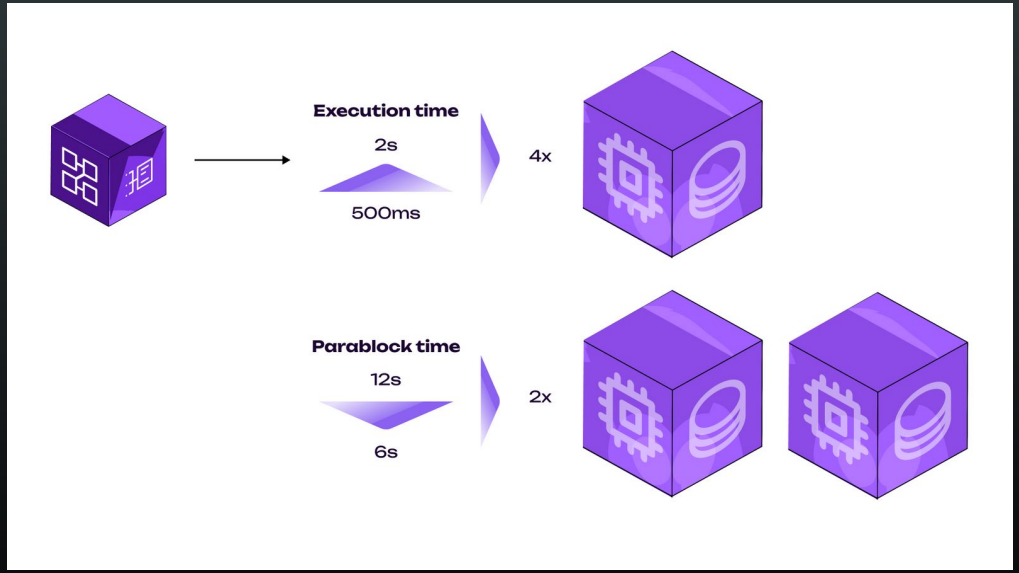
处于讨论阶段，

- https://github.com/polkadot-fellows/RFCs/pull/31

Asynchronous Backing

Parachain 可以不必使用最新的relay block 来构建区块。

https://polkadot.network/blog/elevating-polkadots-performance-and-scale-with-asynchronous-backing



更多功能...

More great features coming...

- 系统平行链 staking, identity, governance
- Sassafras 共识
- 轻客户端 smoldot
- Internode Mixnet
- Social Decentralization
- SPREE
- ……

Thanks.

官网文档：substrate.io
中文文档：subdev.cn

@kaichaosun