

The Price is Right dApp

Chris MacKenzie, Ian Taylor, Derek McCracken, Tony Phan

CS458: Blockchain Principles and Applications

Computer Science Department, Colorado State University

Abstract:

To gain experience with implementing a decentralized application using smart contracts, we created our own ERC20 coin and built a betting application with a clean user interface that is based on the popular game show “The Price is Right”. To add value to our coin, our project links with Metamask where users can deposit Ether to be exchanged for PriceCoin, our native token. The application itself generates a random number between 1 and 100 and the user bets on a range the number is within (or the exact number if the individual is feeling lucky). Based on the leeway the user chooses, the payout changes (the lower the leeway, the higher the payout). This betting application will be easy to understand and use, as well as safe and secure. Users will be able to play a fun game and win cryptocurrency if they are lucky.

Introduction:

This project will attempt to take advantage of the large, growing demand for cryptocurrency betting games. There are already thousands of dApps out there that replicate Blackjack, Poker, Roulette and other popular casino games. This project will instead utilize ideas from the popular show “The Price is Right” to make a unique and fun gambling game. The goal of this project is to allow users to guess a number in a range, and if they guess the correct number or close to the correct number, they win! In this sense, it is similar to “The Price is Right” because the original game show has a player guess how much an item costs, and if they are closest (without going over) they win the prize. Our game will be slightly less complex, and only

involves the user guessing a random number in a preset range of numbers known to the user. In addition, there will not be other players competing against each other, just one player versus the computer. The user will also have a bit of leeway with their guess, picked by the user (explained further in depth in the results section). Aside from the application itself, this project will also focus on creating an ERC20 coin (PriceCoin) where users can trade Ether to interact with our contract. By linking our contract to Metamask, our goal was to add value to PriceCoin and allow users to get their ether back at any point. Our group believes that this can be a fun way to interact with blockchain technologies.

Background:

International regulators began recognizing online crypto betting applications around the year 2014. There are a variety of other betting applications currently on the market that allow users to gamble using cryptocurrencies. As laws surrounding these applications are an ever-changing landscape, the applications are primarily web apps run in the browser and can be added to the home screen of a mobile device running any mobile OS, and are not available in the App stores. Many crypto casino apps are still developed using Adobe Flash, limiting the number of available applications for mobile devices, though many sports betting apps are available. A majority of these applications suffer from the same interoperability issues of other apps in that they only allow users to wager a single type of cryptocurrency. However, there are some that offer the ability to gamble a few of the most prominent cryptocurrencies.

Results:

This project used a Solidity contract with a typical HTML and JavaScript frontend for the web GUI. The web GUI allows the user to choose options for their bet, guess their number, and then place the bet. Options for the bet include leeway and amount to bet. The random number will always be an integer within the range 1 to 100. Without leeway, there will always be a 1%

chance to guess the correct number. Leeway allows the user to get close to the number and still win. However, adjusting this leeway will reduce the payout if the user does end up winning. The leeway will also include a wraparound. For example, if a leeway of 5 is chosen that means that any guess that is within 5 of the true number will be considered a win. So, if the true number is 17 and the user's guess is 12, the user will win with a leeway of 5. The user would also win with a guess of 22 with a leeway of 5 and true number of 17. Wraparound is the idea that the number 100 comes right before the number 1 for the guessing. Wraparound exists to not dissuade the user from guessing very low or very high numbers in the range. For example, with a guess of 99 and a true number of 4, wraparound would mean that the user would win with a leeway of 5. This is because there are only 5 numbers between 99 and 4 with a wraparound: 100, 1, 2, 3, 4. With this idea in place, users will be able to freely guess high or low numbers in the range without being unintentionally penalized.

The application allows the user to select the value of their guess and the amount of leeway with which they would like to place their wager via sliders. There is an input box to input the amount of the wager. The app then displays the range of numbers that is covered with the leeway based on the input guess of the user. Also displayed are the odds of winning, simply calculated based on the amount of numbers covered by the range out of 100, the actual winning odds, and the amount the user stands to win if their guess is correct. The number the user is intended to guess is generated using the keccak256 hashing function using block timestamps, the user's address, and a nonce. Since blockchains are developed to be deterministic, however, this still does not ensure truly random number generation and is a limitation of our project. To ensure that users don't perform any re-entry attacks on our contract, we remove the bet amount that the user chooses from their balances before the random number is generated and reimburse this amount in addition to the payout if they win.

The development blockchain for this project was created using Truffle, which allows us to generate a minute local Ethereum blockchain on our device operating on the port 9545. Along

with the ability to utilize the blockchain, Truffle provides developers with several wallets, loaded with Ether to facilitate the development process. Truffle's unique environment allows for quick compilation and migration of Solidity bytecode to the local network. Locally hosting our blockchain also meant that we could import the network to wallet applications such as MetaMask, allowing developers to interact with the contract as consumers would.

The contract fully interacts with MetaMask and gives the user the ability to exchange their Ethereum for PriceCoin (PRC), which is the currency used to play the game. The contract also allows the exchange from PriceCoin back to Ethereum when the user is done playing and wishes to cash out. An issue with cashing out, however, is that by linking our coin with MetaMask, the value of the PriceCoin is determined by the amount of Ether that is traded in. If no Ether is traded in for PriceCoin, there is no value in the coin and MetaMask declines any transactions (essentially preventing printing money). When users begin adding Ether to the system, PriceCoin gains value and can payout users (up to the collective amount of Ether put into the system. With this collective amount of Ether creating value for PriceCoin, it is possible for a user to win big and take all of the Ether out of the system (forcing everyone else to hold PRC until more Ether is added in). With this problem, we designed the maximum leeway range so the user has a 49/51 chance so the contract makes profit in the long term. Normally the owner of the contract would have to supply an initial amount of Ether to add value to the coin and be responsible for paying out the users but we decided to go with the current approach for simplicity.

Conclusion:

Currently, the application is limited due to the fact that a real world deployment of a betting application would require a great deal of capital in order to pay out winnings to the bettors. Another limitation of the current setup of the project is the constant conversion to the proprietary 'PriceCoin' instead of monitoring the current trading price of Ethereum and adjusting

the conversion rate accordingly. In order to increase the number of users in a real-world deployment, the application could allow for multiple cryptocurrencies to be converted to the game's coin, which would require the monitoring of multiple market prices depending on the currencies allowed.

References:

Draper, A. (2022, April 27). *Best crypto betting sites USA - bet with Bitcoin, Dogecoin & more.*

The Sports Daily. Retrieved April 29, 2022, from <https://thesportsdaily.com/crypto-betting/>

How cryptocurrency casinos are redefining online gambling. NewsBTC. (2022, April 27).

Retrieved April 29, 2022, from

<https://www.newsbtc.com/sponsored/how-cryptocurrency-casinos-are-redefining-online-gambling/>