The UTXO Models Handbook

All Flavors of UTXO models in one menu

By: The UTXO Alliance

2024/12/06

Contents

Overview

It's been a decade since Bitcoin with its underlying computing model, the **Unspent Transaction Output (UTXO) model**, brought the most prominent application of blockchain technology to life - decentralized financial systems.

This seminal pioneering breakthrough inspired subsequent revolutions reimagining socio-economic systems. A second wave introduced **smart contracts**, which allows users to put conditions on financial transactions written in verifiable code which then paves the path for **decentralized applications (dApps)** to emerge; and a third wave introduced self-governing mechanisms embedded in the system. Nowadays, a competitive blockchain must offer a network protocol that meets all previous advancements in addition to having its roadmap heavily focused on maximizing the decentralization-security-scalability triad (aka the **"Blockchain trilemma"**) from research to technical engineering.

Goals

1 This handbook aims to be a presentation card of all the different chain designs of UTXO Alliance members. Aiming to be a handy resource for entrepreneurs, commercial partners and a general audience with minimal technical knowledge.
2 Explain the key aspects of the UTXO model and the functioning of a blockchain using simple visual flowcharts.
3 Expose the rich variety of the different designs implemented by various blockchains that are part of the UTXO Alliance.

Introduction to Blockchains

We recommend these three educational introductions to get up to speed for what you're about to read. These three resources are evergreen (meaning they've aged well with time) and include:

1 Explainer how Bitcoin works: `https://learnmeabitcoin.com/beginners/how-does-bitcoin-work/`
2 Explainer How Blockchains work: `https://andersbrownworth.com/blockchain/`
3 Explainer How Bitcoin Network work: `https://youtu.be/bBC-nXj3Ng4?si=7Yskt-tMlFPb0sRk`

Ingredients of a Blockchain

At its heart, a blockchain is a special kind of database that keeps track of information in a way that's secure, open for anyone to see, and nearly impossible to retroactively change. Unlike traditional databases managed by a single organization, blockchains are maintained by a network of computers working together. This design ensures that no single person or group has complete control over the information, see Fig. 2.

Understanding its core components is crucial for grasping how blockchains function and how different implementations or "flavors" of blockchain systems offer different benefits. In this section, we'll break down the essential "ingredients" that make up a UTXO-based blockchain. By examining these building blocks – cryptographic primitives, transactions, blocks, and the chain itself – we can better appreciate the innovations and variations in different blockchain designs.

As we explore each ingredient, we'll see how they contribute to the overall functionality and security of the blockchain. We'll also touch on how various blockchain projects have modified or extended these basic components to create their own unique characteristics, leading to a rich ecosystem of blockchain "flavors" all stemming from the same fundamental recipe. Lets navigate through Fig.1a) we have the most high-level construction of a blockchain. Each of the color boxes are the core concepts to construct a blockchain, we'll call these our 'ingredients'. So we have 6 ingredients in total:

1 **Hash functions (H) and cryptographic signatures (S)** (blue boxes) - The reason that these two concepts can be labeled under the same ingredient is because signatures use hashes in their internal mechanism. Each of these are crucial and highly used in many other parts of the blockchain
2 **Transaction (Tx)** (red box)- A transaction allows to change data, ie. move crypto value from one party to another
3 **UTXO Set Ledger** (green boxes) - The aggregation of outputs for tracking global and local state

4) **Block (B)** (orange box) - The container of transactions, verification of consensus, and compressed record of history
4 **Protocol (Π)** (purple box) - The formal system by which nodes reach agreement
5 **Network** (gray box) - The system by which nodes communicate and ultimately facilitate agreement

Cryptographic Primitives

Cryptographic primitives form the foundation of blockchain security and functionality. Two crucial elements are hash functions (H) and digital signatures (S).

Hash functions are one-way mathematical operations that convert any input into a fixed-size output, see Fig. 3 (top). In blockchains, they create unique identifiers, link blocks, and support consensus mechanisms like Proof of Work.

Digital signatures Fig. 3 (bottom) are generated using hash functions and provide identity in blockchain systems. Unlike traditional systems where identity is tied to government-issued documents, blockchain identities can be pseudonymous, offering a new paradigm for verification and authentication in digital networks.

Transactions

Transactions are the basic units of state/value transfer in a blockchain. In the UTXO model:

a) Structure: Fig. 4 transactions consist of inputs (black arrows) and outputs (red arrows). b) Inputs: Reference previous transaction outputs (UTXOs) being spent. c) Outputs: Specify new UTXOs being created, including recipient addresses and amounts. d) Conservation Law: The sum of inputs must equal or exceed the sum of outputs (minus a transaction fee). e) Signatures: Each input must be signed by the owner of the corresponding UTXO.

The UTXO Set Ledger

The UTXO set plus additional data is what ultimately the Ledger stores. The slicing of UTXO selection is what a user's wallet performs in order to determine how many outputs an address holds. The Ledger refers to the long running concatenation of transactions via blocks, the UTXO set represents the proverbial "tip of the chain" which is the most relevant perspective of current state. See Fig. **??**

Block

Blocks are containers for transactions and form the backbone of the blockchain: a) Structure: Typically includes a header and a list of transactions. b) Block Header: Contains metadata such as: Previous block hash (creating the chain) Merkle root of transactions Timestamp Nonce (for proof-of-work) c) Proof-of-Work: A mechanism to make block creation computationally expensive, ensuring security. d) Coinbase Transaction: A special transaction in each block that creates new currency and collects transaction fees.

The protocol Π

The Network

Subparagraph. The subparagraph format with the paragraph indent is likely going to be more familiar to the reader.

Special Sections

The module also includes functions to aid in the proper typesetting of multi-line section headers: `\DndFeatHeader` for feats, `\DndItemHeader` magic items and traps, and `\DndSpellHeader` for spells.

Typesetting Savant

Prerequisite: LaTeX distribution

You have acquired a package which aids in typesetting source material for one of your favorite games. You have advantage on Intelligence checks to typeset new content. On a failed check, you can ask questions online at the package's website.

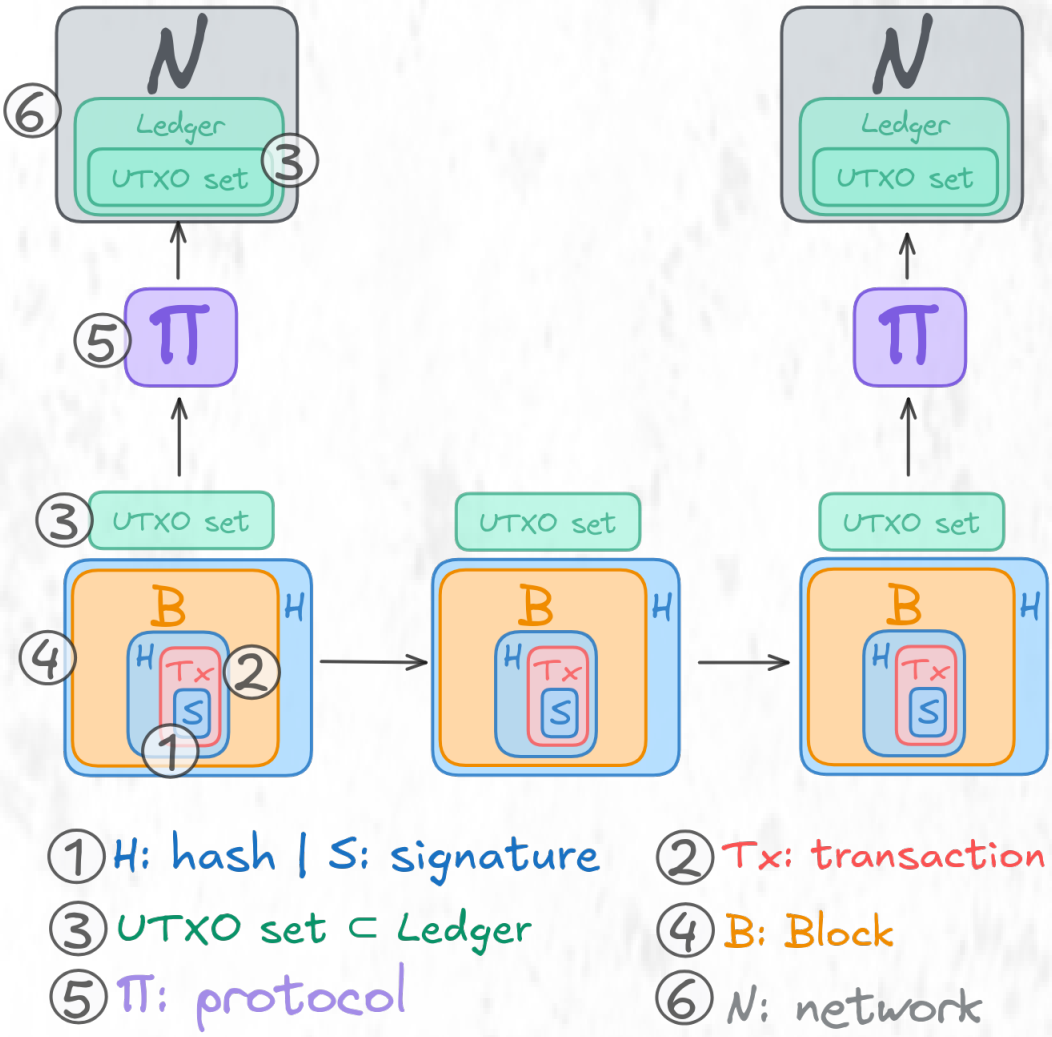

Figure 1: Simplified view of blockchain structure based on the composition of our simple blockchain ingredients.

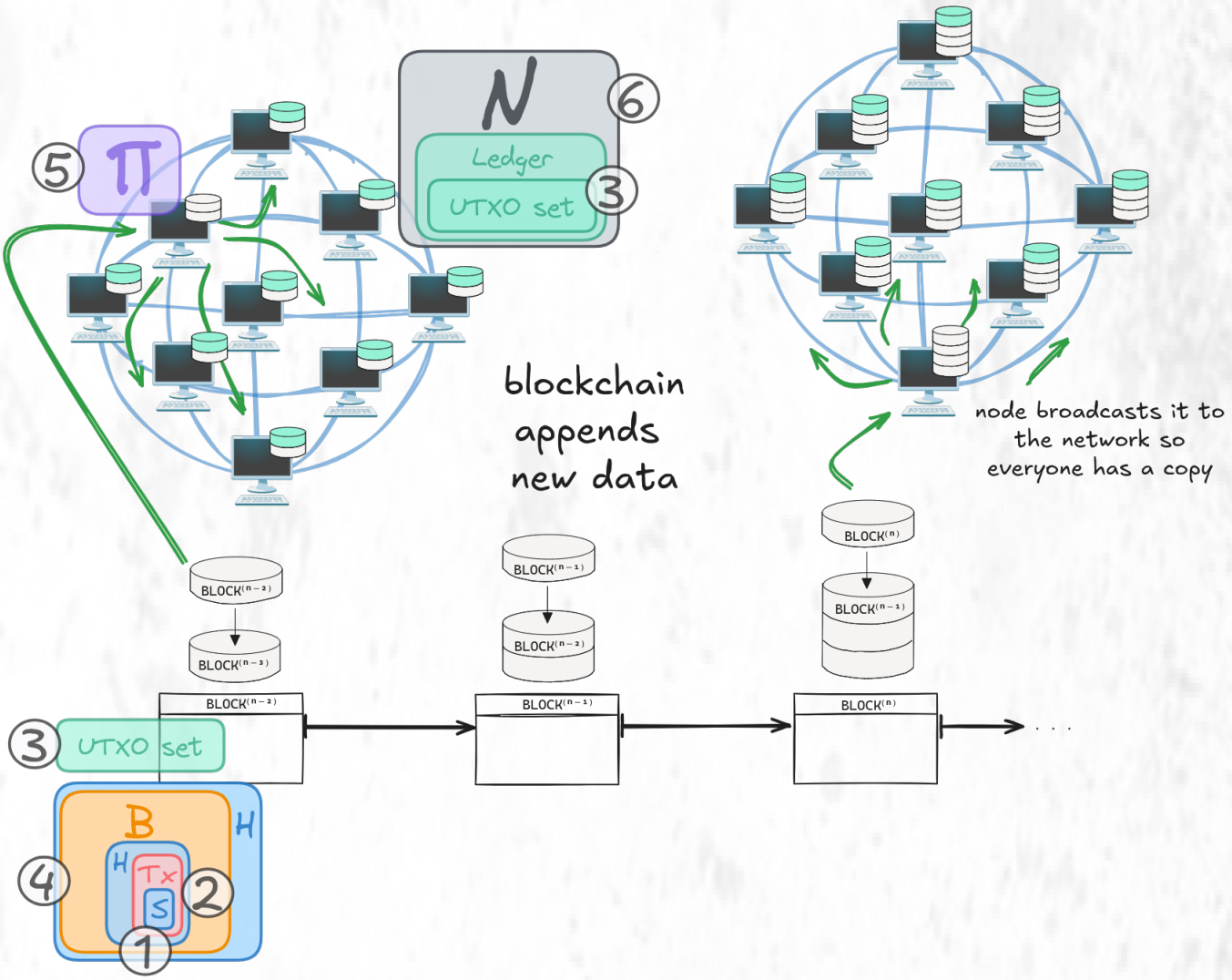

Figure 2: General functioning of a blockchain.

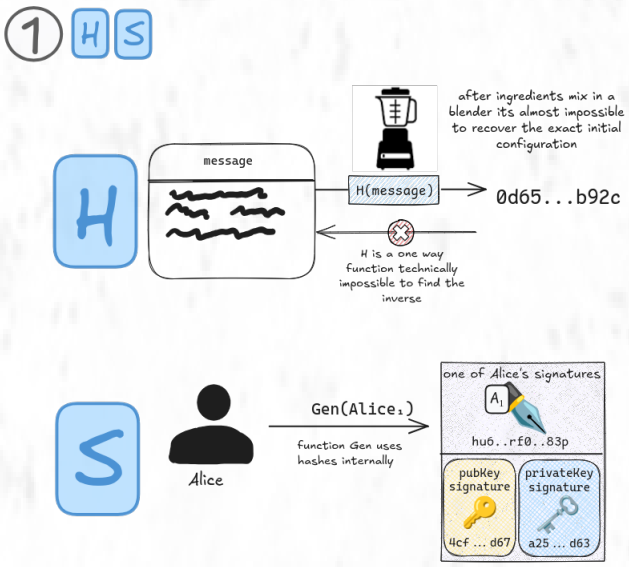

Figure 3: We can see that our label ingredient H (top) refers to cryptographic hash functions which are one-way functions. We can see that our label ingredient S (below) refers to digital signatures, where a private number is transformed into a key pair, one capable of being shared publicly and one forever kept private and secure. The public key can be used like a mailing address or identity, and the private key can perform operations privately which confirm approval, ownership and identity. This functionality is used in many internet and computer protocols besides blockchains.

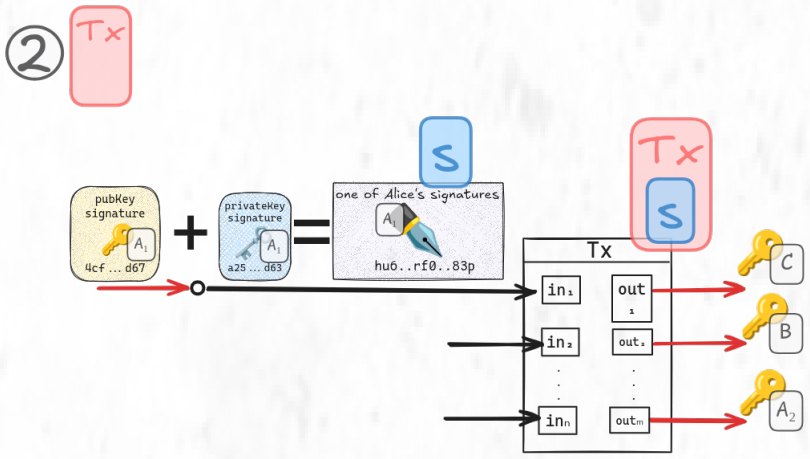

Figure 4: A transaction in the UTXO model.

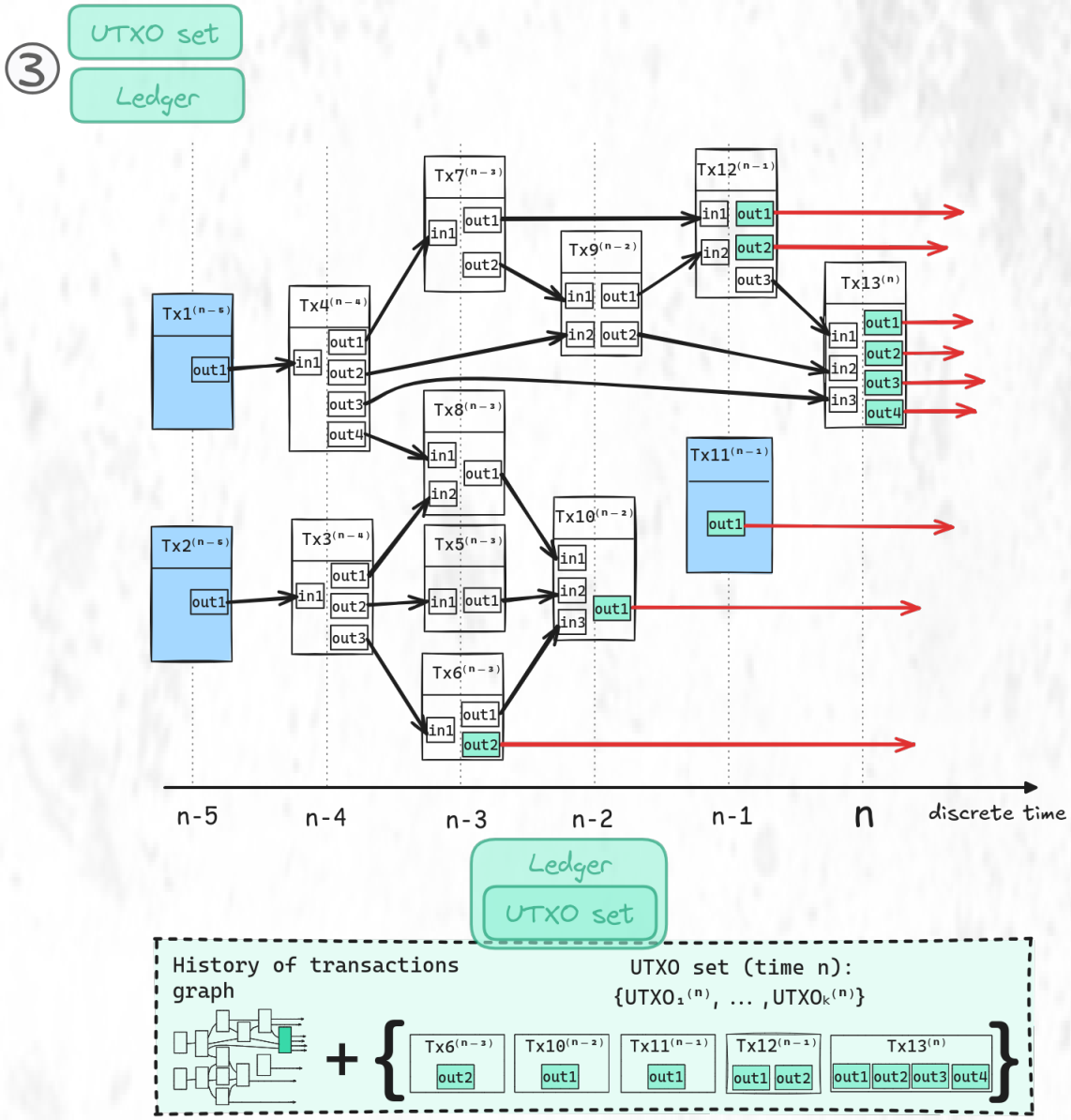

Figure 5: The UTXO set and the UTXO model graph.

Foo's Quill

Wondrous item, rare

This quill has 3 charges. While holding it, you can use an action to expend 1 of its charges. The quill leaps from your hand and writes a contract applicable to your situation.

The quill regains 1d3 expended charges daily at dawn.

Beautiful Typesetting

4th-level illusion

Casting Time: 1 action
Range: 5 feet
Components: S, M (ink and parchment, which the spell consumes)
Duration: Until dispelled

You are able to transform a written message of any length into a beautiful scroll. All creatures within range that can see the scroll must make a wisdom saving throw or be charmed by you until the spell ends.

While the creature is charmed by you, they cannot take their eyes off the scroll and cannot willingly move away from the scroll. Also, the targets can make a wisdom saving throw at the end of each of their turns. On a success, they are no longer charmed.

Map Regions

The map region functions `\DndArea` and `\DndSubArea` provide automatic numbering of areas.

1. Village of Hommlet

This is the village of hommlet.

1a. Inn of the Welcome Wench

Inside the village is the inn of the Welcome Wench.

1b. Blacksmith's Forge

There's a blacksmith in town, too.

2. Foo's Castle

This is foo's home, a hovel of mud and sticks.

2a. Moat

This ditch has a board spanning it.

2b. Entrance

A five-foot hole reveals the dirt floor illuminated by a hole in the roof.

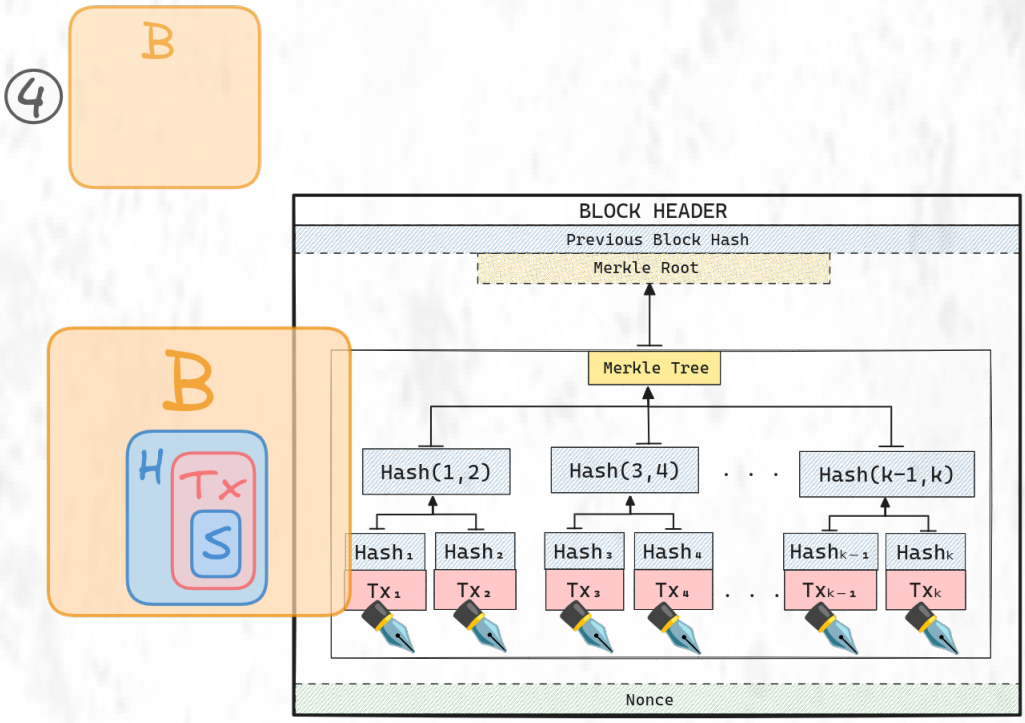

Figure 6: The UTXO set and the UTXO model graph.

Chapter 1: Text Boxes

The module has three environments for setting text apart so that it is drawn to the reader's attention. `DndReadAloud` is used for text that a game master would read aloud.

As you approach this module you get a sense that the blood and tears of many generations went into its making. A warm feeling welcomes you as you type your first words.

As an Aside

The other two environments are the `DndComment` and the `DndSidebar`. The `DndComment` is breakable and can safely be used inline in the text.

This Is a Comment Box!

A `DndComment` is a box for minimal highlighting of text. It lacks the ornamentation of `DndSidebar`, but it can handle being broken over a column.

The `DndSidebar` is not breakable and is best used floated toward a page corner as it is below.

Tables

The `DndTable` colors the even rows and is set to the width of a line by default.

Nice Table

Table head	Table head
Some value	Some value
Some value	Some value
Some value	Some value

Behold the DndSidebar!

The `DndSidebar` is used as a sidebar. It does not break over columns and is best used with a figure environment to float it to one corner of the page where the surrounding text can then flow around it.

Chapter 2: Monsters and NPCs

The `DndMonster` environment is used to typeset monster and NPC stat blocks. The module supplies many functions to easily typeset the contents of the stat block

Monster Foo

Medium aberration (metasyntactic variable), neutral evil

Armor Class 9 (12 with *mage armor*)
Hit Points 16 (3d8 + 3)
Speed 30 ft., fly 30 ft.

STR	DEX	CON	INT	WIS	CHA
12 (+1)	8 (–1)	13 (+1)	10 (+0)	14 (+2)	15 (+2)

Senses darkvision 60 ft., passive Perception 10
Languages Common, Goblin, Undercommon
Challenge 1 (200 XP)

Innate Spellcasting. Foo's spellcasting ability is Charisma (spell save DC 12, +4 to hit with spell attacks). It can innately cast the following spells, requiring no material components:

At will: *misty step*
3/day each: *fog cloud*, *rope trick*
1/day: *identify*

Spellcasting. Foo is a 2nd-level spellcaster. Its spellcasting ability is Charisma (spell save DC 12, +4 to hit with spell attacks). It has the following sorcerer spells prepared:

Cantrips (at will): *blade ward*, *fire bolt*, *light*, *shocking grasp*
1st level (3 slots): *burning hands*, *mage armor*, *shield*

Actions

Multiattack. The foo makes two melee attacks.

Dagger. *Melee or Ranged Weapon Attack:* +3 to hit, reach 5 ft. or range 20/60 ft., one target. *Hit:* 3 (1d4 + 1) piercing damage.

Flame Tongue Longsword. *Melee Weapon Attack:* +3 to hit, reach 5 ft., one target. *Hit:* 5 (1d8 + 1) slashing damage, or 6 (1d10 + 1) slashing damage if used with two hands, plus 7 (2d6) fire damage.

Assassin's Light Crossbow. *Ranged Weapon Attack:* +1 to hit, range 80/320 ft., one target. *Hit:* 4 (1d8) piercing damage, and the target must make a DC 15 Constitution saving throw, taking 24 (7d6) poison damage on a failed save, or half as much damage on a successful one.

Legendary Actions

The foo can take 3 legendary actions, choosing from the options below. Only one legendary action option can be used at a time and only at the end of another creature's turn. The foo regains spent legendary actions at the start of its turn.

Move. The foo moves up to its speed.
Dagger Attack. The foo makes a dagger attack.
Create Contract (Costs 3 Actions). The foo presents a contract in a language it knows and waves it in the face of a creature within 10 feet. The creature must make a DC 10 Intelligence saving throw. On a failure, the creature is incapacitated until the start of the foo's next turn. A creature who cannot read the language in which the contract is written has advantage on this saving throw.

Chapter 3: Colors

This package provides several global color variables to style `DndComment`, `DndReadAloud`, `DndSidebar`, and `DndTable` environments.

Box Colors

Color	Description
`commentcolor`	`DndComment` background
`readaloudcolor`	`DndReadAloud` background
`sidebarcolor`	`DndSidebar` background
`tablecolor`	background of even `DndTable` rows

They also accept an optional color argument to set the color for a single instance. See Table 3.1 for a list of core book accent colors.

```
\begin{DndTable}[color=PhbLightCyan]{cX}
  \textbf{d8} & \textbf{Item} \\
  1 & Small wooden button \\
  2 & Red feather \\
  3 & Human tooth \\
  4 & Vial of green liquid \\
  6 & Tasty biscuit \\
  7 & Broken axe handle \\
  8 & Tarnished silver locket \\
\end{DndTable}
```

d8	Item
1	Small wooden button
2	Red feather
3	Human tooth
4	Vial of green liquid
6	Tasty biscuit
7	Broken axe handle
8	Tarnished silver locket

Themed Colors

Use `\DndSetThemeColor[<color>]` to set `commentcolor`, `readaloudcolor`, `sidebarcolor`, and `tablecolor` to a specific color. Calling `\DndSetThemeColor` without an argument sets those colors to the current `themecolor`. In the following example the group limits the change to just a few boxes; after the group finishes, the colors are reverted to what they were before the group started.

```
\begingroup
\DndSetThemeColor[PhbMauve]
```

Colors Supported by This Package

Color	Description
`PhbLightGreen`	Light green used in PHB Part 1 (Default)
`PhbLightCyan`	Light cyan used in PHB Part 2
`PhbMauve`	Pale purple used in PHB Part 3
`PhbTan`	Light brown used in PHB appendix
`DmgLavender`	Pale purple used in DMG Part 1
`DmgCoral`	Orange-pink used in DMG Part 2
`DmgSlateGray` (`DmgSlateGrey`)	Blue-gray used in PHB Part 3
`DmgLilac`	Purple-gray used in DMG appendix

```
\begin{DndComment}{This Comment Is in Mauve}
  This comment is in the the new color.
\end{DndComment}

\begin{DndSidebar}{This Sidebar Is Also Mauve}
  The sidebar is also using the new theme color.
\end{DndSidebar}
\endgroup
```

This Comment Is in Mauve

This comment is in the the new color.

This Sidebar Is Also Mauve

The sidebar is also using the new theme color.