



有效工作量证明（**Proof of Useful Work, PoUW**）是一种用来提升区块链效率与安全性的新型共识协议。经典比特币式挖矿的过程十分耗能，因为它所用的工作量证明（**Proof of Work, PoW**）形如一个抽签机制，底层的计算工作并没有其他用途。矿工们不得不浪费大量能源来添加一个包含交易的新区块到区块链上。作为对比，有效工作量证明除了抽签机制之外还有在区块链上训练一个机器学习模型的功能。

用户可以以不同的身份参与到工作量证明的系统中：客户向网络提交机器学习训练任务；矿工在诚实地进行一定量的机器学习训练工作之后可以得到一次铸造新虚拟货币的机会；协调员协调并监管训练工作的进行。他们的活动不仅保证了区块链的运行，也帮助解决了真实存在的问题：训练机器学习模型。同时客户的隐私也得到了保护，因为他的机器学习任务由分布式网络计算，而不是由一个中心化的机构管理。我们致力于利用区块链的安全性创建更好的人工智能系统。

在本文中，我们简单比较了其他有效工作量证明方案并且列出了本方案的诸多特征。在我们的系统中，用于区块链挖矿计算的 **nonce** 变量是通过机器学习训练的输入和中间变量计算而来的。我们实现了一个概念验证级产品，证明了对于客户来说，我们的方案比普通机器学习云计算方案更节省，对于比特币矿工来说，我们的方案收益更高。我们的方案同时也证明了在个人消费级硬件上合作训练机器学习模型可以达到不错的效果。

图:

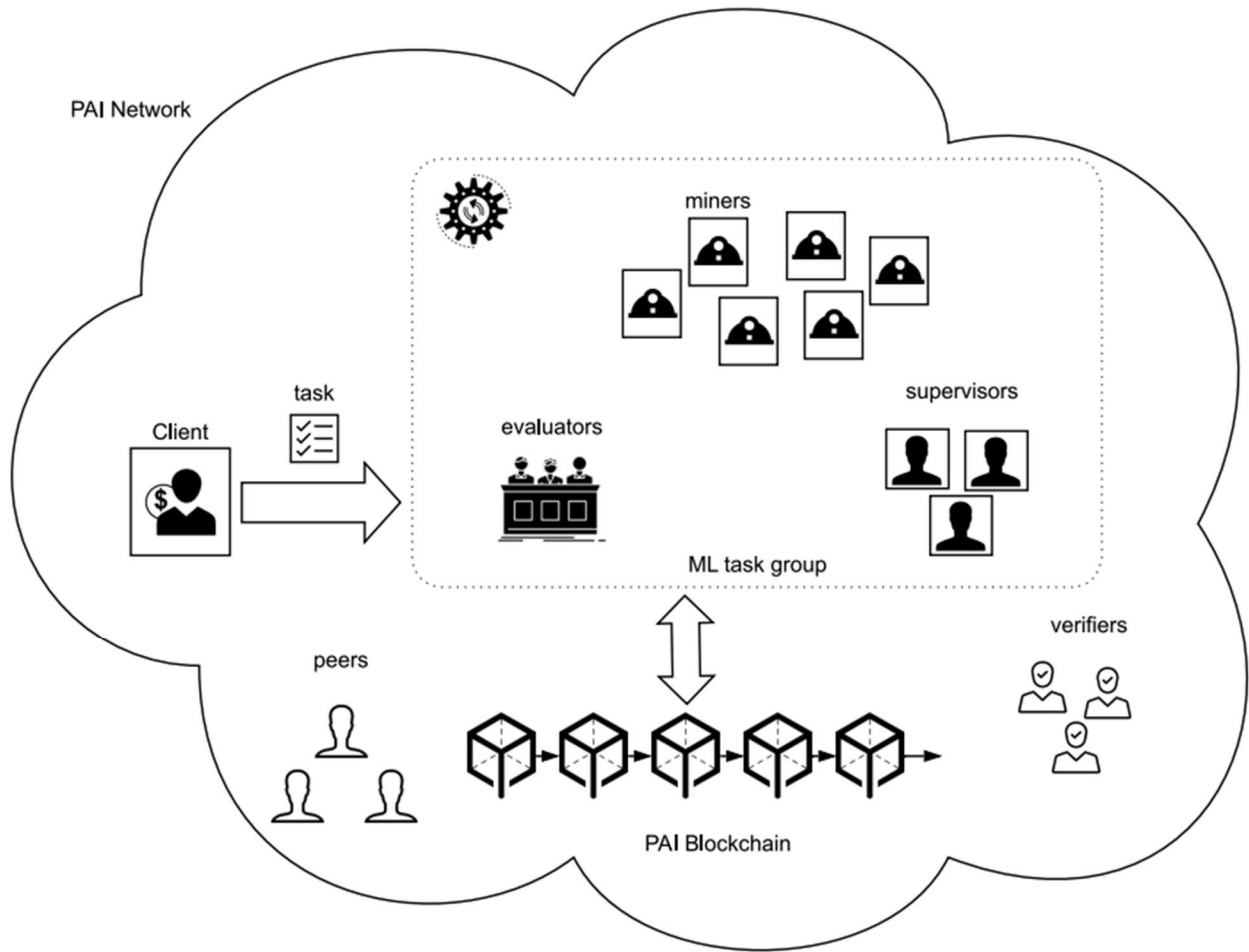


Figure 1. System architecture

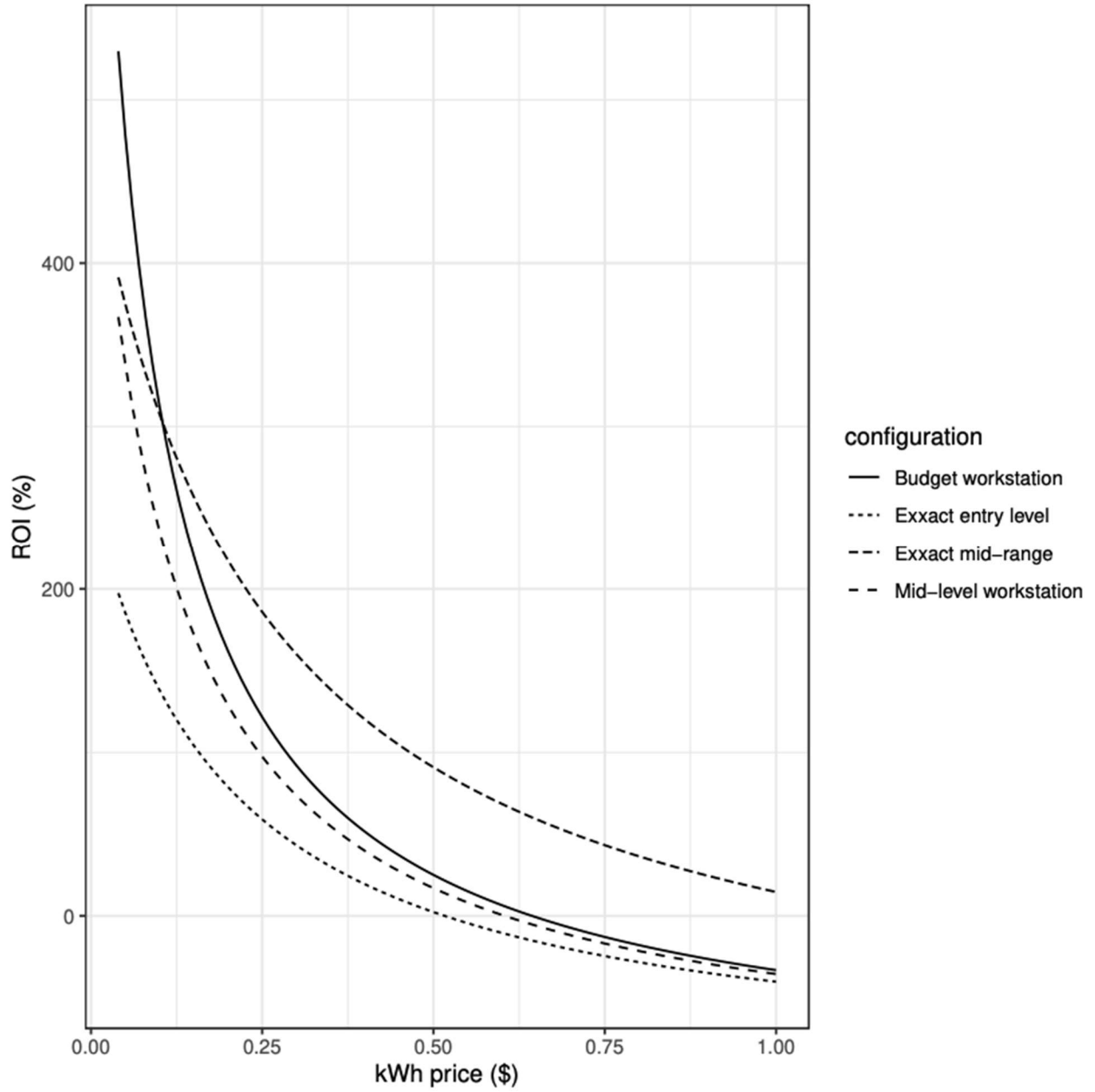


Figure 2. ROI (%) as a function of electricity price.