**Starcash Nukeproofs**: A non-interactive zero-knowledge implementation of Bulletproofs on top of Starcash unforkable realtime blockchain federation for powering infinitely-scalable general-purpose secure MPC applications e.g. a non-clonable blockchain software design, engineering and distribution system and an automated discovery and reply-back engine for collaborative cyber-physical systems comprising of tokenized hardware, sensors, actuators, 3D printers, autonomous systems and cobots.

**Ren Timer**
Orch Network
Email: ren.timer@orch.network

We hereby describe Nukeproofs, an implementation of Bulletproofs[BP], a non-interactive zero-knowledge proof protocol with very short proofs and without a trusted setup to enable secure multiparty-computation(MPC) on top of Starcash unforkable realtime blockchain of Orch Network. Besides enabling MPC it would secure p2p decentralized design, engineering, testing and distribution of non-clonable orchized software applications and components as well as an instantaneous reply-back search engine for distributed cyber-physical systems such as mobile and industrial cobots, IoT sensors & actuators, autonomous machines/platforms and tokenized hardware.

We call this efficient and fast zero-knowledge layer Nukeproofs. And non-clonable software applications and components as nukeproof software apps and components.

## Introduction

Orch team busy implementing Starcash earlier made an attempt to incorporate ZKSTARK as its zero-knowledge layer without a trusted setup. But we were stuck with the size of proofs and computational inefficiency of ZKSTARK soon. Then few months ago Benedick Bunz et al released their work on efficient zero-knowledge proof systems Bulletproofs. After realizing it s the best replacement for ZKSTARK we have quickly decided to implement it for Starcash.

The efficiency of Bulletproofs is stunning in comparison to there ZK systems. A Bulletproof for knowing a 384-bit Pedersen hash preimage is about 1 KB and takes 61 ms to verify. The marginal cost of verifying an additional proof is 2.1 ms. The SHA256 preimage proof is 1.4 KB and takes 750 ms to verify. The marginal cost of verifying additional proofs is 41.5 ms. The proving and
verification time grow linearly. The batch verification first grows logarithmically and then linearly. For small circuits the logarithmic number of exponentiations dominate the cost while for larger
circuits the linear scalar operations do.

## Technology

An important assumption is Proofs=Programs. This non-trivial result is the Curry-Howard isomorphism. But unlike Tauchain, we can implement Turing-completeness in Nukeproofs due to bounded nature of NIZK proofs and presence of Star Power, a form of gas price similar to Ethereum Gas to pay for on-chain computing any complex smart contract or code or a program.

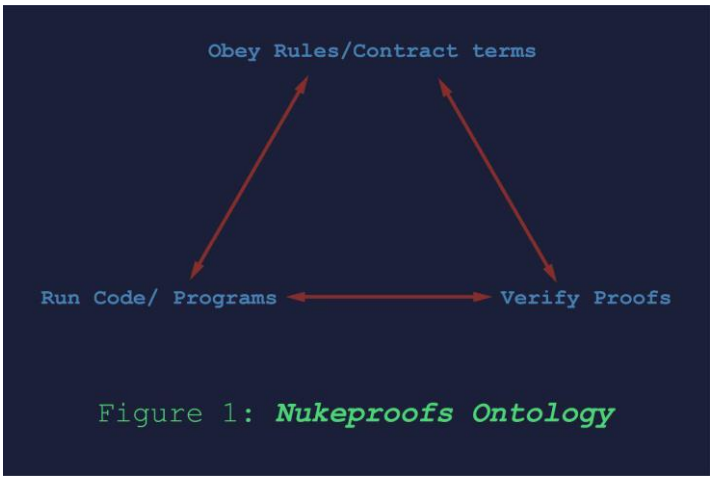


Figure 1: ***Nukeproofs Ontology***

Proof-Program equivalence aka Curry-Howard isomorphism is implemented in all functional programming languages e.g. Haskell. Then we extend it to computational Tinitarianism known as Curry-Howard-Lambek isomorphism by establishing one-to-one correspondence between proofs/programs with Category theory, modern foundation of mathematics(older was Set-theoretic). The software requirements specifications(SRS) of Orchized blockchain software and software components will be written in a Category theoretic Petrinets and its algebraic symmetry [SPN].

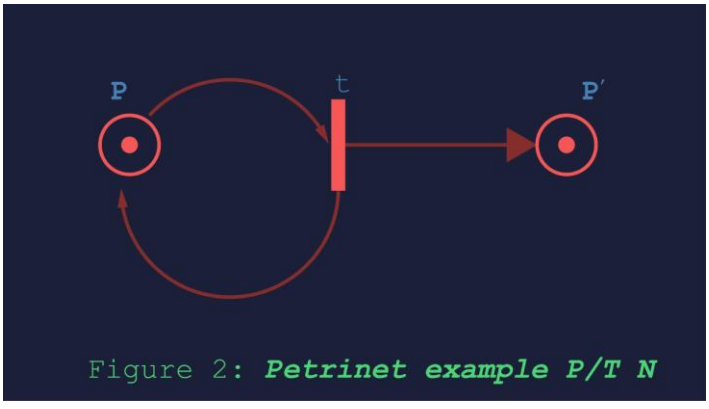


Figure 2: ***Petrinet example P/T N***

## Applications

Here is a practical use case of a group of freelance developers or a small software company Team09 teamed up to deliver a software project prosted by a bonafide corporation Client Corp88 on Orch DevFac peer-to-peer software design, engineering and distribution platform.

Corp88 posted the SRS of the software it wants to get delivered within a predetermined deadline in Nukeproofs category theoretic Pretrinets codenamed CatModels. And they have transferred USD550K toward the commitment deposit to DevFac as per the Standard Contract Terms(SCT). Now Team09 bids for the contract and takes it up. They commit to deliver the debugged software along with source code and runtime execution trace of its test runs within 100 days(deadline).

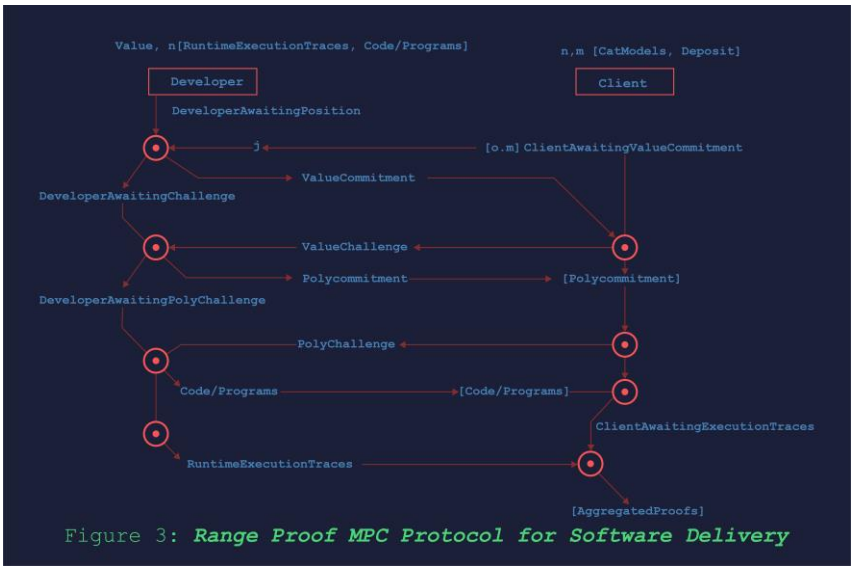

Figure 3: ***Range Proof MPC Protocol for Software Delivery***

Now on or before 100th day, Team09 safely and securely delivers the software, code and its runtime execution trace logs and its test runs of Starcash Blockchain Virtual Machine(BVM). And Corp88 securely transferred funds via locked-deposit to Team09 without exposing themselves(either party) to any undue mutual counterparty risks of non-payments, bankruptcies, unfixed bugs, hidden malicious code and outright frauds.

**Nukeproofs guarantees not only complete anonymity of all parties and confidentiality of all transactions, but also that of all data, source code, binary/runtime code and voice/audio/video stored and processed on Orch Network and Orch-powered platforms, dapps/apps and software components. Nukeproofs in conjunction with BlakeB SHA512 will guarantee freedom to one and all.**

## References

[BP]  Bulletproofs:  Short Proofs for Confidential Transactions and More
Benedikt Bunz,Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille and Greg Maxwell

Stanford University
University College London
Blockstream

[SPN] About Tauchain, Ohad Asor

[OYP] Orch Yellow Paper URL: https://orch.network/static/docs/starcash.pdf