Smart TRB: An Incentive Compatible Consensus Protocol Utilizing Smart Contracts

Nikita Borisov
nikita@illinois.edu

Abhiram Kothapalli
kothapa2@illinois.edu

Andrew Miller
amiller@cs.umd.edu

Abstract

We propose a modified repeated terminating reliable broadcast algorithm to be used as an alternative to the largely inefficient blockchain based consensus algorithm for smaller networks. Our protocol consists of rational nodes following a modified Dolev-Strong consensus algorithm and later reporting to a smart contract. The smart contract then distributes rewards depending on if the nodes have properly followed the protocol. We i) describe previous work by Clement et al. [2] which this works motivations are largely based upon; ii) describe our protocol from a game theory perspective to account for rational nodes; iii) rigorously prove that rational players will choose to adhere to our protocol; iv) argue why our protocol is a more efficient solution to the current blockchain based consensus algorithms.

Keywords— TRB, game theory, Ethereum, smart contracts

1 Introduction

1.1 Previous Work

We build our protocol largely on the classic Dolev-Strong algorithm with authentication as described by Kumaresan [3]. Kumaresan’s modified protocol follows the following four requirements of a terminating reliable broadcast:

1. Termination: Every correct process delivers some value.

2. Validity: If the sender is correct and broadcasts a message \( m \), then every correct process delivers \( m \).

3. Integrity: A process delivers a message at most once, and if it delivers some message \( m \neq \text{senderFaulty} \), then \( m \) was broadcast by the sender.

4. Agreement: If a correct process delivers a message \( m \), then all correct processes deliver \( m \).
Unfortunately, while Kumaresan’s Dolev-Strong protocol satisfies the requirements of a terminating reliable broadcast algorithm it fails to account for rational nodes who may deviate from the protocol in order to maximize their utility.

This shortcoming is first addressed by Clement et al., which proves that in a situation containing rational nodes that attempt to maximize their own utility, the Dolev-Strong protocol may not hold. Clement et al. achieves the following. i) Detailed the need to recognize rational players who may deviate from a consensus protocol in order to maximize their utility. ii) Formally expresses the terminating reliable broadcast protocol as a game in which rational players can behave selfishly by not sending messages to save costs. iii) Proves that the Dolev-Strong algorithm cannot protect against selfishly acting players. iv) Proposes an alternative protocol, Just TRB, capable of tolerating rational selfish players. The proposed protocol includes three modifications: A predictable communication pattern that can detect nodes that choose not to forward messages, a friends/enemies status to mark deviating players, and a penance message system to punish deviating players. v) Uses game theory analysis to prove that Just TRB is a Nash equilibrium and therefore rational players will adhere to Just TRB.

While Clement et al. [2], proposes a viable solution to rational nodes it choses to abstract the utility that nodes recieve for following the protocol by assuming that all nodes are stakeholders of the system that get some implicit reward if consensus is achieved. We challenge this assumption by reasoning that in most use cases such an implicit utility does not exist. For example let us consider a third party that makes an application which requires decentralized consensus. If the third party choses to hire private nodes to achieve consensus then the hired nodes recieve no implicit utility for following the protocol.

1.2 Contribution
In order to create a more viable utility model we propose a new protocol, Smart TRB, in which utility is provided from outside the protocol. In the protocol, a third party funds an Ethereum smart contract [1] and then hires nodes to perform consensus. After all the nodes finish $N$ rounds of consensus they report to the smart contract which then verifies that players have followed the protocol and distributes the initial funds accordingly. We formally describe and thoroughly analyze this protocol and prove that it is incentive compatible.

2 Smart TRB Protocol
2.1 Description
The Smart TRB Protocol can be broken into 3 distinct parts: the client who sends requests to the consensus network, the nodes which participate in the consensus algorithm, and the smart contract which rewards nodes for their work. We will describe all the nodes participating in the protocol as $N$, all byzantine nodes as $B$ where $B \in N$ and $|B| < b$, all clients as $T$. 
2.1.1 Client Protocol

A client simply sends a request some node \( q \in N \). The client will later request results from any node \( p \in N \). In order to ensure that the output has been proposed by \( q \), the client will only accept a result with \( q \)'s signature.

2.1.2 Node Protocol

Initially all nodes in \( N \) will register with the smart contract. Every node is numbered in the order of registration. Because all the content of a smart contract is publicly visible, this will also inform the clients about which nodes are available to send requests to. Once registered, every node is capable of accepting requests from clients which are stored in its queue (This process runs continuously in the background). The nodes then run \( K \) rounds of a modified Dolev-Strong algorithm where in round \( i \), node \( i \) mod \( N \) is the leader which gets to propose a request from its queue. The modifications are as follows:

Modification 1: We impose a predictable communication pattern so that nodes can detect if another is cutting costs by not forwarding messages. Our predictable communication pattern requires that in each D-S instance node \( p \) must send every node \( q \) at least two messages. Each of these messages can either contain a meaningful or dummy value. We will call any sequence of messages adhering to these rules an acceptable message sequence.

Modification 2: We enforce a penalty for not forwarding messages using the following rules. We use Node \( p \) and Node \( q \) to represent two arbitrary nodes in \( N \) where \( p \neq q \).

- All nodes maintain a status label for other all other nodes. \( p \) can label \( q \) as either good or bad.
- All nodes begin with labeling each other as good.
- Whenever \( p \) detects that \( q \) has not followed an acceptable message sequence, \( p \) will label \( q \) as bad. Once a node is labeled bad, it remains bad throughout the remaining Dolev-Strong rounds and cannot make amends.
- If \( p \) considers \( q \) bad then \( p \) does not send messages to \( q \).
- At the end of \( K \) Dolev-Strong rounds all nodes report their observed statuses of other players. If \( p \) observes \( q \) as good it reports \( f \) for friend, otherwise it reports \( e \) for enemy.
- The smart contract then deducts from a nodes’ rewards depending on the number of enemies the node has made.

Finally each nodes stores the outputs of each Dolev-Strong round and reports to the clients when requested.
2.1.3 Smart Contract Protocol

We begin by assuming that the smart contract receives an endowment $E$ from outside of the protocol. The smart contract will then allow up to $N$ nodes to register and initially assigns each nodes reward to $E/N$. The smart contract will then wait to receive enemy reports from all nodes $p \in N$.

Once this step is complete, the smart contract will proceed to deduct node $p$’s reward for every node $q \in N - \{p\}$ as follows: If $q$’s reports $p$ as an enemy, then $p$’s reward is deducted by some constant $\theta$. This leads to $p$’s maximum cost of $N \cdot \theta$ and the total possible deductible amount to be $N^2 \cdot \theta$. This leads to the additional assumption that $E > N^2 \cdot \theta$.

2.2 Pseudocode

**Algorithm 1** Client Protocol

1: $N \leftarrow \text{smartContract}_N$\Comment{wait after this step}
2: send input to $q \in N$
3: $i \leftarrow 0$
4: result $\leftarrow \emptyset$
5: while result does not contain $q$’s signature do
6: result $\leftarrow \text{Node}_i$’s outputs
7: $i \leftarrow i + 1$

**Algorithm 2** Node Protocol for arbitrary node $p$ numbered $p_i$

1: register with smart contract
2: outputs $\leftarrow []$
3: queue $\leftarrow []$
4: bad $\leftarrow \{\}$
5: in the background: queue $\leftarrow$ queue + client’s input
6: in the background: if client requests output, send outputs to client
7: while $i < K$ do
8: run Dolev-Strong with the following modifications:
9: if $i \mod N = p_i$ then
10: propose element from queue \Comment{$p$ is the leader}
11: for all $q \in N - \{p\}$ do
12: if $q \in$ bad then
13: $p$ does not forward messages to $q$
14: if messages$_q \notin$ AcceptableMessageSequence then
15: bad $= $ bad $+ q$
16: outputs$[i] =$ DSprotocol$\_output$
17: queue $= $ queue $-$ outputs$[i]$
18: $i \leftarrow i + 1$
Algorithm 3 Smart Contract Protocol

Ensure: receives report $R_p$ for all $p \in N$
Ensure: receives endowment $E > N^2 \cdot \theta$

1: for all $p \in N$ do
2: $\text{reward}_p \leftarrow E/N$
3: for all $q \in N - \{p\}$ do
4: if $R_{pq} \neq f \lor R_{qp} \neq f$ then
5: $\text{reward}_p \leftarrow \text{reward}_p - \theta$
6: distribute $\text{reward}_p$ to $p$

3 Assumptions

Assumption 1. The cost of client communication is free

Assumption 2. Sufficient endowment $E$ is placed in the smart contract. Additionally $E > N^2 \cdot \theta$

Assumption 3. Rational players can be modeled as risk averse players who act to maximize the worst case utility. The worst case arises from the worst set of Byzantine players in combination with the worst set of strategies those players can take

4 Definitions

Definition 1. Player In order to describe our protocol from a game theory perspective, we will treat it as a game and rename all our nodes as players. Players are simply nodes with that attempt to maximize their own utility.

Definition 2. Acceptable Message Sequence. Player $p$ follows an acceptable message sequence towards player $q$ if, for every round $i \in K$, $p$ sends $q$ at least two messages containing either a meaningful value or a dummy value.

Definition 3. Report. Message $R_p$ that is sent to the smart contract by every player $p \in N$ after $K$ Dolev-Strong rounds containing $p$'s status with every player $q \in N - \{p\}$. A status can either contain $f$ for friend or $e$ for enemy. $R_{pq}$ denotes $p$'s chosen status for $q$

Definition 4. Good. Player $p$ is considered good by player $q$ if $p$ follows an acceptable message sequence towards $q$. $p$ is considered bad otherwise.

Definition 5. Honest. Player $p$ is defined to behave honestly if it reports every player $q$'s behavior to the smart contract such that if $q$ behaves good $R_{pq} = f$ and $R_{pq} \neq f$ otherwise.

Definition 6. Message Cost. We assume a baseline cost $\mu$ for every message player $p$ has to send player $q$. $M$ is the maximum message cost of all the messages $p$ has to send $q$
Definition 7. Report Cost. Utility cost incurred by smart contract after receiving \( R_p \) for all \( p \in N \). \( C_p^q \) is defined to be the report cost incurred on \( p \) by \( R_{qp} \). We set the report cost of friendship to be zero:

\[
\forall p, q \in N, R_{pq} = f \land R_{qp} = f \Rightarrow C_p^q = 0
\]

We set the report cost of all other scenarios to be \( \theta \) to be discussed:

\[
\forall p, q \in N, \neg(R_{pq} = f \land R_{qp} = f) \Rightarrow C_p^q = \theta
\]

Definition 8. Reward. Amount dispensed by the smart contract to every player \( p \) after receiving \( R_q \) from every player \( q \). We define player \( p \)'s reward, \( reward_p \), as follows:

\[
\forall p \in N, reward_p = E/N - \sum_{q \in N - \{p\}} C_p^q
\]

Definition 9. Spiteful Strategy \( \sigma_s \). Strategy in which player \( q \) appears good to \( p \) but will always attempt to report the opposite of \( p \) with \( R_{pq} \neq R_{qp} \). We define \( p \)'s worst case to be when all byzantine players \( q \) decide to follow the spiteful strategy.

5 Rationality Analysis

In order to prove that rational players will adhere to Smart TRB we will take the following steps:

1. assume that rational player \( p \) will attempt to maximize its worst case utility and define a bound for the report cost, \( \theta \), such that \( p \) is gains the highest utility by following the protocol.

2. assume that all players \( q \in N \) follow the spiteful strategy and show that utility \( U_{\text{max}} \) is the best case for \( p \) over all possible strategies

3. assume that \( p \) follows the correct protocol, and show that even if all \( q \) follow the spiteful strategy, \( p \)'s worst case utility is \( U_{\text{min}} \)

4. show that \( U_{\text{max}} = U_{\text{min}} \) and therefore \( p \) incurs no additional cost by following the protocol

5.1 \( \theta \)-bound

Because \( p \) will attempt to maximize its worst case utility, we consider the case in which all \( q \in N - \{p\} \) is playing the spiteful strategy, in which \( q \) appears good to \( p \) but \( R_{pq} \neq R_{qp} \).

Strategy \( \sigma_1 \): Player \( p \) sends messages to every \( q \in N - \{p\} \)
Strategy $\sigma_2$: Player $p$ randomly sends messages to $n\%$ of $q \in N - \{p\}$

In order for $p$ to always pick $\sigma_2$ we want:

\[
\text{Cost}(\sigma_1) \leq \text{Cost}(\sigma_2)
\]

\[
(N - 1) \times M + b \times \theta \leq (b + (N - 1 - b) \times (n\%)) \times \theta + (N - 1) \times (1 - n\%) \times M
\]

\[
(N - 1) \times n\% \times M \leq (N - 1 - b) \times n\% \times \theta
\]

\[
\frac{N - 1}{N - 1 - b} M \leq \theta
\]

5.2 Smart TRB is a Nash Equilibrium

Lemma 1. If all $q \in N - \{p\}$ follow the spiteful strategy, $(N - 1) \times M + b \times \theta$ is the least cost $p$ can incur.

Proof. Because all $q \in N - \{p\}$ follow the spiteful strategy, $R_{pq} \neq R_{qp}$, $p$ minimizes its cost by not sending any messages leading to an overall cost of $(N - 1) \times \theta$ only due to report cost.

\[
(N - 1) \times \theta = (N - 1 - b) \times \theta + b \times \theta
\]

\[
= \frac{(N - 1 - b)(N - 1)}{(N - 1 - b)} M + b \times \theta
\]

\[
= (N - 1) \times M + b \times \theta
\]
Lemma 2. If $p$ follows Smart TRB, $p$'s maximum cost regardless of $q \in N - \{p\}$ strategy is $(N - 1) * M + b * \theta$

Proof. $p$'s worst case is again when all $q$ play the spiteful strategy. Under this scenario because all $q$ appear good $p$ will send all $q$ messages as the protocol dictates and will incur $(N - 1) * M$ message cost. Additionally because for every byzantine player $q$ $R_{pq} \neq R_{qp}$, $p$ will also incur a total report cost of $b * \theta$. This leads to a total cost of $(N - 1) * M + b * \theta$.

Theorem 1. Following Smart TRB provides the highest utility and is therefore a weak Nash equilibrium

Proof. From Lemma 1 and Lemma 2, $p$'s minimum cost from not following the protocol is the same as $p$'s maximum cost from following the protocol. $p$ can therefore expect the least cost in the worst case by following the Smart TRB protocol.

6 Protocol Adherence Analysis

Lemma 3. If rational player $p$ considers player $q$ bad, then $p$ will behave badly towards $q$

Proof. Because $p$ considers $q$ bad, $q$ is not following the protocol and therefore is a Byzantine node. Because we defined $p$'s strategy as maximizing its worst case utility, $p$ will expect the worst possible report from $q$ where $R_{qp} \neq f$. Therefore $p$ can be viewed by $q$ as good or bad without changing $p$'s utility. This causes $p$ to default to bad behavior towards $q$ to save message costs.

Lemma 4. If rational player $p$ considers player $q$ good, then $p$ will behave good towards $q$

Proof. From Theorem 1, because following Smart TRB is a Nash equilibrium, $p$ cannot save any costs by deviating from the protocol. Therefore $p$ will send $q$ messages as per the protocol.

Lemma 5. Rational player $p$ will behave honestly

Proof. Let us consider $p$'s honesty with one player $q$. Suppose $p$ considers $q$ bad. Then $p$ can use the same reasoning in Lemma 3 to expect $R_{qp} \neq f$. Therefore $p$ can elect to follow the protocol by reporting $R_{pq} = e$ with no additional cost.

Suppose $p$ considers $q$ good. From lemma 2 we know $p$ will be good to $q$. If $q$ is non-byzantine then $R_{qp} = f$ and $p$ benefits from $R_{pq} = f$. On the other hand if $q$ is byzantine, $p$ can expect that $q$ plays the spiteful strategy, where $R_{pq} \neq R_{qp}$, and therefore $p$ expects the same cost with $R_{pq} = f$ and $R_{pq} = e$. Therefore $p$ can elect to follow the protocol by reporting $R_{pq} = f$ with no additional cost. Because $p$ will elect to report $R_{pq} = f$ if $q$ is good and $R_{pq} = e$ if $q$ is bad for all $q \in N$, $p$ will behave honestly.
Theorem 2. Rational player \( p \) will adhere to the Smart TRB protocol

Proof. Because Lemma 1, 2, and 3 hold a rational player \( p \) attempting to maximize its utility will follow all the requirements of Smart TRB.

7 Conclusion

We have described the classic Dolev-Strong protocol and introduced an additional protocol, Just TRB, that makes Dolev-Strong incentive compatible. We additionally build upon Just TRB by redefining its utility model with a concrete reward, independent of the consensus protocol. We describe our protocol by outlining its smart contract, client, and node protocols. We set a bound for the cost of being declared an enemy such that this cost balances out the cost saved from not forwarding messages. We use this bound to prove that Smart TRB is incentive compatible. Finally we show that rational player \( p \) will follow all components of the protocol.

8 References

References

