# EPR-ereum
# bridging different worlds

Benjamin Bollen

July 18, 2017

## Overview

Proof-of-Work mining successfully secures Ethereum, however it does not allow the computational power of Ethereum to scale as more full nodes join the network.

We present an overlay protocol to scale the capacity of decentralised applications on public Ethereum. Our solution manages all value on Ethereum and provides an on-chain marketplace for pooling computational resources of full nodes allowing them to contribute and earn gas rewards linearly from the execution power they provide to Ethereum.

The solution does not modify the scaling properties of Ethereum directly, rather it aims to get more computational *gas mileage* out of the same Ether by minimising the verification burden put on the Proof-of-Work miners. To this end we introduce a Byzantine fault-tolerant, staked meta-consensus mechanism. This mechanism allows us to scale computational capacity with the number of groups of nodes available. By moving the verification burden away from the Proof-of-Work miners we bypass the *verifiers dilemma*[1] while retaining the full replay history of Ethereum.

We detail the protocol and discuss an early analysis of attack vectors. We imagine possible use-cases and review the gains by enabling Eprereum for the application. At the end we place this proposal in relation to existing work on scaling Ethereum.

[1]The verifiers dilemma states that the verification burden for honest miners in Nakamoto consensus systems must be small compared to the sealing effort lest the honest miners be vulnerable to attacks. We will discuss the dilemma in more detail further.

## 1 It's all about gas

In Ethereum gas accounts for every execution step. A transaction includes a *gas price* and a *gas limit*. The gas limit sets the maximum gas that can be burnt during the execution of this transaction. When the execution completes the total gas used is deducted from the account balance of the transaction *sender* at the set gas price[2].

In late spring of 2017 a steep increase in the number of transactions processed on the Ethereum blockchain has been registered. All the while the average gas used per transaction has remained in first approximation constant. The accompanying higher market valuation of Ether had the price per transaction skyrocket. In response the average gas price has started a correction downwards at the time of this writing. [graph]

This demonstrates that the Ethereum protocol has scaled successfully under an increase of the number of transactions. However, it leaves unanswered how Ethereum can scale for more computationally intensive applications. We will argue that it is not only the price that is prohibitive to build applications that consume more gas. It has been highlighted that Nakamoto consensus systems have an inherent requirement to keep the block validation to a mimimum. Consequently this keeps the gas price for transactions validated by the Proof-of-Work miners high,

[2]The gas price is set in Ether per gas [ETH], where gas is a number.

as the total block fee, $f = \sum_{tx} \text{gas} \cdot \text{gasprice}$. From this it is clear that for honest miners security and profitability are optimised with a supply of many low-gas, high-gas price transactions.

The security that Proof-of-Work miners generate is rooted in the adversarial race the miners are in to solve the block sealing puzzle first. Only the miner who contributes the block is awarded the block rewards and block fee. Other miners are expected to validate the correctness of the transactions in a block for the good of the network without reward. They obviously have an incentive to make sure the block does not contain invalid transactions, because that would invalidate all work they build on top of it. Verifying transactions of mined blocks, however, carries the risk of falling behind on mining the new block. This is a brief summary of what has been understood as the verifiers dilemma[3][Teutsch].

If the verifiers dilemma is implied by the Nakamoto consensus and its reward structure, then it can be avoided by examining other incentive structures. The mining paradigm to date forms the foundation of the two biggest public blockchains and as such our objective in this work is not to replace it. Rather we will present an opt-in, overlay protocol that constructs a new scaling dimension for decentralised applications on Ethereum.

# 2 Bridging different worlds

Going forward we define the results of the Proof-of-Work consensus of Ethereum to be true. We note that a Nakamoto consensus engine can rollback state, however, our construction will be local to a block and as such invariant to which branch of the consensus engine eventually accumulates most work.

As an overlay protocol on Ethereum, all Eprereum nodes are constructed to verify the Ethereum blockchain. As a result, we can use smart contracts on Ethereum to construct a deterministic, global[4] one-to-many communication channel without incurring an overhead on the number of Eprereum nodes in the network.

Communication in the other direction, however, is expensive as it requires transactions to be validated by the Proof-of-Work miners at a high gas price.

# 3 Connecting the wires

# 4 Steering network health

[3] see appendix for more details - todo

[4] Note that this global symmetry is only valid under the stated assumption that the Eprereum network is invariant under the probabilistic finalisation of Ethereum. Here without loss of generality we assume that the global symmetry is valid, but this is a requirement for an implementation to observe.