

# Plasma

スケーラブルな自律型スマートコントラクト

ジョセフ・プーン joseph@lightning.network  
ヴィタリック・ブテリン vitalik@ethereum.org

2017年8月11日

ワーキングドラフト <https://plasma.io>

## 概要

Plasmaは、世界中の分散型金融アプリケーションのほとんどを扱えるたったひとつのブロックチェーンを可能にする、秒あたりの状態の更新を多くの量（潜在的に十億）までスケールができるスマートコントラクトの強制執行と、インセンティブのために提案されたフレームワークである。これらのスマートコントラクトは、トランザクションの状態遷移を強制する基礎となるブロックチェーン（例：Ethereum）に最終的に依存するネットワークの取引手数料を介して、自律的に動作を継続する動機づけがされている。

私たちは、金融活動だけでなく、中央集権型サーバファームへの代替を提案するであろう、世界的で永続的なデータ・サービスの経済的インセンティブを構築も行う、自律分散的なアプリケーションのための処理の拡張方法を提案する。

Plasmaは、設計の二つの主要部分から構成されています：すべてのブロックチェーンの計算を、MapReduce関数のセットとして、およびナカモトコンセンサスのインセンティブがblock withholding攻撃を阻止することを理解した上で、既存のブロックチェーンの上にPoS(Proof of Stake)トークンを結合するためのオプションの方法として、再構築することである。

この構造は、詐欺の証拠を使用することによって状態遷移を親チェーンで強制することができるスマートコントラクトをメインブロックチェーンに構成することにより、達成される。私たちは、ツリー階層にブロックチェーンを構成し、ブロックチェーンの履歴とマークル証明を約束したMapReduce計算を強制した、個々の独立した分岐ブロックチェーンとして、それぞれを扱う。親チェーンによって執行された子チェーンに、誰かの台帳の取引を作成することで、その人は最小限の信頼（Rootchainの可用性と正確性を仮定する）で、信じられないほどのスケールを実現することができる。

非グローバルデータのグローバルな執行の周りの最大の複雑さは、データの可用

性とBlock withholding攻撃を中心に展開され、データの継続的な正しい実行を動機づけ、強制するメカニズムを作成しながら、障害のあるチェーンからの脱出を可能にすることによって、Plasmaは、この問題の緩和策を持っている。

障害のない状態の間、Rootchain（すなわちEthereum）に、定期的にマール値だけがブロードキャストされているため、これは非常にスケーラブルで、低コストな取引および計算を可能にすることができる。Plasmaは、高いスケールで持続的に動作する、分散型アプリケーションを可能にする。