Lotto Whitepaper

Brian Bigdelle

October 2019

1 Abstract

In this paper, we present a thought experiment of a lottery built on blockchain technology using a game called Lotto. Coins can be thought of as lottery "tickets" that can be sold between users or mined that only have value to the current game. The lottery ends when a randomly decided number of blocks are mined, successful mining rewards the miner with a random number of coins as well. A main, "Master", blockchain holds the transaction history of every completed game. A temporary blockchain holds the transaction data for the current game. When the current game ends, the temporary blockchain is appended to the end of the Master blockchain and a new temporary ledger is born.

We make no assumptions on the readers technical knowledge and provide a cursory overview of key terms in order to understand Lotto.

2 Technical Background to the Blockchain

Since Bitcoin's explosion in popularity, there is significant interest in technologies developed on the blockchain. There are countless reasons for the widespread adoption of blockchain technologies, from decentralization to anonymity between users. In the context of crypto currency, the blockchain is a digital receipt that accounts for every transaction ever made for the particular crypto. The notion of decentralization comes from the verification of these transactions. Unlike a traditional banking system, where the bank verifies that these transactions are not fraudulent, cryptocurrency relies on the public to verify the legitimacy of the blocks. There are numerous resources that provide lectures on the subject of mining so I will provide only a cursory overview. Every user of a particular crypto protocol must have a wallet in order to send or receive money. This wallet is known to the world by a public key, and private to the user is a private key that allows for verification of a transaction. A transaction between User A and B is packaged digitally as a potential block to add to the blockchain that contains some history of the block before it, the transaction details, and a "hash" that is made with the public and private keys of both users in the transaction. The hash can be thought of as a black box, where a string goes into the box, and a same length string exits the box. The hash function is deterministic, but small changes in the input result in drastic changes in the output. Verifying a block is a game of guessing the string, called a nonce, that is further hashed with the private and public keys that will result in a hashed output string that is less than the current hashed output string. For example, say that an unconfirmed block has a 32 bit hash, the goal of a miner is to find a value called a nonce that can be hashed with the 32 bit hash that gives a value less than that hash. This is done by guessing until the nonce is found, once found, the miner broadcasts to other miners and they can quickly perform the hash themselves to verify. The prize for all this hard work is a known number of coins.

3 Lotto Description

Lotto is designed to function as the first true crypto lottery. Every transaction block contains a timestamp, the hash ... ... and a game iteration ID. This represents the number lottery we are currently on. Coins are associated with a game ID that is specific to the game they were mined during. Every game has has a random lifespan that consists of an unknown number of coins allowed to be mined. If the number of coins mines hits or exceeds that number, the game ends. The blockchain network is comprised of two chains, one master blockchain with all completed game transactions and one temporary chain that begins with a genesis block and holds transaction data until the game ends. Once the game ends, the temporary chain is added to the master blockchain.

4 Technical Background to Lotto

In every other cryptocurrency at the time of this writing, the prize is a fixed number of coins that is known to the entire network. The worth of the coins may fluctuate but the reward is consistent. Note that some cryptocurrencies have rewards that inversely scale with the number of existing coins so that there is a limited supply. In Lotto, the reward for the coins is random in accordance to a block independent, identically distributed (i.i.d) distribution that is strictly positive. Note that we only deal with positive coins, there is no penalty for mining that is represented in negative rewards. Each Lotto game begins with the verification of 1 genesis block going to a holding wallet. Users only need to check transactions on the current game iteration which marks a significant scalability improvement over traditional cryptocurrencies with blockchains of multiple gigabytes.

5 Scalability

The key issue facing blockchain technologies is scalability. As more users participate in the blockchain, transaction volume increases and more blocks are added to the chain. This increases the time needed to verify a transaction. With Lotto, this issue is largely mitigated by only relying on the most current iteration of the game. This significantly drops the transactions the must be verified in order to process a new transaction. When a game ends, this GAME CHAIN is added to the end of the MASTER CHAIN. All transactions on the master chain are largely irrelevant. This echoes a traditional lottery where tickets from old lotteries have no value.

6 How does the game end?

When a game begins, a genesis block is mined in order to kick the game off. A hash is created using a combination of the miners private and public keys, the game ID, and the time of the week in seconds. Every block on this game is stamped with this hash, it is public to the entire network. We will refer to it as the GAME HASH.
When a new block is mined after the genesis block, another hash is created that is a combination of the hash of the previous block with the hash created by the public and private keys of the miner who successfully mined. If this hash is less than the GAME HASH, then the game ends. If it is not, then the game continues and every subsequent block is hashed with the hash of all the previous blocks in order to compute a new hash and compare it to the GAME HASH. When the CURRENT HASH is less than the GAME HASH, the game ends.

In pseudo code:

```
CURR_HASH = Void;
GAME_HASH = Void;

i = 0;

WHILE GAME_HASH > CURR_HASH:
    IF i == 0:
        GAME_HASH = HASH(MINER_PUBLIC + MINER_PRIVATE + TIME_OF_WEEK)
    END
    i = i+1;
    BLOCK_HASH = SUCCESSFUL_MINER_ID;
    CURR_HASH = HASH(BLOCK_HASH+CURR_HASH);
END
```

7 Proposed Technical Approach

7.1 Block-chain development

There are two courses of action (COAs) that stand out to us for development of Lotto.

1. Develop coin on new block-chain.

2. Develop token on existing block-chain.

The choice in COA comes down to differences in philosophy. We view Lotto as a functionality enabled by an existing block-chain and therefore decide to use COA 2.

7.2 ERC20 Compliance

Our proposed solution is to build Lotto as an ERC20 compliant token on the ethereum blockchain. The choice of ethereum over any other existing block-chain is mainly due to the existence of the Ethereum Virtual Machine. The EVM provides a natural and intuitive platform on which to build Lotto by providing a pool of miners to verify transactions and keep the Lotto block-chain healthy.

7.3 Token Mining

The drawback of using an existing block-chain is that mining becomes less straightforward than on a dedicated block-chain. Lotto lives on ethereum and therefore all Lotto blocks are processed by the EVM by an ethereum miner, giving ether as a reward to the successful miner. The miner may or may not be involved in Lotto and therefore there is no notion of a ”Lotto reward” from successful mining. Miners in the pool who help verify transactions are incentivized by ”gas” which is the cost of verification that sellers give to verifiers as a thank-you for verifying their transaction.

Users who hold Lotto cannot directly mine more Lotto, however they can do the following to stake money for a random number of tickets. A Lotto holder can chose to ”burn” some of his LottoCoin, say 100 at a time, with the associated gas fee. The EVM allows for a smart contract that can reward the user with a random number of LottoCoin. The gas fee is then paid to the EVM in order for the transaction to be verified. The user can only burn fixed denominations of LottoCoin in order to keep the game fair. This way all users, regardless of how many tickets they hold, stake the same amount of gas in order to verify the transaction. Burning 1000 LottoCoin is not a way to save the gas fees associated with burning 100 LottoCoin 10 separate times. This also gaurantees that the blockchain remain healthy since the LottoCoin gambler is paying for his own verification. This is also provides LottoCoin an inherent value is supported by the price of gas.

8 Game Economics

An essential aspect of Lotto Coin comes with the monetary value that it holds. The game is dependent on unpredictability and inherent instability. Since after each iteration of the game ends, the coin resets in value, it is the role of the holder of a coin to try to sell at the moment before the game crashes, before the value of his coin is lost. This value is based on the energy requirements needed to mine, and the random reward for mining. Once a miner is rewarded, he can take his given coins and sell at a price that reflects a profit on the energy that he used for those coins. At this point, the coin fluctuates in value based on the degree of the reward of future mining, speculation of the game's end time, and demand for Lotto Coin.

While some criticisms of cryptocurrency is the instability that many have displayed since its creation, Lotto Coin is built on this volatile nature.