Casper Association

R&D Overview

June 23

INTRODUCTION

Introduction

Blockchain technology continues to evolve rapidly. Smart capital places a premium upon establishing R&D teams capable of feeding actionable research to upstream engineering for the benefit of the wider ecosystem.

Active and ongoing research is required to deliver features such as scaling, interoperability, advanced cryptography, distributed storage, selective privacy, verifiable compute.

R&D within a resource constrained environment (as compared to other networks) is a challenge. Fortunately synthesising existing and emerging research is highly cost effective - no need to reinvent wheels.

A synthesis driven approach will require building trusted relationships in the open source research space. This requires visibility in the right circles, acknowledging the work of others, and exhibiting diplomacy & tact.

THEMES

Themes

The set of possible research themes is extensive. It is important to focus upon an impactful subset and to achieve timely ‘wins’.

A win is defined as that which enlarges the design space available to an integration architect tasked with building a Casper enabled solution.

A foundational theme will be applications of zero knowledge cryptography (e.g. scaling). Porting ACTUS to a ZK-VM is a focalising theme.

- Advanced Cryptography
  - ZK, FHE, MPC
  - Quantum Resilience
- Virtual Machines
  - General vs Special Purpose
  - EVM | WASM | ZK | Other
- Interoperability + Scaling
  - Bridges + ZK-RollUps
  - Wallets -> beyond bip32
- ACTUS
  - Contract lifecycle -> VM
  - Risk Modelling

ZK Cryptography

A tsunami of ZK cryptography is in the process of washing over the blockchain space. pertinent use cases include scaling, identity, VMs.

Blockchains will evolve into cryptographic verification engines. On-chain compute will increasingly move to ZK enabled environments at the edge.

RECOMMENDATIONS

- **Establish zero knowledge cryptography expertise**
- **Sponsor and support ZK community**
- **Build L2 ZK-rollup scaling environment for mass NFT mints**
- **Integrate a 3rd party zero knowledge machine, e.g. Miden VM**
- **Explore collaborations with synergistic ZK projects**

Quantum Resilience

Quantum computing is a rapidly evolving domain space. R&D activity is intense and extremely well funded by state & non-state actors. Hardware platforms & software paradigms are emerging in the research space.

Production grade systems are expected to come on stream by 2030. Whilst such systems directly threaten the cryptographic primitives underpinning today's blockchain platforms, they also act as incubators of innovation.

For example, banks (e.g. JP Morgan) are prototyping blockchain networks whereby nodes are run within specially designed TEE's in which entropy is derived from a Quantum Random Number Generators (QRNG).

RECOMMENDATIONS:

- Establish quantum cryptography academic links
- Commission a quantum resistant cryptography report
- Explore design of a QRNG beacon

Virtual Machines

There are multiple general purpose VM backends targeting blockchain environments, EVM & WASM are currently the dominant backends. There also exist special purpose VM's targeting specific use cases.

Associated smart contract paradigms typically revolve around either a low level API (e.g. Casper) or a higher order domain specific language (e.g. ink! | ask!). Typically a DSL is syntactic sugar over the low-level API.

Production grade ZK VMs exist and more are coming. E.G. by end of Q1 of next year Polygon's zk-stark based Miden VM will be onstream.

RECOMMENDATIONS

- Explore porting ink! & ask! to Casper R&D Overview
- Explore integrating an EVM
- Review ZK VM landscape
- Prototype a ZK VM running within a ZK rollup

Interoperability

Interoperability allows different self-sovereign blockchain protocols to actively communicate with each other, i.e. to interact and share data.

Various interoperability modalities exist. Some are eco-system specific, e.g. Polkadot's XCM. Others are asset specific, e.g. wBTC.

A common design pattern is that of the bridge. They are risk-laden as evidenced by numerous high profile hacks. Existing bridge solution providers with successful track records should be integration targets.

RECOMMENDATIONS

- Review bridge landscape, sort by TVL, security, impact ..etc.
- Issue integration bounties to top 5 bridges
- Offer to bootstrap bridge liquidity
- Partner with DeFi entities seeking CSPR yield

Scaling

An L1 network is by definition resource constrained in respect of execution, storage & consensus. Optimisation can scale an L1 to it's practical limit.

Beyond such a limit one must resort to other scaling techniques. Such techniques scale the system either vertically or horizontally.

Execution can be sharded via L2 ZK-Rollups. Storage can be pruned and historical state served by edge nodes. Validator sets can be grouped into sub-committees. Known techniques exist awaiting implementation.

Mass NFT minting events are happening with increased frequency. Scaling is necessary to support this important use case.

RECOMMENDATIONS

- Implement L2 as a ZK rollup with proofs posted to L1
- Explore integrating an EVM
- Review ZK VM landscape

ACTUS Standard

Adoption of new global financial standards is a multi-decadal process. The ACTUS standard is now in it's second decade and momentum is increasing.

It standardises a wide array of financial contracts at both the informational and algorithmic levels. However the standard is only partially defined and implementations are thin on the ground. More work needs to be done.

Establishing verifiable trust, issuing tokenised securities, & servicing payment channels are blockchain native features. But successfully porting ACTUS to a blockchain enabled environment remains an open problem.

RECOMMENDATIONS

- Support ACTUS Foundation (in progress)
- Develop multiple standalone implementations (in progress)
- Implement within a smart contract environment (in progress)
- Explore running ACTUS algorithms in a special purpose ZK-VM

OUTREACH

Considerations

Outreach in an R&D setting is predicated upon navigating the interface between academia & the private sector. This requires a tactful approach.

Channels include workshops, conferences, papers, articles, podcasts. It is absolutely essential that the R&D team's profile is visible & respected.

Tactical and/or strategic collaborations with external teams are highly encouraged. Care is taken to nurture long term relationships.

Grant programs are the bedrock of most R&D programs. Due to resource constraints, grants are tightly scoped & incremental in size.

Channels

- Collaborations
  - University of Cambridge -> ACTUS
  - University of Kent -> Quantum Cryptography
  - University of Zurich -> Macro crypto-economic analysis
  - University of Luzern -> Secure Multi-Party Computation
  - + 1 in APAC -> ???
  - +1 in USA -> ???
- Sponsorships
  - High Impact Conferences
    - FC2022, FC2023, ZkProof, RWC2023, Crypto 2023
  - Workshops & Hackathons (special purpose)
- Grants
  - Research Fellowships & Post-Docs
  - Independents & teams

Grants

- Mechanism for nurturing fruitful relationships in various environments
- Research fellowships, post-docs, independents, teams
- Short, medium or long term in respect of ‘ROI’
- Focus may be hard (technology) or soft (ideas/relationships)
- Highly effective for focussing work upon a certain subject, e.g. ZK proof verification upon Casper.
- Due to resource constraints, grants are tightly scoped & incremental.
- Failure to issue any grants so far due to logistical issues

Case Studies

Case Study #1: as a result of sponsoring a post-doc at the University of Kent's Quantum Cryptography department, an invitation was received to attend a high impact event at the University of Cambridge. At this event cutting edge research was revealed in the field of quantum money.

Case Study #2: as a result of attending a high impact conference, an informal agreement was made to evaluate a ZK circuit specification language being developed by a private sector entity. This work has led onto evaluating a VM leveraging the aforementioned specification language.

Case Study #3: as a result of attending a high impact conference, a well written research paper on parallel execution was evaluated. In return, input was given in a joint review of state compression techniques.

TEAM

Considerations

Building a team in a resource constrained environment is a challenge. The challenge is heightened by the fact that funding R&D teams is expensive.

Costs are optimised by offering task orientated fixed duration contracts, e.g. 6 months to work upon a ZK Rollup, as opposed to open ended employee contracts. Senior team members would ideally be employees.

Regardless of contract type, team members are paid in FIAT. However CSPR bonuses form part of all packages. Bonuses are linked to quality of work & impact upon the the platform at the technological level.

Team members should be comfortable in public speaking environments. It is essential that the team is visible across the wider research community.

Amplifying team synergies is key to it's cohesiveness and effectiveness. Upstream impact requires harnessing the team's collective skillset.

Composition I

- Head
- Assistant
- Principal Scientist
- Applied Cryptographer
- VM Designer
- Penetration Tester
- Engineer x 4
- Intern x 2

Composition II

- Head
- Applied Cryptographer
- Engineer x 3
- Intern x 2

Material Expenses

- Hardware
  - R&D Machines
  - SRE Infrastructure
- Outreach
  - Attendance @ conferences & workshops
  - Co-working spaces - e.g. Silicon Valley & Singapore
- Subscriptions
  - e.g. Messari et al

BUDGET

Budget

Compact teams operating in low noise environments with a tight set of doable objectives can be highly cost effective. Overlaying a smart outreach program can amplify the team's impact - i.e. punch above it's weight.

Scaling into a reasonable budget is a sensible approach. A few strategic key hires will swiftly result in improved visibility and deeper network. Some early wins in terms of delivery will justify further and continued spending.

Remarks

The upper estimation of a yearly budget towards establishing an impactful R&D team was 2.98m CHF. The actual 2023 budget was 1.28m CHF.

A reduced budget results in a diminished impact. Scaling stretches costs over a longer timeframe, e.g. 18 or 24 months. Whilst some entities may accept CSPR, most will require FIAT.

For further information see spreadsheet (R&D tab).

Casper Association

R&D Overview

June 23