CoinBlock – Colored coins for real time prediction markets and decentralized decision making

http://coinblock.org

Abstract

CoinBlock is a protocol which enables anyone to issue digital assets on top of Bitcoin, Litecoin or any other compatible blockchain. CoinBlock colored coin assets are issued by publishing a "game definition" which specifies the behavior & properties of the asset. CoinBlock assets have a wide variety of applications such as implementing strategy games, prediction markets or for representing company ownership & handling organizational decision making. To view a CoinBlock asset, anyone can simply install the underlying blockchain, install the open source CoinBlock web application and import the game definition.

Events

CoinBlock is designed around the concept of events in which coinholders can cast votes by transferring their coins to addresses matching a specified format. Once all blocks for an event have been mined, the event completes and one option is determined as the winning option for that event. New coins are created according to the inflation scheme specified in the game definition and these new coins are distributed to everyone who voted correctly, in proportion to the quantity of their correct votes.

Voting Options

CoinBlock events generally include two or more voting options. Each option has the possibility of becoming the winning option for its event. One voting address format is associated with each voting option in an event.

Address Scheme

To achieve compatibility with a wide variety of blockchains, CoinBlock uses standard pay to pubkey hash (P2PKH) transactions for voting. Users can get voting addresses through vanity generation, a process where addresses are randomly generated until an address is found matching the format of the desired voting option. A "voting identifier" of between 1 and 6 characters in length is extracted from each address. CoinBlock's address scheme then maps this voting identifier to an option_index (positive integer) which is temporarily associated to voting options for transactions confirmed during the blocks of the associated event. Some addresses do not match a voting identifier and are therefore non-voting addresses. Currently, the CoinBlock web application implements a single, protocol level address scheme. This scheme is based on the base58 addresses used in Bitcoin and similar cryptocurrencies. This address scheme supports 679,798,074 voting address formats. 26 of these are single character formats, 16*58 are two-character formats, 8*58^2 are three character formats etc and 1*58^5 are 6 character formats.

Voting Transactions

Each event runs for range of blocks determined in the game definition. Voting transactions must be confirmed within these blocks in order to be included in the event. Additionally, transactions from the underlying blockchain are only considered to be voting transactions if they spend colored coins and if they include outputs made to voting addresses.

Votes may be defined in several different ways. In the case of an asset used to represent company ownership, votes may defined simply as the total number of coins that a user can demonstrate ownership of. For example, company shareholders could vote on hiring/firing decisions by moving colored coins between their own addresses. In the case of a strategy game or prediction market, votes may be defined as a "coin days destroyed" or "coin blocks" in which case votes are proportional to coin age.

Event Winning Rules

Once an event is completed, a winning option is determined and each CoinBlock node creates new colored coin UTXOs of the correct amount at each address which was used to cast a vote for the winning option. Several different event winning rules may be used depending on the desired application. Some event rules may be implemented in a fully decentralized manner while others require centralization. Several event winning rules are:

- Max votes under cap wins – In this rule, a voting cap such as 25% or 60% is specified for an event. In general, the voting option with the most votes is declared the winner. But to prevent one option from winning with an overwhelming majority of the votes, a cap is instituted and any option above the cap is disqualified. Because the winner is determined entirely by on-chain events, this rule does not require any centralization.
- Winner determined by oracle – For this rule, an individual or URL determines the winner of an event. This rule requires some centralization; for all Coinblock nodes to remain in sync, all nodes must agree on the winner for every event.

Game Starting Block

In order to identify all movement of colored coins and to check for voting transactions, the underlying blockchain must be run as a full node. This is accomplished by adding "txindex=1" to the configuration file for bitcoin-derived blockchains. The CoinBlock web application communicates with the underlying blockchain by making RPC calls but also maintains its own copy of the blockchain in an indexed SQL database, to enable performant querying of the blockchain. To allow CoinBlock assets to be issued at any time, CoinBlock game definitions include a "game starting block". CoinBlock nodes running that game are not required to process transactions included in blocks prior to the game starting block.

Genesis Transaction & Genesis Amount

To issue a new asset, a transaction on the underlying blockchain is defined as the genesis transaction for the new colored coin. The hash of the genesis transaction and the amount of colored coins created by that genesis transaction are specified in the game definition.

Buy-in Policies

Some colored coin assets may be defined so that coins are only created through the genesis transaction. Such assets may be said to have no buy-in policy and the value of assets defined in this way would be expected to fluctuate based entirely on their demand (since there is zero inflation and no supply). However, other assets may be defined with a buy-in policy such as having a game-wide buy-in cap or having unlimited buy-ins. For games with such a buy-in policy, users can send coins of the underlying blockchain into an escrow address. In exchange, new colored coins are created and sent to the address specified in the buy-in transaction. For games with unlimited buy-ins, colored coins may be understood to derive their value from the escrowed coins. In this case, there may be a fixed exchange rate between colored coins and the coins of the underlying blockchain.

Escrow Addresses

For assets employing centralized event winning rules or for assets which use a buy-in policy and run on top of existing blockchains such as Litecoin or Bitcoin, full decentralization is not possible. To facilitate buy-ins, an escrow address is specified in the game definition. Colored coins may be created by sending underlying blockchain coins to the escrow address and similarly colored coins may be removed from circulation by sending colored backs to the escrow address. When colored coins are destroyed in this way, the escrow administrator(s) must refund underlying blockchain coins to the sender by signing a transaction to the sender with coins equivalent to the value of the destroyed colored coins.

Vote Effectiveness Functions

In some CoinBlock applications such as real time prediction markets, counting votes equally across all blocks of a round gives players an incentive to avoid voting early in the round and instead waiting until near the end of the round to vote, when it's easy to predict the outcome of the event. To mitigate this problem, game definitions may specify a vote effectiveness function which assigns an effectiveness factor to each block of the round. This means that players who vote early in the round are credited for a higher number of votes and therefore receive a higher payout than players who vote late in the round. Currently CoinBlock supports two vote effectiveness functions:

- constant - votes are counted equally throughout each event.
- linear decrease – votes counts for 100% in the first block of the round and decrease linearly until the final block of the round where votes count for 0%.

In games which employ a linearly decreasing vote effectiveness function, players have incentive to maximize their voting rewards by voting early in the game when their UTXOs will count for maximal votes. Players who vote late in the round are better able to predict the winning option but at the cost of being credited with fewer votes for their UTXOs and therefore receiving a smaller reward for their winning votes.

Custom Blockchain

A custom blockchain implementing the CoinBlock protocol may be able to eliminate the points of centralization as a described above. Some progress has been made on the development of a

fully decentralized CoinBlock blockchain under the "EmpireCoin" brand. EmpireCoin implements the "Max votes under cap wins" event winning rule and uses an empire theme in which one event is concluded every 10 blocks in which players can vote for any of 16 modern empires. On this blockchain, the empire with the most votes but under the 25% voting cap wins. This experimental blockchain faces several challenges. One is that miners may exclude all transactions except their own in order to keep all payouts for themselves. Selfish mining and excluding transactions to influence the outcome of a round also pose challenges.

Strategy Games

In events determined entirely by voting transactions, individuals may employ different voting strategies to maximize their voting payouts. For example players may vote for several voting options at random, vote for the same option in every round or write an algorithm which votes automatically based on an in-depth analysis of past events, current voting scores and other information sources. For some event types, knowledge of how others plan to vote may be beneficial, encouraging collaboration and collusion among voters. Players may outsource their voting decisions to an API that they write, or to an API controlled by a third party. Through such an API, a voter can give control of his or her voting decisions to a third party without giving up the private keys to his or her coins. By gaining control of the voting rights for a large amount of coins, syndicates or "voting pools" may develop which can achieve good returns for their members by influencing voting outcomes. Interactions between players, voting pools and mining pools who have some control over voting outcomes create endless possibilities for collaboration, & competition in strategy games which emulate real-world politics and empire building. Based on these game mechanics, many players may choose to join a voting pool rather than engaging in the time consuming process of analyzing the blockchain and communicating with others to inform their voting decisions. When players join, they can do research on the rates of return and reputation of the various voting pools in order to choose the best option. Competition among voting pools seeking to expand their influence by gaining the voting rights of many players is key to ensuring the fairness and integrity of the game.

Prediction Markets

CoinBlock's voting protocol is an ideal mechanism for implementing prediction markets. In CoinBlock real time prediction markets, players vote on questions such as "Will the US dollar go up or down vs the Euro by block 10080?" CoinBlock prediction markets are pari-mutuel and inflation-subsidized: users don't lose money if they vote incorrectly but they do win a small amount of coins by voting correctly.

Get Started

To get involved, please visit CoinBlock.org and sign up for a web wallet account. Or get a Litecoin or Bitcoin full node running, install CoinBlock yourself, import a game definition and start playing. Or to experiment with our custom blockchain, download and install EmpireCoin.

EmpireCoin Core: http://github.com/TeamEmpireCoin/EmpireCoin
EmpireCoin Web: http://github.com/TeamEmpireCoin/empirecoin-web