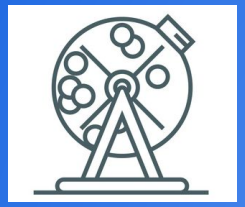


The Open Source Cardano Lottery

Fundraising for Green and Social Good Projects on Cardano

Fund 9 Proposal on Ideascale: https://cardano.ideascale.com/c/idea/415197
GitHub Repository: https://github.com/lley154/cardano-lottery

The Problem

Cardano Green and Social Good projects need alternative fundraising options and the Cardano ecosystem needs more high quality open source projects.

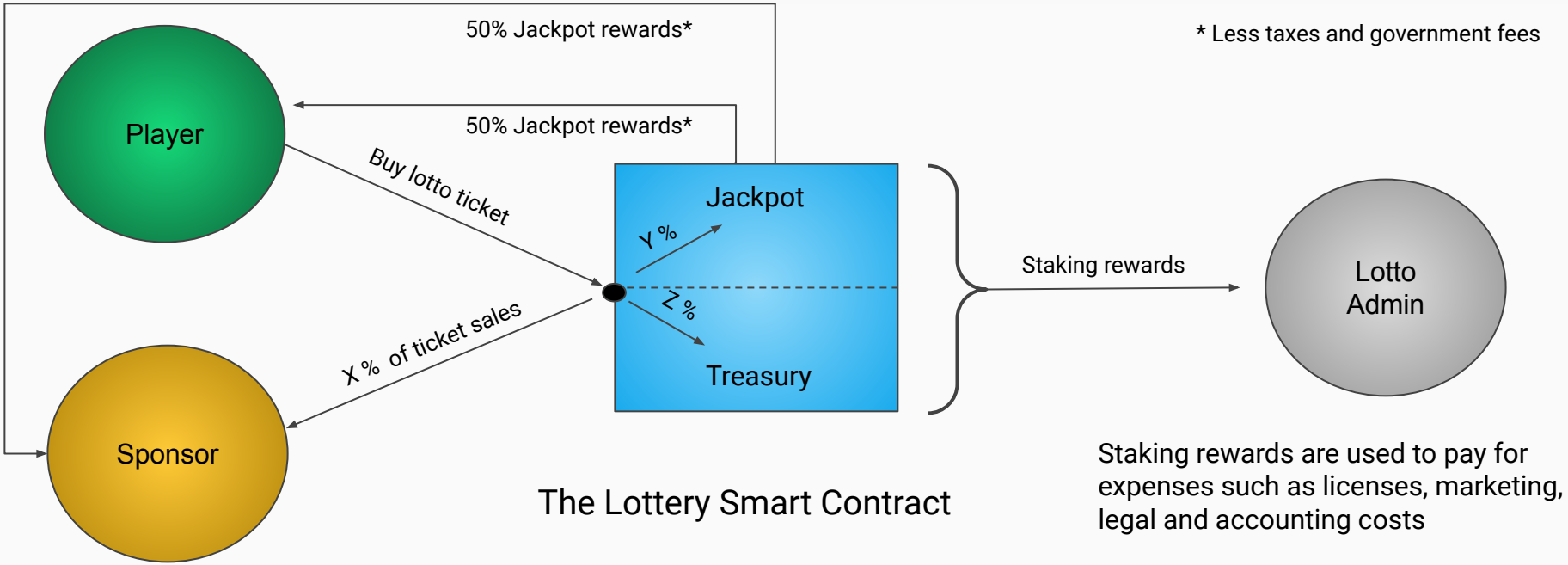
The Solution

Continue to build out The Open Source Cardano Lottery for fundraising of Green and Social Good Cardano projects.

The Lottery uses a novel approach by making it entirely decentralized and only using blockchain smart contract interactions. This trustless model does not require “trusting” the lotto admin (or a 3rd party Oracle) to run and operate the lottery.

All code is open source which contributes to the Cardano open source community.

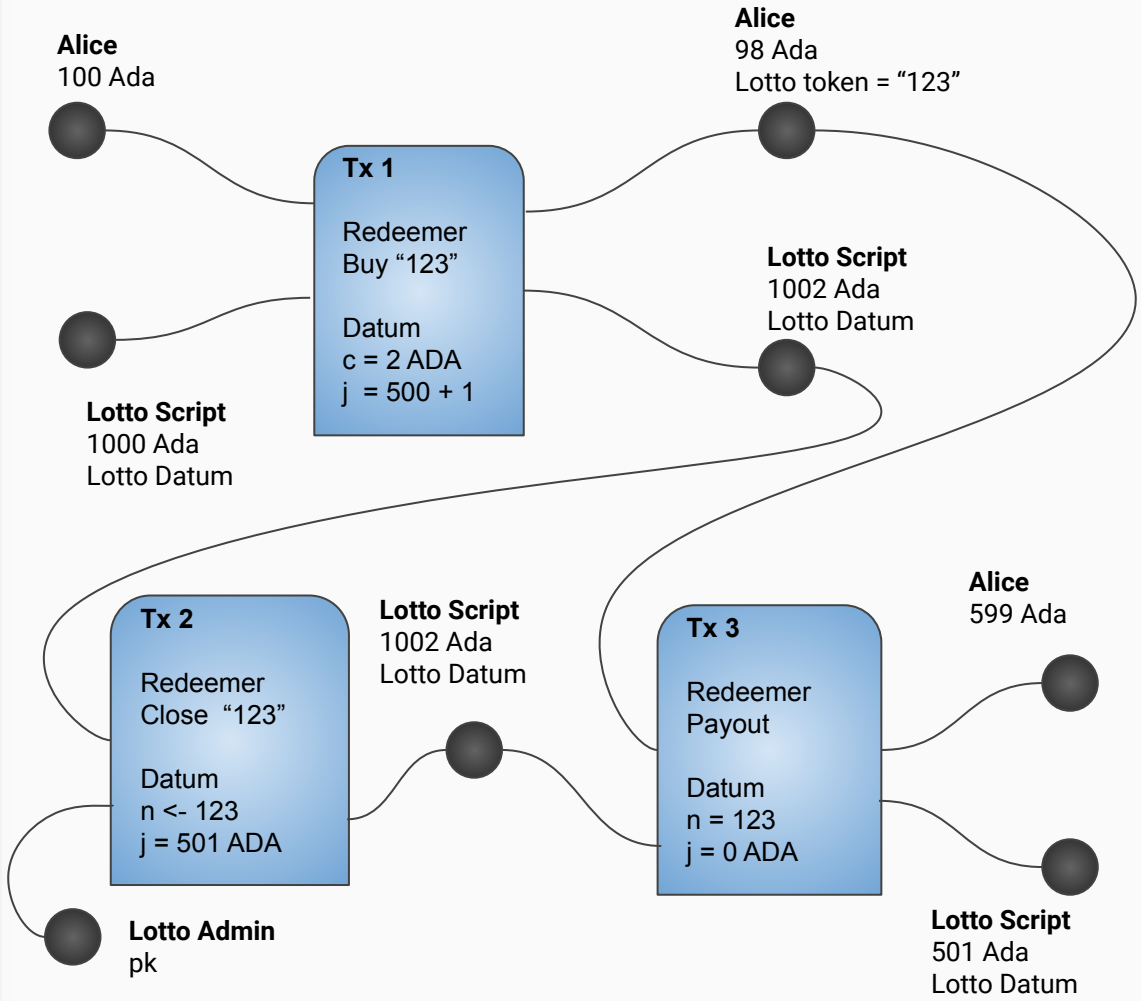
How it works


50% Jackpot rewards*
* Less taxes and government fees
Player
50% Jackpot rewards*
Buy lotto ticket
Jackpot
Y %
Z %
Treasury
Staking rewards
Lotto Admin
X % of ticket sales
Sponsor
The Lottery Smart Contract
Staking rewards are used to pay for expenses such as licenses, marketing, legal and accounting costs

Blockchain Technology

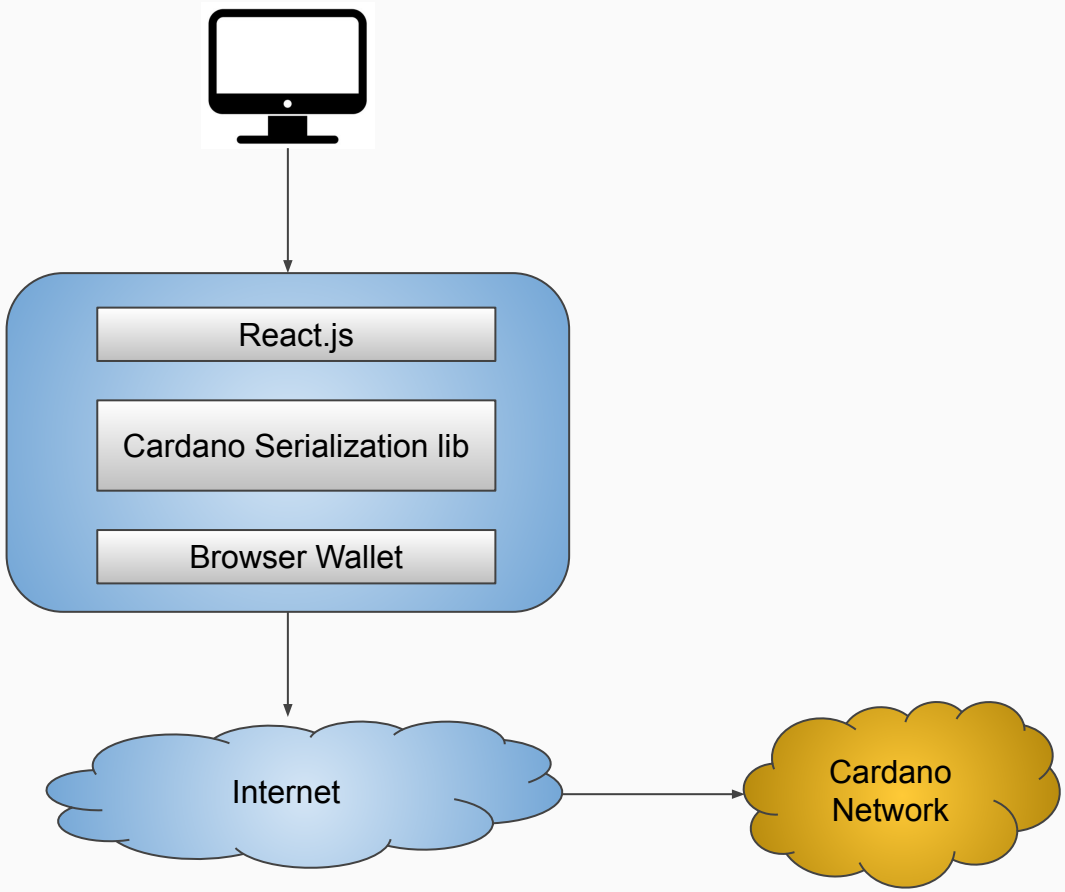
This is a simplified diagram that shows some of the transactions involved during a lottery cycle

Lotto Datum
{ admin public key pk,
ticket cost c,
winning number n,
jackpot j,
treasury t,
...
}



Technology Stack

For the MVP 0.2.0 Beta release, browser wallet integration will be the primary user interface for interacting with the lottery.



Milestones

The journey ahead

KPIs

Key Performance Indicators

Completed Items (0.1.0 Beta Release on May 6, 2022)

- Working state machine code
- Logic splitting between 2 validators by using thread tokens for communication
- PAB created from bash shell scripts
- Performance enhancements to fit the plutus code within the max 16KB TX size limits
- Documentation and video tutorials

Current Positive Impact as of June 10th, 2022

- 1000+ Github pageviews
- 150+ Unique visitors
- 150+ clones, 30+ unique clones
- 8 stars
- 4 forks

Target for year end 2022

- Beta 0.2.0 released
- 3 pilot lotto sponsors identified
- 10,000+ Github pageviews
- 1,500+ unique visitors
- 1,500+ clones, 300+ unique clones

Lottery Roadmap

Future Roadmap Items

- Mobile app integration
- Governance model/contract that allows for changing of the lotto parameters
- Multi-player winners
- Jackpot sweeteners (eg adding NFT and/or custom currencies)

Project Risks

Technical Risks

Exceeding Plutus Script size limits

- Mitigation: Leverage Plutus V2 and CIP-33 (Reference scripts)

Vulnerabilities / Loss of funds

- Mitigation: Engage with the developer community to review the open source code and obtain feedback from the beta releases

Legal and Regulatory Risks

- Mitigation: The production launch of a Cardano blockchain lottery will be done by a separate legal entity with a gaming license in an appropriate jurisdiction

Funding

The amount of funding requested for the Beta 0.2.0 release to create an MVP is $29,750

Developer rate is $85 / hr

Task	Resource	Effort	Cost
Browser wallet integration	Developer	80 hrs	$6,800
Plutus V2 updates and code refactoring	Developer	60 hrs	$5,100
Random number generator using player based entropy	Developer	100 hrs	$8,500
Staking rewards of Ada locked at the lotto contract	Developer	20 hrs	$1,700
Automated & property based testing	Developer	40 hrs	$3,400
Integration testing and user acceptance testing	Developer	40 hrs	$3,400
Documentation and video tutorials	Developer	10 hrs	$850
Total		**350 hrs**	**$29,750**

The Proposer

Lawrence Ley

- 20+ yrs in application development
- Founder and developer of The Open Source Cardano Lottery
- Computer Science degree from University of Toronto
- Plutus pioneer 2nd cohort
- Crypto and open source enthusiast
- Linkedin Profile: https://www.linkedin.com/in/lawrenceley/

Appendix

Detailed Design

Lottery Detailed Design

- When a player purchases a lotto ticket, they will receive a lottery token with the token name being the hash of the number they have selected
- After the required amount of tickets have been purchased*, the lotto admin closes the lottery so no more lottery tickets can be purchased
- The players then reveal their numbers which is used to seed the random number generator
- When ½ of the purchased tickets** have been revealed, the lotto admin can then draw the winning numbers. The random winning number uses both the previous transaction id and the sum total of the revealed numbers as inputs.
- To claim a winning ticket, a player will then redeem their token which is a hash of the winning number
- 50% of jackpot rewards will go to the winner (less taxes and government fees) and the remaining jackpot will go to the sponsor
- For every ticket purchased (configurable)
- 40% goes to the current lottery cycle jackpot
- 40% goes to the lottery treasury
- 20% goes to the sponsor
- The lottery contract staking rewards goes to the lotto admin

* The number of tickets that need to be purchased must be an amount that is greater than the total value locked into the lotto smart contract. This is to disincentivize the lotto admin from purchasing all the tickets in a lottery cycle which they could then use to predict the winning number in advance.

** We need to ensure there is sufficient entropy for the random number generator by requiring ½ of all tickets purchased in a current lottery cycle to be revealed. This will also prevent the lotto admin from drawing the winning numbers with only a small number of revealed numbers which he could then use to predict the winning number in advance.