## 1 Summary

Four years after the Bitcoin white paper, Vitalik Buterin, a Russian-Canadian crypto-enthusiast, and a few others developed the Ethereum platform to broaden the scope of blockchain-based applications beyond just cryptocurrency. Ethereum provides developers with a blockchain platform upon which they can build and deploy *decentralized* applications. A built-in Turing-complete programming language enables the composition of *smart contracts* through just a few lines then executed within the Ethereum Virtual Machine (EVM).

## 2 Strengths of the paper

So many cool things about this paper, but here are just 2:

1. Although blockchain predates Bitcoin, one can argue that Satoshi Nakomoto deserves credit for reintroducing the technology into popular culture. At the same time, Buterin deserves applause for realizing the vision held by the blockchain inventors at a time when all the hype was around cryptocurrency, namely Bitcoin. This approach highlights the fundamental difference between Bitcoin and Ethereum: the incentive and ideas behind Bitcoin led to it being used as a store of value, whereas Buterin and his peers' design rendered Ethereum a platform through which to enforce *smart contracts*.
2. It is evident that Butelik is a pragmatist. He admits that the CLI (command line interface), i.e., the transaction sending mechanism, likely being met with demur by the majority of 'business people' limits decentralization from mainstream adoption. However, this can be alleviated through well-designed GUI (graphical user interface) components or another interface to ease communication between the EVM (Ethereum Virtual Machine) and a 'business person'.

## 3 Weakness of the paper

Though this is not a true academic paper, it remains one of my all-time favorites simply because of the balance between the novel ideas introduced and how, as a result of Buterin's writing, approachable the paper still is. For the sake of pointing something out, maybe Buterin could have used a (fictional) scenario to relate back to the technical ideas to maintain cohesion between them and also, relate their use to the same, albeit fictional, scenario.

## 4 Future work opportunities

I wonder whether someone has already explored combining proof-carrying code (PCC) with Ethereum to, say, prove the adherence of a random query, $Q_r$, to a set of pre-defined safety rules, $S$, prior to letting it be applied to some data stored within an underlying blockchain.