EOS Network Foundation

On behalf of the EOSIO+ Coalition

Faster Finality

INTENT TO BID ON THIS REQUEST FOR PROPOSAL ARE

DUE BY OR BEFORE

30 MAY 2022

1.0 RFP GENERAL INFORMATION **3**
1.1 CONFIDENTIALITY 3
1.2 RFP DOCUMENTS 3
1.3 RESERVATIONS FOR AWARD AND REJECTION OF PROPOSALS 4
1.4 FORMAT REQUIRED FOR RFP RESPONSES 4

2.0 INTRODUCTION **5**
2.1 FOUNDATION OVERVIEW 5
2.2 REQUEST FOR PROPOSAL QUESTIONS 5
2.3 RFP SCHEDULE 5

3.0 PROJECT INFORMATION **6**
3.1 GLOSSARY 6
3.2 PROJECT SCOPE 6
3.2.1 BUSINESS REQUIREMENTS 6
3.2.2 TECHNICAL REQUIREMENTS 6
3.2.3 PERFORMANCE AND EXTENSIBILITY REQUIREMENTS 6
3.2.4 SECURITY REQUIREMENTS 7

4.0 RFP RESPONSE GUIDELINES **7**
4.1 SUBMISSION AND RECEIPT OF PROPOSAL RESPONSES 7
4.2 STRUCTURE OF RFP RESPONSE 7

EXHIBIT A - CERTIFICATE OF AUTHORITY **8**

EXHIBIT B - QUESTIONS **9**
RESPONDENT COMPANY OVERVIEW 9
KEY PERSONNEL AND SUBCONTRACTORS 9
TECHNICAL QUALIFICATIONS 9
APPROACH AND METHODOLOGY 10
REFERENCES 10
SOLUTION COST AND SCHEDULE 10

1.0 RFP GENERAL INFORMATION

The EOS Network Foundation (“ENF”), on behalf of the EOSIO+ Coalition (collectively “ the EOSIO+ Coalition”), is conducting this Request for Proposal (“RFP”) to implement near-immediate byzantine fault-tolerant deterministic finality as part of the core EOSIO protocol in order to improve responsiveness of applications, reduce confirmation times for deposits on exchanges, atomic swap and interchain communications. In addition, this serves as a prerequisite for improved horizontal scalability of transactional throughput via parallelization..

This RFP is being issued to a select group of companies and/or individuals, which are hereafter referred to as “Respondent”.

This RFP specifies requirements from the EOSIO+ Coalition and invites proposals from Respondents for the provision of services defined within it. The EOSIO+ Coalition reserves the right to award contracts in any manner including but not limited to a single Respondent for all or some of the requirements, and multiple Respondents for components of the requirements.

1.1 CONFIDENTIALITY

This RFP is confidential to the EOSIO+ Coalition. Persons or groups submitting proposals (“Respondents”) must not, and agree they will not, distribute this document of the information contained within it to any third party, including the wider EOSIO community, without the written agreement of the EOSIO+ Coalition.

1.2 RFP DOCUMENTS

The EOSIO+ Coalition reserves the right to modify the requirements of this RFP as well as the process utilized by this RFP at any time.

No Reimbursement for Costs. Respondents will incur all costs associated with creating a response to this RFP, no matter the expense. This includes any costs incurred due to delays by the EOSIO+ Coalition in responding or in making a decision.

Authority. By submitting a response for your company, you attest that you have full power to enter into the submission of this RFP response on behalf of your company.

1.3 RESERVATIONS FOR AWARD AND REJECTION OF PROPOSALS

This RFP is not an offer to contract. Even if the Respondent provides a solution that meets all requirements, the EOSIO+ Coalition is not obligated to enter an agreement. The EOSIO+ Coalition reserves the right to make no selection or may choose any Respondent at its sole

discretion. The EOSIO+ Coalition is not obligated to explain its decision making process to any external parties, including the Respondents.

After evaluating the proposals, the EOSIO+ Coalition will make a determination of which solution provides the highest value to the EOSIO+ Coalition. The selected Respondent may be provided additional proposed conditions for entering into a contract with the EOSIO+ Coalition.

1. The EOSIO+ Coalition reserves the right to request additional information from any or all Respondents to evaluate any or all proposals.
2. Before awarding a contract, the EOSIO+ Coalition may request evidence of qualifications, insurance, or other information deemed necessary.
3. The EOSIO+ Coalition may choose to modify the requirements within this RFP when negotiating a contract with the selected Respondent.
4. The EOSIO+ Coalition reserves the right to amend the schedule published within this RFP.
5. The EOSIO+ Coalition may disqualify a proposal if the deadlines stated within this RFP are not met.

1.4 FORMAT REQUIRED FOR RFP RESPONSES

This section describes the format and content required for responses. **Failure to conform to these guidelines may result in disqualification of the response.**

1. Any information provided above what has been specifically requested may be submitted as a separate document only if it adds value specifically to deliberations about this RFP.
2. For each question in Exhibit B, a simple affirmation that the requirement is met will not be considered complete. Each question requires a short, concise explanation as to how the requirement will be met.
3. Occasionally, the Respondent may offer an explanation that explains how more than one requirement will be met. Is it acceptable to copy / paste the same answer for multiple requirements. However, questions should not be grouped together.
4. Pricing not included in this response will not be considered valid cost elements if the Respondent is selected.
5. The Exhibits should be submitted in a Microsoft Word document, Google Doc, or PDF. The pricing spreadsheet may be submitted in a Microsoft Excel document, Google Sheets document, or PDF.

2.0 INTRODUCTION

2.1 FOUNDATION OVERVIEW

The EOS Network Foundation exists to contract the development of world-class corporate identity and branding elements of the organization with a mission to do the following:

- Convey unity amongst participating stakeholders;
- Emote technical excellence and promise of a better future; and
- Express the cohesive vision of improving the world and lives of every individual through new efficient and equitable ways for individuals to empower themselves through fair dealings with other individuals.

2.2 REQUEST FOR PROPOSAL QUESTIONS

After reading this RFP, is it expected that Respondents will need clarification on a variety of points. Respondents must submit questions by the scheduled deadline listed below. The EOSIO+ Coalition will consolidate questions from all Respondents into a single document but remove all reference to which Respondent asked a particular question. The consolidated answers will be distributed to all Respondents per the schedule below.

Submit any questioned regarding this RFP to:

operations@eosn.foundation

2.3 RFP SCHEDULE

The following schedule will be followed to complete the selection of a Respondent to this RFP. Respondents must adhere to this schedule or risk disqualification.

Step	Activity	Deadline
01	RFP released to Respondents	23 MAY 2022
02	Respondents submit Intent to Bid	30 MAY 2022
02	Questions about the RFP by Respondents submitted back to the EOSIO+ Coalition	06 JUN 2022
03	Answers to Respondent questions published to all Respondents	10 JUN 2022
04	RFP responses (Exhibits A & B) to be submitted to the EOSIO+ Coalition	24 JUN 2022
06	Business awarded	01 JUL 2022

3.0 PROJECT INFORMATION

3.1 PROJECT SCOPE

3.2.1 BUSINESS REQUIREMENTS

ID	Requirement
BR01	The solution will provide a mathematical proof of safety for a new consensus algorithm to replace the existing EOSIO consensus algorithm. For the algorithm to have the property of safety, it must not lead to the generation of cryptographic evidence indicating that two conflicting blocks are both final (a finality violation) under the assumption that no more than a third of the participants (by weight) of any currently or previously active consensus participant set in the history of the blockchain have violated the rules of the algorithm. Safety must be guaranteed in the asynchronous network model and must be shown to hold even throughout a change to the active set of consensus participants.
BR02	The solution will provide an additional mathematical proof that the same consensus algorithm proven to have the property of safety as part of BR01 also has the additional property referred to as accountability. The consensus algorithm has the accountability property if: the cryptographic evidence used to determine a particular block is final also indicates which consensus participants necessarily signed the confirmations that led to the block becoming final; and, if a finality violation occurs, the branches containing the two conflicting final blocks have enough evidence (stored just within the block headers) to enable the generation of a cryptographic proof (of finality violation) that correctly attributes blame for the finality violation on at least a third of the participants of the recently active consensus participant set that was common to the history of both branches. The accountability proof must show that a consensus participant which followed the algorithm rules correctly would not be unfairly blamed in an accepted cryptographic proof of finality violation.
BR03	The solution will provide an additional mathematical proof of liveness for the same consensus algorithm proven to have the property of safety as part of BR01 and proven to have the property of accountability as part of BR02. The proof must show that under the scenario where less than a third of the participants of the currently active consensus participant set are faulty (which is to say that they have either violated the rules of the algorithm or have crashed or been arbitrarily delayed in processing/communication) and assuming that blocks will still be produced by block producers in a manner consistent with the finalization rules of the consensus algorithm, it will always remain theoretically possible for the remaining participants of that set to work together to generate cryptographic evidence indicating the newly produced blocks are final and to do so without leading to a finality violation.
BR04	The solution will provide a theoretical analysis on latency and communication

	overhead for the same consensus algorithm proven to have the properties of safety, accountability, and liveness in BR01, BR02, and BR03, respectively. The communication overhead analysis should discuss how the number of cryptographic authenticators and also the bits of the messages communicated by the consensus participants with each other scales as the size of the consensus participant set grows. This analysis should be considered both in the case when the active leader coordinating consensus remains stable, as well as in the "view-change" case when the leader must be changed. Ideally, the communication overhead will be shown to scale linearly with the size of the consensus participant set in both cases. The latency analysis should discuss the number of rounds of back-and-forth communication required between consensus participants starting from when a new proposed block is created to when that block can be considered final. Ideally, the latency analysis will show the algorithm has a property of responsiveness which is to say that under the condition where less than a third of the participants of the active consensus participant set are faulty and the currently selected leader is not faulty, the leader and other non-faulty consensus participants can work towards finalizing a block in time depending only on actual message delays and independent of any presupposed upper bound on message transmission delays (as may be the case for algorithms designed for a synchronous network model).
BR05	The proofs and analysis from BR01 to BR04 will be submitted to the EOSIO+ Coalition Scalability+ working group for approval before incorporation into any deployed solution.

3.2.2 TECHNICAL REQUIREMENTS

ID	Requirement
TR01	The solution will deliver a PR to the nodeos github repository which introduces a consensus protocol feature that when activated will switch from the existing EOSIO consensus algorithm to the new consensus algorithm implementing faster finality and for which proofs and analysis were provided as part of BR01 to BR04.
TR02	The solution will incorporate a cryptographic proof of fast finality consensus in the block headers, so that a block can be recognized as final by a light client (a client that does not need to execute the transactions in the block) without relying on a trusted API node.
TR03	The solution will implement linearly aggregable signatures in the EOSIO codebase in order to keep block header size as small as possible, while also making it convenient to explicitly prove block confirmations from consensus participants.
TR04	The solution will deliver a proof-of-concept demonstrating how, in the event a finality violation occurs, a light client can generate a cryptographic proof of finality violation (as discussed in BR02) and submit to an EOSIO smart contract that is then able to validate the proof and attribute blame for the finality violation to the consensus participants that violated the rules of the consensus algorithm by

	double confirming conflicting blocks.

3.2.3 PERFORMANCE AND EXTENSIBILITY REQUIREMENTS

ID	Requirement
PER01	The solution will not result in a significant increase (e.g. more than triple) of the average block header size or a significant increase in the average block header processing time, even with a consensus participant set size as large as 100. It is acceptable to assume that the active consensus participant set will not change more frequently than once per 10 minutes for the purposes of this performance analysis.
PER02	The solution will allow light clients to very quickly advance from the latest final block ID they already know and trust to the block ID of the latest final block available in the network (with the help of an API node but without requiring trust in the API node). In particular, the light client must not be required to download all block headers in the range between the starting final block ID they already know and trust and the ending final block ID. Instead, data related to a sparse number of block headers within that range should only be required to be transmitted to and validated by the light client. In particular, that sparse number can scale with the number of changes to consensus participants set within that range but should not scale with the number of blocks within that range.

3.2.4 DEPLOYMENT AND MAINTENANCE REQUIREMENTS

ID	Requirement
DMR01	The solution will be deployed onto the Jungle chains.
DMR02	Respondent will fix errors in the solution's codebase found within six months of the deployment on the last chain.
DMR03	Respondent will provide consultancy options to assist other chains in deploying the solution.

4.0 RFP RESPONSE GUIDELINES

4.1 SUBMISSION AND RECEIPT OF PROPOSAL RESPONSES

For consideration, proposals must be received ahead of the scheduled deadline stated within this RFP. Any proposals submitted after the deadline or deemed incomplete **WILL BE REJECTED** unless a specific exemption is granted by the EOSIO+ Coalition at its sole discretion.

Proposals must be submitted electronically. Submit the proposal and/or any questions related to this RFP to:

operations@eosn.foundation

4.2 STRUCTURE OF RFP RESPONSE

Respondents should structure their proposals with the two sections listed in the Exhibits:

Exhibit A: Certificate of Authority

Exhibit B: RFP Questionnaire

Additional information (marketing materials, case studies, etc) may be submitted in a separate document.

EXHIBIT A - CERTIFICATE OF AUTHORITY

The undersigned certifies that he/she has the complete authority to contractually bind the proposing company and to submit a response to this RFP on the company's behalf. The undersigned has read all components of this proposal, including any exhibits and attachments. By submitting this signed proposal, the undersigned acknowledges an intent to accept a contract if this proposal is selected by the EOSIO+ Coalition.

Item	Value
Signed Name (printed)	
Title	
Legal Name of Respondent Submitting	
Address One	
Address Two	
City / State / Postal Code	
Country	
Email Address	
Phone	
Telegram Handle (if applicable)	
Company URL	
Authorized Signature	
Date Proposal Submitted	

EXHIBIT B - QUESTIONS

Respond to all questions within a copy of this document and return your response as either a Google Doc or a Microsoft Word document.

RESPONDENT COMPANY OVERVIEW

1. State the full name, address, and other contact information of your company. Indicate what legal entity type your company operates as (e.g. individual, partnership, corporation, etc) and in which country and state / province / territory is it registered.
2. Provide a brief summary of your company including its history. Include sufficient information to demonstrate your capability to manage a project of this size and scope.

TECHNICAL QUALIFICATIONS

Include a description of how EACH requirement (in Section 3) will be met.

3. If your company's solution will not meet every requirement defined in Section 3, please identify which requirements will not be met.
4. Provide examples of similar projects that your company has successfully delivered.

APPROACH

5. Describe your approach to post-implementation support and transferring approach knowledge to the EOSIO+ Coalition staff.
6. Would you project and service level guarantees in our agreement?

SOLUTION COST AND SCHEDULE

7. Provide a spreadsheet identifying the total costs of the solution outlined in Section 3. Identify as applicable: labor, software licensing, maintenance / support fees, hardware, and other expenses.
8. Detail the payment schedule and include any milestones that may trigger a payment
9. Provide a rough estimate of the project schedule.

REFERENCES (OPTIONAL)

10. Supply three references of customers to whom you provided similar solutions.