PolyCash

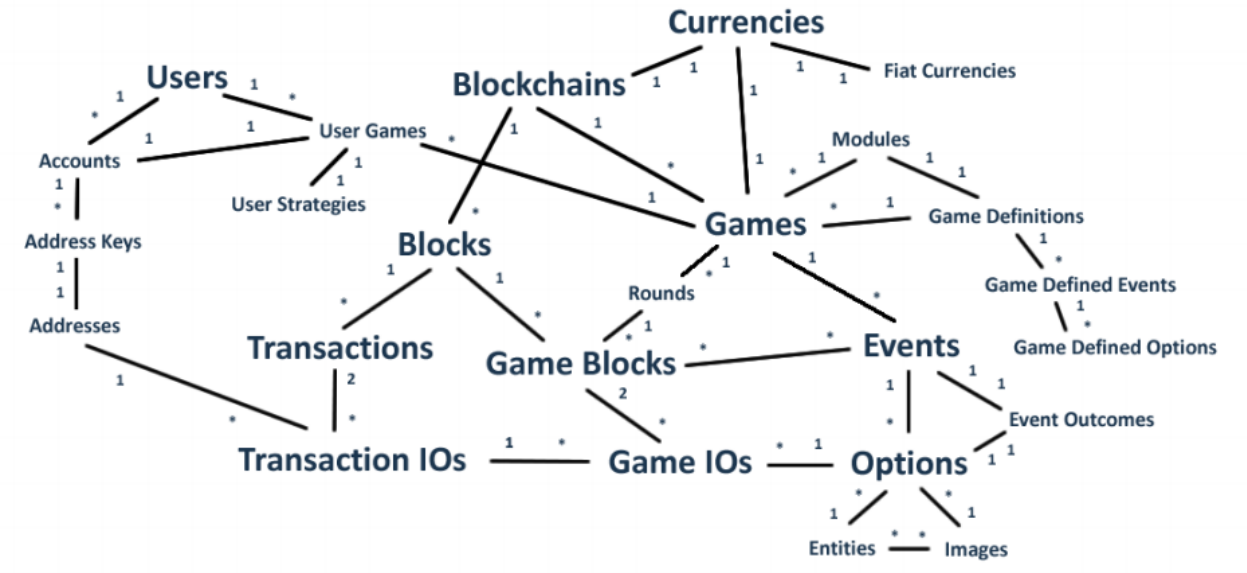
The ultimate protocol for the next generation of money

https://poly.cash

Introduction

PolyCash is a protocol which makes it easy to issue highly functional crypto assets without writing code. PolyCash is an implementation of the colored coins concept and allows anyone to issue second layer tokens on top of Bitcoin, Litecoin and other UTXO based blockchains. PolyCash is a tokenization solution and is ideal for launching crypto assets backed by tangible sources of value like commodities, real estate, intellectual property & financial assets. PolyCash serves as a virtualization layer for the blockchain and extends the functionality of Bitcoin with betting (prediction market) functionality. PolyCash is envisioned as a cornerstone for the alternative financial system and includes functionality for printing physical crypto cards. PolyCash is an open source web application which functions as a wallet and can be installed on your local computer or on a public facing server. The wide range of functionality provided by PolyCash makes this protocol ideal for launching games and PolyCash uses the term "game" to describe crypto assets (tokens). PolyCash has been developed by the PolyCash Foundation. The PolyCash Foundation continues to develop this technology while also using it to build a business for betting on sports, eSports & more.

Figure 1. A diagram showing the PolyCash schema.



Part 1. PolyCash as a token issuance protocol. Introducing the game definition.

PolyCash is a protocol which supports a wide variety of functionality. Some PolyCash-protocol crypto assets may be used to represent ownership of companies and to conduct shareholder votes while others are used for sports betting & other games. PolyCash supports this diversity by defining each crypto asset with a "game definition" also known as an "asset definition". The game definition is a JSON format text file containing all the parameters for a crypto asset. The game definition together with data from the underlying blockchain provides all the data needed to fully sync a crypto asset. To install a crypto asset you need to install the blockchain that it runs on, install PolyCash and then copy paste and import the game definition into PolyCash.

Ideally, a simple crypto asset's game definition may be defined when the asset is launched and then never changed. For assets incorporating prediction market events, the game definition often changes when PM events are added and resolved. When a base parameter for an asset is changed, the game is reloaded from the game's starting block. When a PM event is changed, the game is reloaded from the block where betting started for that event.

A list of the parameters that are included in each asset's game definition are described in section 5 of this paper.

Part 2. Peer to peer betting & PolyCash's approach to the oracle problem.

PolyCash-protocol crypto assets support pari-mutuel prediction markets by default. Pari-mutuel betting is betting where payments are pooled, and odds are calculated based on the amounts staked on each possible outcome. In pari-mutuel betting, odds and payouts are not fixed until all bets have been placed. This contrasts with fixed odds betting where the odds and payout for a bet are set when the bet is placed.

PolyCash enables betting on Bitcoin and similar blockchains using standard Pay-To-PubKey-Hash (P2PKH) transactions through an address scheme that associates each address to an integer called an "option index". Each PM event has starting and ending blocks specifying when bets can be placed and has a list of options representing possible outcomes for that event. Players place bets by burning coins to one of their own addresses matching the option index of the outcome that they want to bet on. Once the outcome for an event has been resolved, the protocol creates new coins equivalent to the quantity of coins burned in that event and deposits the new coins to UTXOs associated with winning bets. Betting transactions must be confirmed in the blocks associated with an event or else the coins will have been burned for nothing.

Projects aimed at creating unstoppable decentralized prediction markets based on distributed ledger technology (DLT) have attracted a great deal of public interest and funding. Examples include Augur, Gnosis, Bitcoin Hivemind (formerly Truthcoin), Delphi, Bodhi, Wagerr and Stox. Fully decentralized prediction markets are difficult to implement due to the unsolved challenge of perfectly integrating information about real world events into the blockchain without trusting any party. Even more difficult than the problem of resolving event outcomes is the challenge of ensuring that only well-defined and easily verifiable events are included.

Augur solves the oracle problem through crowd reporting and incentives which reward individuals for adhering to the group consensus. This approach is valid but relies on the Rep token being at least somewhat widely distributed among different parties to avoid collusion by a majority.

PolyCash provides a mechanism for reaching consensus but does not force nodes to be in consensus. Rather than trying to solve the oracle problem with incentives, PolyCash delegates the problem of maintaining consensus to the node operators. Each node operator is technically able to resolve events in any way that he or she chooses. When PolyCash nodes are not in consensus on a crypto asset, they can still transact with each other, but they will have different perceptions of the amounts of transactions. Node operators should disable trades & withdrawals when not in consensus. Nodes who allow trades or withdrawals while not in consensus or while using a game definition which is later changed run the risk of losing money or defrauding users.

The PolyCash application hashes the game definition for each installed asset and displays this hash publicly, allowing nodes to quickly check if they are in consensus with their peers. Conflicting nodes can easily identify their points of disagreement by comparing their respective game definitions. These differences must be resolved on each node by the node operator

Games should be designed with well-defined and easily verifiable events to avoid consensus problems. Whenever a new user sets up a node, she has incentive to join the majority consensus to make transacting with other users easier and to avoid time-consuming game reloads from resolving disputes about event outcomes. Rather than manually entering the outcome of each event, node operators can use APIs and other data sources to automatically set event outcomes.

Any individual or group attempting to promote an event outcome which doesn't match reality faces an uphill battle in convincing peer nodes to adopt the falsehood. Event outcomes can be changed by any node at any time in the future. This lack of finality means that there is no fixed date by which the falsehood can be locked in. This lack of finality and the psychology of groupthink should lead consensus to form around the truth.

Until prediction market events are resolved, UTXOs holding bets associated with those events are marked as unresolved. Prior to being resolved, these unresolved bets can be traded as individual units but should not be included in general transactions. In the case where unresolved bets are included in general transactions, they are valued at zero. If such a bet is eventually resolved as a winner, its amount gets changed from zero to its payout amount, providing unexpected gains to anyone holding UTXOs which derive from that transaction.

Part 3. Wallet functionality.

PolyCash includes wallet functions for sending and receiving PolyCash-protocol assets as well as native blockchain assets like Bitcoin and Litecoin. Unlike the original Bitcoin client, PolyCash shows each UTXO individually, allowing users to locate and perform operations on a specific UTXO. PolyCash also includes a user interface for betting as well as an explorer for viewing transactions, blocks and meta data associated with any installed blockchains.

Part 4. Physical crypto cards & decentralized exchange functionality.

PolyCash is designed to be a cornerstone for the alternative financial system. In addition to the functions described above, PolyCash also includes functionality for printing physical crypto cards. PolyCash makes giving someone coins as easy as giving them a business card. Using PolyCash, you can design prepaid crypto cards containing coins in the currency of your choice. All that's needed to create your own physical money is the PolyCash app, card stock paper, a printer and a paper cutter. To create cards, open your PolyCash wallet and deposit coins. Follow the wizard to create your cards, then download and print the PDFs and cut up your cards. For more secure cards, purchase scratch off stickers online and apply them to cover the secret keys on the back of your cards. These cards are prepaid bonds issued by you. Of course, it's possible to create "counterfeit" cards which look like they have money on them but don't, and therefore some level of trust is required between the buyer and seller of these cards. You can put your name & phone number on the back of your cards so that buyers can contact you if they have a problem redeeming their card.

Crypto cards allow PolyCash to function as a decentralized exchange: people can print crypto cards and exchange them for cash. We are also building orderbook functionality into PolyCash which will allow users to trade cryptocurrencies directly through the PolyCash web app.

Part 5. Detailed description of the parameters and concepts of PolyCash assets.

Reliance on full nodes

Colored coins can run on blockchains using SPV nodes. But PolyCash requires the use of full nodes. This design decision was made for efficient performance, based on the assumption that many games may be running on any blockchain. Be sure to add "txindex=1" to the configuration file when installing blockchains to be used with PolyCash. PolyCash communicates with the underlying blockchain by making RPC calls but also maintains its own copy of the blockchain in a relational database, for quickly running queries about blockchain data. Since PolyCash can access data from the underlying blockchain at any time via RPC calls, not all transactions from the underlying blockchain need to be loaded into the SQL database. To reduce loading time, each blockchain in PolyCash has a "first required block" parameter which is based on the minimum game starting block of all games running on that blockchain. PolyCash fully loads all transactions from the first required block of each blockchain going forward.

Inflation based on gamified proof-of-stake

PolyCash allows crypto assets to be created with a fixed supply or with an exponentially inflating supply. Inflation is seen as a negative trait of money. But when the money created by inflation is distributed fairly and transparently, inflation can be a fun element of gamification and can incentivize participation in prediction markets. In PolyCash assets with non-zero inflation, unrealized gains build up over time based on the size and age of UTXOs. Unrealized gains are realized whenever a UTXO is spent in a transaction associated with a PM event. Spending a UTXO in a non-betting transaction forfeits any unrealized gains associated with that UTXO. In inflationary games, players should regularly realize their unrealized gains by betting. Players who realize their gains regularly will on average experience a stepwise exponential increase in the quantity of their tokens. In comparison, players who don't realize their gains will only experience a linear increase in the quantity of their tokens. In these games, players

can grow their balances faster than inflation simply by performing better than average in inflation-subsidized prediction markets.

Environmental benefits of gamified proof-of-stake

Proof-of-work consumes an enormous amount of energy, which could have been reduced if Bitcoin had separated its security mechanism from its emission schedule. A version of PolyCash's gamified inflation functionality can be incorporated in a native blockchain to implement a cryptocurrency which separates its security mechanism from its emission schedule. In such a cryptocurrency, 25 coins could be paid out to proof of work miners every block. An additional 750 coins would be paid out to the coin holders by gamified proof of stake after every 10th block. By paying only one quarter of the currency to proof of work miners, this currency would reduce the amount of mining by three quarters, saving an equivalent amount of energy. In this blockchain, betting events are held one at a time in a series and the winning option is determined based entirely on transactions included in each event, according to the rules of that game. We include a description of this cryptocurrency in this paper because this was the initial idea which launched the PolyCash project. This version of gamified inflation has not been developed in a native blockchain but it's functionality can be simulated in PolyCash as a second layer token.

Benefits of blockchain agnosticism

By piggybacking on top of existing networks such as Bitcoin, PolyCash assets inherit the desirable properties of money provided by these networks including physical decentralization, censorship resistance, fungibility, durability, divisibility & portability. By remaining blockchain agnostic (compatible with many different blockchains), dependence on any blockchain or development team is minimized. Blockchain agnosticism allows token issuers to shop around between blockchains, putting asset issuers in a good position to choose blockchains with cheap on-chain transaction fees.

PolyCash's address scheme

To achieve compatibility with a wide variety of blockchains, PolyCash uses standard Pay-To-PubKey-Hash (P2PKH) transactions for betting transactions. Users can find betting addresses through vanity generation, a process where addresses are randomly generated until an address is found matching the desired option index. A "voting identifier" of between 1 and 6 characters in length is extracted from each address. PolyCash's address scheme then maps this voting identifier to an option index, an integer which associates an address to a betting option. PolyCash 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 option indices. 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.

Rounds

Rounds divide blocks in a game into consecutive groups and are defined by the "round_length" parameter of an asset. Setting inflation based on coin rounds destroyed rather than by coin blocks destroyed reduces inflation and reduces congestion on the blockchain by changing the incentives of players to bet once per round rather than once per block for inflationary assets.

Event winning rules

The PolyCash protocol allows events to be resolved in several different ways. The different ways that an event can be resolved are specified the "event winning rule" parameter of the game definition. Currently every event winning rule requires that exactly one option is determined as the winner but in the future the protocol may be modified to support situations where payouts are made to multiple options in an event. Currently, the following event winning rules are supported:

- Max votes under cap wins – This is a rule used for strategy games like the blockchain for environmentally friendly gamified proof of stake as described above. In this event winning rule, a voting cap such as 25% or 60% is specified for an event. The option with the most bets but not exceeding the voting cap is declared as the winner of the event.
- Virtual soccer match – This event winning rule was developed to demonstrate the virtual sports betting application of the PolyCash protocol. This event winning rule simulates a virtual soccer game, with each team having the possibility to score each time a block is mined, based on pseudo-random data derived from the block hash.
- Winner determined by game definition – This is the event rule used for prediction markets. Here the winning option is set based on the outcome of real-world events. This can be accomplished by pulling outcome results from peer nodes, by referencing APIs or by the node operator manually entering event outcomes.

Genesis transactions & genesis amounts

To create a new crypto asset, a blockchain transaction is specified as the genesis transaction for the new token. The genesis transaction hash and the quantity of tokens created by that genesis transaction are included in each assets game definition.

Escrow amounts

PolyCash crypto assets should be backed by tangible sources of value. PolyCash supports Tether-like functionality by allowing money in any currency to be specified as value sources in the game definition for a crypto asset. To indicate that a crypto asset is backed by dollars, bitcoins or other currencies, enter the amount and currency for each associated value source when creating your asset. This list of value sources will show up in the "escrow amounts" section of your assets game definition. The PolyCash user interface shows asset balances but can also display the equivalent value in the currency of the users' choice, based on the escrow amounts for the asset and assuming PolyCash has relevant exchange rates in its database.

Buy-in and sell-out policies

Most PolyCash assets have a supply which is static or which changes based only on inflation. These assets have buy-in and sell-out policies set to "none." But PolyCash supports the idea of assets where the supply can be increased by depositing money into an escrow. Setting a buy-in policy for an asset pegs its value to the value of its buy-in currency. For example, for an asset with an "unlimited" buy-in policy and running on the Bitcoin blockchain, sending BTC to an escrow address associated with the asset triggers new coins to be created and credited to the player who just bought in. Similarly, setting a sell-out policy on this asset would allow players to withdraw BTC from the escrow by destroying in-game

coins by sending them to a burn address. Buy-in and sell-out policies are experimental and are not recommended for production use as of the publication of this paper.

Bet effectiveness functions

In the gaming industry, some bookmakers allow bets to be placed on sporting events while the events are going on. This is called in-play betting. Bookmakers must quickly update the odds during in-play events, to avoid making a loss as developments occur in the sporting events.

Pari-mutuel betting has traditionally only been used to allow betting prior to the start of events but has not been used for in-play betting. PolyCash enables pari-mutuel in-play betting through the concept of bet "effectiveness".

Counting bets equally across all blocks of an event gives players an incentive to avoid betting early in the round and instead waiting until near the end to bet, when it's easier to predict the outcome. PolyCash approaches this problem with an "effectiveness function" which assigns an effectiveness factor to each block in an event. Payouts are weighted by effectiveness and therefore players who bet early receive higher payouts than players who bet for the same outcome later in the event. Players who bet late are better able to predict the winner but receive lower odds and payouts.

Currently PolyCash supports two effectiveness functions:

- Constant – bets count equally throughout each event.
- Linear decrease – bets counts for 100% in the first block of an event and decrease linearly until the final block. The slope of the linear decrease can be specified in the game definition.

Effectiveness functions are not only applicable to in-play events. A linearly decreasing effectiveness function can also be used when betting ends prior to the beginning of a sporting event, to give a small advantage to players who bet early and set the initial odds, while giving slightly lower payouts to bettors who bet near the end of the betting period.

Part 6. Three levels of trust for decentralized applications.

Decentralized applications may require trust in several different ways. We have categorized trust into 3 levels as it relates to PolyCash.

Level 1: (Highest Level of Trust) Holding funds on behalf of another party

PolyCash is designed as a multi-user application. People who don't wish to install PolyCash on their local computer can sign up for a web wallet on a public facing PolyCash node. This is a relatively high level of trust because these users are entrusting custody of their funds to a third party.

Level 2: (Intermediate Level) Adding new PM events and changing base parameters of game definitions

When someone creates a new crypto asset, they publish and share its game definition with other nodes who begin tracking that asset by importing its game definition. For assets with prediction market functionality, the game definition is frequently changed as events are resolved and new events are added. Nodes must maintain consensus as the game definition changes and may entrust one node to be the authority on approving changes to the game definition.

Level 3: (Lowest Level) Resolving event outcomes

PolyCash gives node operators the technical ability to resolve events as they please. But resolving events incorrectly can break consensus and affects player balances. Still, there is less ambiguity about the outcomes of events than there is about adding events, making this the lowest level of trust.

Roadmap

1.	Development of the PolyCash web app & GUI	Complete
2.	First crypto assets launched on the PolyCash platform	Complete
3.	Ongoing development of the PolyCash application & protocol	In Progress
4.	Building a betting business using this technology	In Progress
5.	Making PolyCash known and available to the public	In Progress

Get Started

PolyCash is the ultimate protocol for the next generation of money. We've invested time and money in building an application which is elegant, highly functional, performant and secure. You can get a great understanding for how PolyCash works by visiting https://poly.cash and signing up for our free promotional Crypto Duels game for betting on crypto prices. To launch your own crypto asset or to print your own line of physical crypto cards, please check out our code on Github. The PolyCash Foundation is building a business based on this technology and is seeking investors. For more information please contact polycashcrypto@gmail.com