

BCDV1011 Design Patterns for Blockchain

Business patterns

A large, dark blue, diagonal shape that starts from the bottom left and extends towards the top right, covering the lower half of the slide.

Common patterns

- Escrow
- Voting
- Payment
- Assets
- Timestamp
- Broker

Escrow

- An Escrow is an arrangement for a third party to hold the assets of a transaction temporarily
- The smart contract holds the asset
- The rules of the smart contract may be the third party
- The use of an escrow account in a transaction adds a degree of safety for both parties

Escrow – variants and features

- Contingent beneficiary
- Decreasing term payout
- Deferred payment
- Endowment
- Escheatment
- Security Deposit
- Proof of funds
- Restricted funds
- Arbitration
- Trust Fund
- Annuity
- Trustless

Voting

- A vote is used to express a wish to follow a particular course of action
- Provides representation of the wishes of multiple parties
- Guides collective action
- Most important part of governance

Voting – variants and features

- Bidding
- Auction
- Election
- RFP
- Arbitration
- First past the post
- Proportional
- Representational
- Weighted

Payments

- A payment is the action or process of paying someone or something or of being paid
- Part of the value transfer in business transactions
- Requires settlement

Payment – variants and features

- Licensing
- Consignment
- Royalties
- Incoterms
- Invoicing
- Purchase Order
- Split Tender
- Taxation

Assets

- An asset is property owned by a person or company, regarded as having value and available to meet debts, commitments, or legacies
- May increase in value or be depreciated
- Can be physical or abstract

Asset – variants and features

- Fractional
- Equity
- Alternative
- Vesting
- Restrictions

Timestamp

- A digital record to the time of occurrence of a particular event
- State data stored on immutable blockchain
- Can be physical or abstract

Timestamp – variants and features

- Content - hash of content
- Anchor - hash of data set
- Provenance - ownership chain
- Traceability - actions on asset
- Ordering - transaction ordering for queueing

Broker

- Arranges transactions between a buyer and a seller
- Creates a decentralized marketplace
- Auctions - market making
- Sales - facilitating

Building an escrow service

- Three party transaction
 - Buyer
 - Seller
 - Agent

Building an escrow service

- Three party transaction
 - Buyer
 - Seller
 - Agent
- Role-based access control

Building an escrow service

- Flow
 - Conditions for release are set
 - Buyer transfers funds to contract
 - If conditions met
 - Agent releases to Seller
 - If conditions fail
 - Agent releases to Buyer
 - Agent gets a % or fixed fee

Smart contract

- Use RBAC pattern
- Make parties payable
- Agent can release or revert
- Fixed fee for agent

Web interface

- Website represents the seller
- Buyer interface
 - The buyer selects the escrow agent
 - The buyer selects the conditions (some sort of oracle?)
 - The buyer sends the funds
- Agent interface
 - The agent checks condition
 - Agent releases or reverts