Pari: a High Performance Permissionless Decentralized Betting Service

Rui Morais

October 2023

Abstract

The Pari protocol introduces a novel decentralized betting protocol with the goal of seamlessly onboard Web 2.0 and Web 3.0 betters. Pari leverages the robustness of blockchain technology to facilitate transparent and tamper-resistant betting, while offering a user experience on par with centralized systems in terms of latency and scalability.

This is achieved by outsourcing some components of the protocol to an efficient decentralized payments network, including payments and Sybil resistance, avoiding the need for having accounts or tokens in the Pari network. Pari focuses only in hosting and executing betting contracts in a decentralized way, which use the parimutuel betting system instead of the traditional peer-to-peer betting. This system facilitates peer discovery, increasing the liquidity of the markets.

1 Introduction

Betting, a pastime deeply rooted in human history, has long been a confluence of skill, chance, and strategy. While the thrill of prediction and potential for reward remain constants, the mechanisms and platforms through which people bet have evolved dramatically. Today's digital age has ushered in online platforms, enabling easier access and broader participation. Yet, as with many industries that have migrated online, betting platforms are primarily centralized, often leading to concerns about fairness, transparency, control, and security.

Decentralized betting platforms try to solve these issues, however in doing so they sacrifice some of the experience the user is accustomed to. This happens because these platforms inherit the problems of the underlying blockchains, namely high fees, high latency and low throughput.

The Pari protocol described in this document is an attempt to conciliate the advantages of both systems, while at same time minimizing its problems. If successful, it can revolutionize the world of betting.

1.1 Value Proposition

Pari protocol value proposition can be summarized in the following way:

- The service is decentralized, meaning that more than 2/3 of the voting power of network is needed to validate and execute betting contracts, making it fairer and more trustworthy.
- Every part of the service, from the proposal of the betting contracts to the bets and the execution of the contracts is public, so anyone can verify its correctness.
- Any user can propose betting contracts.
- The service is pseudo-anonymous and does not require any type of registration.
- It uses the parimutuel betting system, which does not have much online presence compared to other systems and itself can be a reason for users to join.
- The service has low fees and low latency.
- The Pari node has minimal computing requirements because it outsources part of the work to an independent payments network.
- The Pari network is permissionless, meaning any user can run a node and win rewards by validating and executing betting contracts.

2 Pari Protocol Overview

The diagram provides a visual representation of the Pari Protocol's system architecture.

- **Pari Network**: Nodes with voting power of the Pari network are called representatives and communicate with each other to validate betting contracts by reaching consensus on them. The betting contracts are proposed by users through nodes. Execution of contracts and the corresponding payments to the winners also require consensus of the representatives.
- **Proof of Investment**: The mechanism to prevent Sybil attacks on the Pari Network. The stake of each Pari node is proportional to the investment made to the Pari's Development Fund, which is an account on the payments network. This can be increased anytime and the stakes are updated from time to time. The proof of investment is made with a signature proving the ownership of the private key of the account that made the investment. Due to performances reasons, the number of representatives on the Pari network will probably be capped. However, Delegated Proof of Investment protocols can be be developed off-chain so that smaller investors can also win rewards and are incentivised to participate.

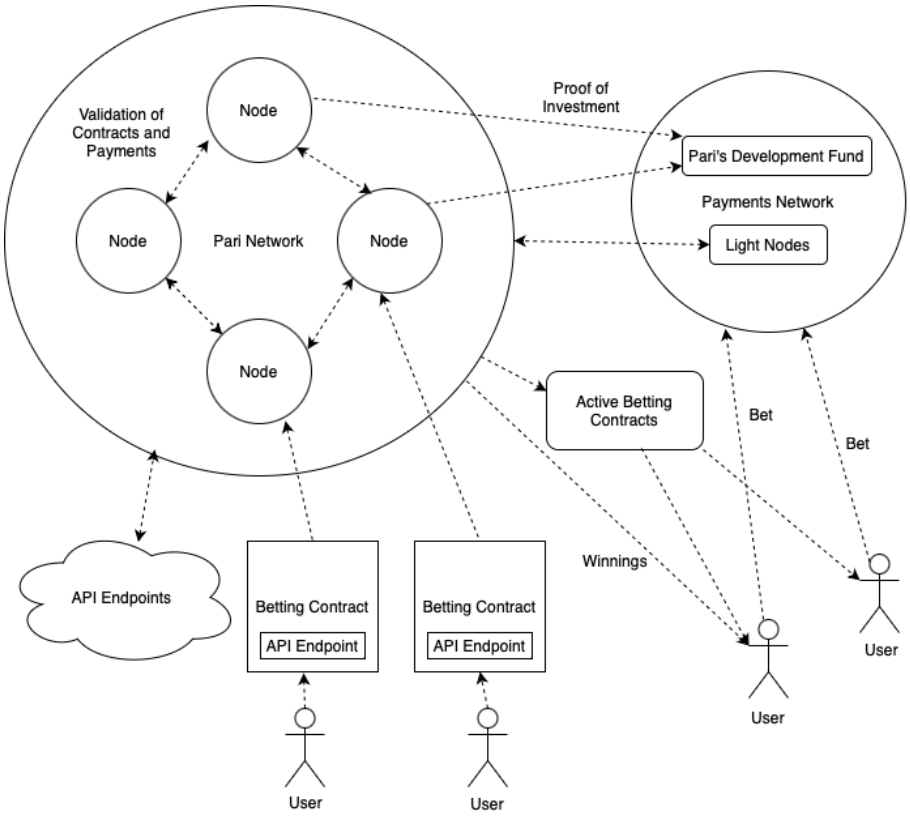

Figure 1: Pari Protocol Overview

- **Betting Contracts**: Each of these contracts is associated with a well defined event, with a start and an end, and with an account corresponding to each of the outcomes of the event. One or more API endpoints report the outcome of the event and a time window can be added in order to minimize non execution of the contract due to unresponsiveness of API endpoints.

- **API Endpoints**: A list compiled by the development team of Pari with trusted and reputable sources to make sure that no malicious endpoints are added to the network. However, anyone can propose new APIs.

  Each betting contract condition can have one or more API endpoints to minimize centralization and increase redundancy. For example, the contract can stipulate that two sources need to give the same information for the contract to be executed or that a second source can be used if the first is unresponsive. In case the contract cannot be executed, the bets are returned to the users.

- **Users**: Users can interact with the Pari protocol in three possible ways:

    1. Propose new betting contracts, which they send to a Pari node, that broadcasts it to the rest of the network to be validated.
    2. Users can also make requests to the Pari network directly (through to the node's RPC) or indirectly (through a website or application) to know what betting contracts are active.
    3. They can then bet on them by making payments directly in the payments network to the account of the associated outcome in the contract.

- **Light Nodes**: Each Pari full node must have access to the payments network to verify what payments have been done, including investments and bets, and to make the payments to the winners of the bets.

3 Betting Process Flow

The betting process within the Pari Protocol has been meticulously designed to ensure a seamless, transparent, and fair experience for participants. Here is a step-by-step breakdown of the entire flow, from contract initiation to the eventual distribution of winnings:

1. **Contract Proposal by Nodes**: Initiated by a user through a node, a betting contract, encompassing event details, potential outcomes, allocated accounts, and associated API endpoints, is proposed to the network.

2. **Contract Validation and Agreement**: The proposed contract undergoes rigorous validation by nodes in the Pari network. Checks are made for account availability and validity of the associated API endpoints. After consensus is achieved, the contract becomes active.

3. **User Bet Placement**: With the contract now active, users can begin placing bets. Upon entering a website that is an explorer of the Pari network, users are presented with a neatly organized list of upcoming events, allowing them to effortlessly navigate through their betting options.

   Each event displays real-time odds derived from the total amount of bets placed by users in each outcome, so they can easily grasp the current betting trend and make an informed decision.

   Should a user decide to place a bet, they are presented with a QR code linked to an address in the payments network controlled by Pari representatives. With their wallet of the payments network, users can swiftly transfer their desired bet amount by simply scanning the QR code. This eliminates the need for registrations or logins.

4. **Outcome Determination**: Once the event concludes, Pari representatives initiate data retrieval from the trusted API endpoints specified in the betting contract and converge to achieve consensus on the event's outcome and the winning bets. Other nodes on the network can independently verify the execution of the contract.

5. **Fee Deduction and Distribution**: A nominal fee, as predetermined, is deducted from the total pool and goes to a representative selected in a weighted random lottery. The seed used can be the contract itself plus the outcome, since it is unpredictable.

6. **Payout to Winners**: The remaining amount, after fee deduction, is distributed to the winners. Using the payments network, swift and efficient payouts are made to the accounts from which the winning bets originated.

7. **Contract Conclusion and Account Recycling**: With the winnings distributed, the betting contract concludes. The associated payments network accounts are emptied and are now available for future betting contracts.

4 Technical Details

Given the value-centric nature of betting systems, ensuring security is of paramount importance. The Pari Protocol has been designed with multiple layers of security measures, safeguarding against potential vulnerabilities and ensuring a trustworthy environment for participants.

4.1 Distributed Key Generation (DKG) Protocol

At the start of the protocol, Pari representatives generate an amount of sets of keys (public keys and corresponding private keys that can be used in the payments network) in a distributed way with a DKG protocol by distributing some quantity of shares proportional to the weight of the representatives without the need of a trusted dealer.

This means that no representative has access to a single private key, and at least a threshold t of voting weight is needed for a private key to be used to sign a transaction.

The generated public keys represent accounts and will be used in betting contracts as a way to associate a user bet to a given outcome. After the execution of the contract, the payments to the winners and the corresponding fee to the elected representative are made using the Threshold Signature Scheme. The more accounts are controlled by Pari representatives, the more active betting contracts the network can handle and the bottleneck will be in the payments network.

4.2 Parimutuel Betting System

A parimutuel betting system has the following characteristics:

- **Pooling of Bets**: Unlike fixed-odds betting where the bettor knows the potential payout when placing the bet, in parimutuel betting, all bets of a particular type are placed together in a pool.
- **Dynamic Odds**: There are no fixed odds in parimutuel betting. The odds change in real-time based on the number and amount of wagers placed on each outcome.
- **Determining Payouts**: Once the event concludes and winners are determined, the pool is divided among the winners. But before that, the house or the track will take its share or "takeout" from the pool as a commission for hosting the event. The remaining amount is then distributed among the winning ticket holders. The payout to winners is determined by dividing the remaining pool (after the takeout) by the number of units bet on the winning selection.

For example, let's consider a simple horse race. If 100 is bet on Horse A to win and 200 in total is bet on Horse B to win, and the house takes a 10% commission: If Horse A wins, the house takes its 30 commission (300 total * 10%), leaving 270 proportionally. Those who bet on Horse A would share this 270. If you had bet 10 on Horse A, you'd get (10/100) * 270 = 27 as your payout. If Horse B wins, the payout process would be similar, but the distribution would be among those who bet on Horse B.

This system was chosen to decrease the complexity of the system, and to increase the scalability and the liquidity of the protocol by having an implicit peer discovery mechanism. For example, in traditional peer-to-peer betting, a better bets some amount on a given outcome at a proposed odd, which then needs to be matched by other better and this can be hard to achieve in an non liquid market. Parimutuel does not have that problem, because a user can unilaterally bet any value in an outcome and the odds will be determined in the end by all bets.

4.3 Betting Contract

- **Event**: API endpoint that points to the id of the event.
- **Start**: API endpoint that points to start of the event.
- **End**: API endpoint that points to start of the event.
- **Status**: API endpoint that points to status of the event, i.e., if it already started, finished, etc.
- **Execution Window**: Interval of time after the end of the event when the betting contract needs to be executed. If not executed in time (because

the API endpoint is unresponsive, for example), the bets are returned to the betters.

- **Betting Period**: Before or during the event, or both.
- **Conditions**: Fields of the API endpoint that define the outcomes. For example, the outcome will be based on comparing the score of team 1 and team 2. The specific condition for the bet a comparison of the score of team 1 and the score of team 2, so there will be three possible outcomes: team1.score ¿ team2.score; team1.score ¡ team2.score; team1.score = team2.score.
- **Accounts**: One account for each unique outcome defined in each condition.
- **Signature**: Optional field with a signature corresponding to an account in the payments network. The amount invested by the account is used to prioritize its proposed betting contract relative to others.

4.4 Network Time Protocol (NTP)

Nodes within the Pari network use NTP to synchronize their local clocks at the star and restart of the node, ensuring all nodes operate with a consistent perception of time, critical for event start and end timestamps.

4.5 Consensus Algorithm

A consensus algorithm is needed to validate the betting contracts and to execute them, i.e., agree on what are the amounts to be transferred and to who. Any consensus algorithm with high throughput and low latency can be used. It can be synchronous/leader-based or asynchronous/leaderless, since betting contracts are independent of each other.

The choice of the consensus algorithm will depend on the degree of synchronization of contract execution of the representatives, namely what bets are accepted as valid according to each local time. The higher the synchronization, the less conflicting values in the consensus process and a leaderless should achieve less latency. Otherwise, it could be more performant to have an elected leader propose an execution of the contract. However, this can lead to other issues, like censorship resistance.

4.6 Fee Structure

A nominal fee, predetermined, is deducted from the total bet pool before distributing winnings and distributed among all Pari nodes proportionally to their investment. This serves as a revenue stream for node operators, rewarding them for their services and maintaining the network.

4.7 Payments Network Requirements

An ideal payments network has the following properties:

- Low latency transactions: The lower the latency, the better the user experience.
- Zero or low fees: No fees greatly decrease the complexity of the protocol and increase the user experience.
- Medium to high throughput: The ability to scale as the demand increases is important to maintain the quality of the service.
- Decentralization: The consensus power is distributed by different entities.
- Eco-friendly: The consensus algorithm is efficient and does not require big amounts of energy.
- Easy integration: The RPC of the node has the required features and it is well documented.
- Time-tested: The older the project, the better.
- Light clients or low requirements for running a node: The lower the requirements, the lower the requirements for a Pari node as well and the greater the decentralization of the network.
- High liquidity: The currency is not concentrated in the hand of few.
- Non-inflationary or low inflation: Inflation increases the supply of the currency, making each unit of it to worth less.

5 Roadmap

As with any progressive technology, the Pari Protocol is on a journey of continuous refinement, growth, and adaptation. Here's a roadmap sketching out the anticipated trajectory:

- **Q1 2024**: Start of development.
- **Q3 2024**: Minimal Viable Product delivery, launch of the beta version of Pari to a limited number of users for feedback and stress-testing and conduct comprehensive third-party security audits to identify potential vulnerabilities and address them proactively.
- **Q4 2024**: Documentation and Tutorials: Release comprehensive documentation, user guides, and tutorials to assist new users and nodes in joining and navigating the Pari ecosystem.
- **Q1 2025**: Official Release: Rollout of the Pari Protocol to the public.

6 Conclusion

In a world where trust in centralized systems is waning and the performance of decentralized systems is subpar, the Pari Protocol emerges as a beacon of transparency, fairness, and user experience. By elegantly merging the principles of Parimutuel betting with the cutting-edge capabilities of decentralized technologies, Pari promises to revolutionize the betting arena.

With a clear roadmap laid out and an unwavering commitment to continuous improvement, the future of Pari is not just about bets and payouts; it's about building a community-driven platform where every stakeholder, from a casual bettor to a dedicated node, finds value, trust, and excitement.

As we look ahead, we invite pioneers, enthusiasts, and visionaries to join us on this journey. Together, we'll redefine betting for the digital age, anchored in transparency, driven by community, and propelled by innovation.