

**10 JANUARY 2023**

**VALA.AI  
PROJECT  
REPORT**

# EXECUTIVE SUMMARY

Starting in May 2021, Vala LLC embarked on a project to develop a platform for decentralized prediction markets. Using the Bitcoin SV network and Bitcoin script, we developed multiple open-source tools, including an LMSR-based smart contract market maker and a non-custodial Bitcoin wallet. Our unique system for implementing market oracles and a transparent revenue scheme resulted in an open, user-driven prediction market platform. After a successful public Beta test from September to November 2022, we gained invaluable insights that have shaped our future development strategy.

Their platform can be explored at [Vala.ai](https://vala.ai), the published code is available on [github.com/valapm](https://github.com/valapm), the blog can be read at [blog.vala.ai](https://blog.vala.ai), detailed documentation can be referred to at [docs.vala.ai](https://docs.vala.ai), and updates can be followed on [Twitter](https://twitter.com/valaai).

# INTRODUCTION

Vala LLC is an innovative company dedicated to advancing distributed systems, with a primary focus on prediction markets. We strive to harness the potential of these decentralized systems, aiming to revolutionize the way information is aggregated and predictions are made. This report delves into our two-year journey of research, development, and deployment of a novel decentralized prediction market, marking an important milestone in our ongoing mission to shape the future of predictive analysis.

# PROJECT OVERVIEW



The project aimed to create a decentralized prediction market platform, driven by the potential benefits these systems offer. Harnessing the power of collective insights, prediction markets integrate information from diverse sources, making them resistant to manipulation and providing a more

comprehensive understanding of various scenarios. Their application potential spans a broad spectrum - from health & medicine, environmental protection, and public corporations management, to scientific theory & discovery, and disaster response coordination.

Decentralized prediction markets further amplify these advantages. They do not hold user funds in custodial accounts, thereby reducing time-based risk. They operate

globally, unaffected by jurisdictional limitations and are uncapped, enhancing their capacity to root out corruption. They also enable anonymous usage, reducing risks for whistleblowers, and efficiently aggregate information due to reduced friction.

Our aim with this project was not only to leverage these benefits but also to contribute to the evolution of prediction markets by developing a user-friendly, open, and secure platform. This report explores the journey of our project, from inception to deployment, and the lessons we learned along the way.



Resolved Prediction Market

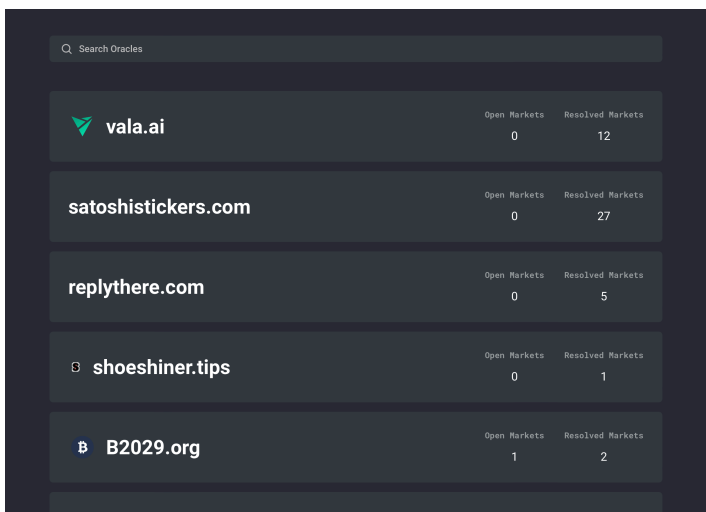
# TECHNICAL RESEARCH AND SELECTION

Our journey began with a thorough technical evaluation. We opted for a UTXO-based blockchain, recognizing its scalability potential, a crucial aspect for facilitating high-frequency markets. Among the various UTXO-based chains, Bitcoin SV emerged as the preferred choice. Its significantly lower network fees and extensive smart contract capabilities were particularly attractive for executing our sizable and complex smart contracts.

To manage the complexity of these smart contracts, we needed a high-level language that compiles down to Bitcoin Script. For this purpose, we chose sCrypt. However, it's worth noting that this choice presented its own set of development challenges down the line.

As for the market maker selection, Robin Hanson's LMSR was chosen. The LMSR, or Logarithmic Market Scoring Rule, facilitates continuous trading in prediction markets, even in situations of low liquidity, which we anticipated. The resulting blend of technological components laid a solid foundation for the development of our prediction market platform.

# MARKET ORACLE RESEARCH AND IMPLEMENTATION



Oracle	Open Markets	Resolved Markets
vala.ai	0	12
satoshistickers.com	0	27
replythere.com	0	5
shoeshiner.tips	0	1
B2029.org	1	2

Live Oracle Overview

For the creation and resolution of markets, our research led us to use traditional oracles due to their straightforwardness and practicality. In our setup, the oracles were tasked solely with market creation and resolution, with smart contracts ensuring they held no additional influence over the markets.

Trustworthiness of oracles emerged as a key concern. We decided the optimal solution was to maintain

maximum transparency and delegate the judgement of oracle reputability to the user. To maintain decentralization, we established a process allowing anyone to become an oracle without needing approval. The DNS system was employed as an independent source of trust. Oracles were required to add a DNS entry to their domain, thus validating their domain ownership to users. This approach allowed users to evaluate trust based on this information.

Further, the decision-making history of oracles was made sufficiently transparent to users, providing additional context for trust assessment. This balanced solution, combining user judgement and transparency, addressed the oracle trust issue effectively in our platform design.

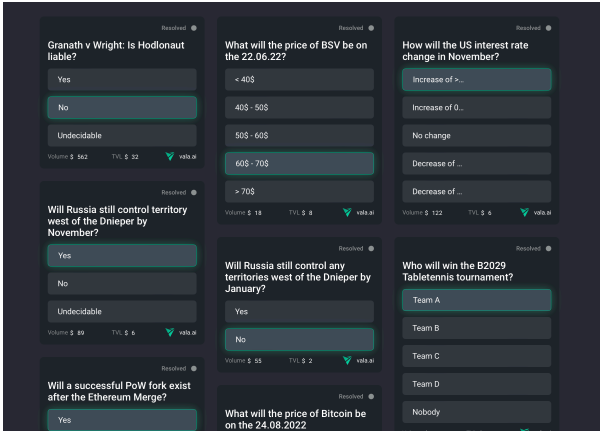
# REVENUE SCHEME SELECTION

Establishing a suitable revenue scheme was crucial for both platform sustainability and oracle incentive structure. After testing different options, we chose a flat fee per trade for the platform. For the oracles, a self-decided flat fee at market creation was implemented. This dual-fee structure supports continuous operation while encouraging active oracle participation.

# DEVELOPMENT

## OPEN SOURCE TOOLS

The development phase initiated with the creation of essential open-source tools. Key among these was a Bitcoin script library for advanced fixed-point arithmetic. Specifically, this library allowed us to implement logarithmic and exponential



Market Overview

functions in Bitcoin script, which were critical for our LMSR-based market maker. Additionally, we crafted a Bitcoin script library for Merkle tree compression and validation to maintain data integrity while managing increasing state sizes efficiently. Both these tools were released under a permissive license to stimulate community-wide innovation.

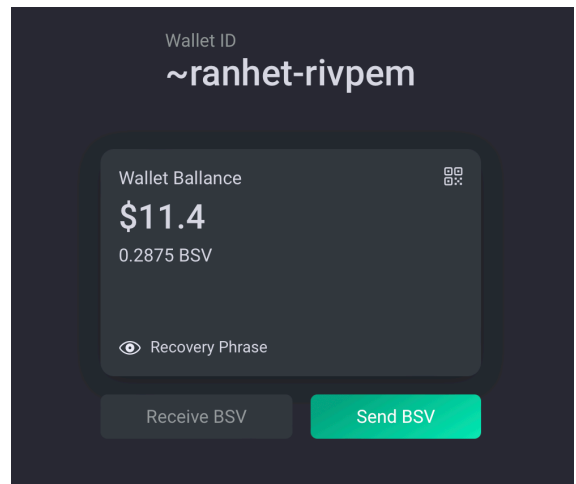
## LMSR-BASED SMART CONTRACT MARKET MAKER

Our LMSR-based smart contract market maker forms the backbone of our prediction market. Implementing the LMSR in a smart contract allowed us to automate the market maker function and reduce the risk of manipulation.

We developed and released the LMSR-based market maker smart contracts alongside an extensive TypeScript library for interacting and deploying them. This library, available for use by developers, forms the core for creating and trading in decentralized prediction markets on our platform.

## DEVELOPMENT OF NON-CUSTODIAL BITCOIN WALLET

For our platform, it was crucial to provide users with a secure, privacy-preserving method of interacting with our prediction markets. We achieved this by developing and releasing a non-custodial Bitcoin wallet. Rather than relying on traditional authentication methods, we incorporated zero-knowledge proofs for accessing users' encrypted



Vala.ai Wallet

backups. This innovative solution minimizes required trust and bolsters security, making the wallet more resilient against attacks and unauthorized access.

## **DEVELOPMENT OF PREDICTION MARKET PLATFORM**

To cap off our development efforts, we designed and deployed a comprehensive prediction market platform. Our platform's design and deployment were centered around the principle of trustlessness: our backend server only serves as an indexing service, while all trading and market logic happens on the client-side, using our library.

This approach ensures that users retain complete control over their funds and trades. The platform is intuitive, facilitating easy creation of markets, placements of bets, and rewards distributions. Through our development efforts, we have created a user-friendly, open, and secure platform for decentralized prediction markets.

## **PUBLIC RELATIONS AND OUTREACH**

Throughout the project, we maintained an active engagement with the public and our user community. Aiming to foster transparency and assist users in navigating our platform, we launched detailed documentation available at [docs.vala.ai](https://docs.vala.ai). Alongside this, we kickstarted a technical blog ([blog.vala.ai](https://blog.vala.ai)) where we publish articles detailing our tools and methodologies. To ensure maximum reach and interaction, we advertised our platform and shared updates predominantly on Twitter. This multi-pronged outreach strategy helped us garner attention, foster trust, and maintain an



open dialogue with our users and the broader community. Additionally, a Telegram group was created to provide support and a room for discussions.

# BETA RELEASE AND RESULTS

We rolled out our Beta version in September 2022, offering a valuable opportunity to test our platform in a live environment and garner real-time feedback. The Beta test period was both illuminating and constructive, during which users created 56 different markets, made 1184 trades, registered 20 different oracles, and accumulated a total of 168 users who signed up and created wallets. The platform processed 1297 transactions, amounting to an estimated 75 MB in total.

The feedback we received was overwhelmingly positive, with users appreciating the platform's intuitive interface and efficient performance. Our approach of minimizing centralization significantly lowered resource consumption, allowing us to operate everything on a cost-effective \$10/month virtual private server (VPS).

However, the Beta testing phase wasn't without challenges. We encountered and resolved several technical problems, including a critical vulnerability in our smart contract code that was promptly disclosed and quickly fixed, ensuring no funds were lost. Fortunately, there were no instances of oracles providing false information, indicating that technical risks may be more significant than those associated with oracle trust.

Several key insights emerged from the Beta phase. User feedback revealed that while decentralization is a crucial feature, it isn't a primary concern for most users. We found that even slight increases in complexity can lead to considerable confusion and problems for users, highlighting the importance of simplicity as a primary goal for platforms like ours.

We also discovered that, despite offering a promising technical foundation, the barriers to using Bitcoin SV are currently too high to justify its use for a platform like ours, at least for the present. The development effort required was significantly greater than expected, providing valuable insight for future resource planning and technical decisions.

This Beta release and the lessons learned have been instrumental in shaping our future strategies and have provided a firm foundation for our next stages of platform development. We look forward to implementing these insights to deliver an even better prediction market platform to our users.

# CONCLUSION AND FUTURE DIRECTIONS

Reflecting on our project, we are pleased with the results and the invaluable lessons learned, which have significantly shaped our understanding and planning for future endeavors. We have identified key areas of improvement that will guide our next steps in developing decentralized prediction markets.

The need for users to own Bitcoin SV (BSV) emerged as a major limitation, primarily due to its restricted ecosystem. Future projects will aim to be more inclusive, potentially integrating more universally accessible options like USD, rather than being bound to specific, smaller blockchains. This adjustment should broaden our user base and increase our platform's accessibility.

One area we are keen to explore is the removal of the centralized transaction indexer. There are promising advancements in this domain that could significantly enhance the decentralization and resilience of our platform.

We anticipate the ease of implementing smart contracts and their reliability to improve substantially in the future. Such improvements will simplify the development process and further strengthen the robustness of our platform.

Proof of work will also be explored as a mechanism for value exchange and a verifiable commitment to reputation. We are even considering the development of prediction markets without the dependency on blockchain technology, pushing the boundaries of current paradigms.

Overall, despite the challenges encountered, we consider the project a success. It has enriched our knowledge, honed our skills, and provided insights that have shaped our vision for future projects. Our commitment to evolving prediction markets remains strong, and we look forward to incorporating these lessons into our future work.