Covenants

درس بلاک چین
ارائه دهندگان:
دانیال خراسانی زاده
محمدجواد کشاورزمولائی

سال 1404

سوال

آیا میتوان UTXO ای داشت که فقط در یک مسیر خاص یا آدرس خاص خرج شود ؟

مفهوم

Covenants یا میثاق

امکان محدود و رد تراکنش حتی پس از احراز هویت صاحب آدرس UTXO

مثال های ساده

محدودیت زمانی
محدودیت بر آدرس مقصد
محدودیت بر مقدار ارسال شده
محدودیت بر مسیر خرج
محدودیت روی تعداد ورودی و خروجی
...

کاربرد ها

خزانه امن (Vault)

قالب سازی تراکنش (Transaction Templating)

کنترل ازدحام (Congestion Control)

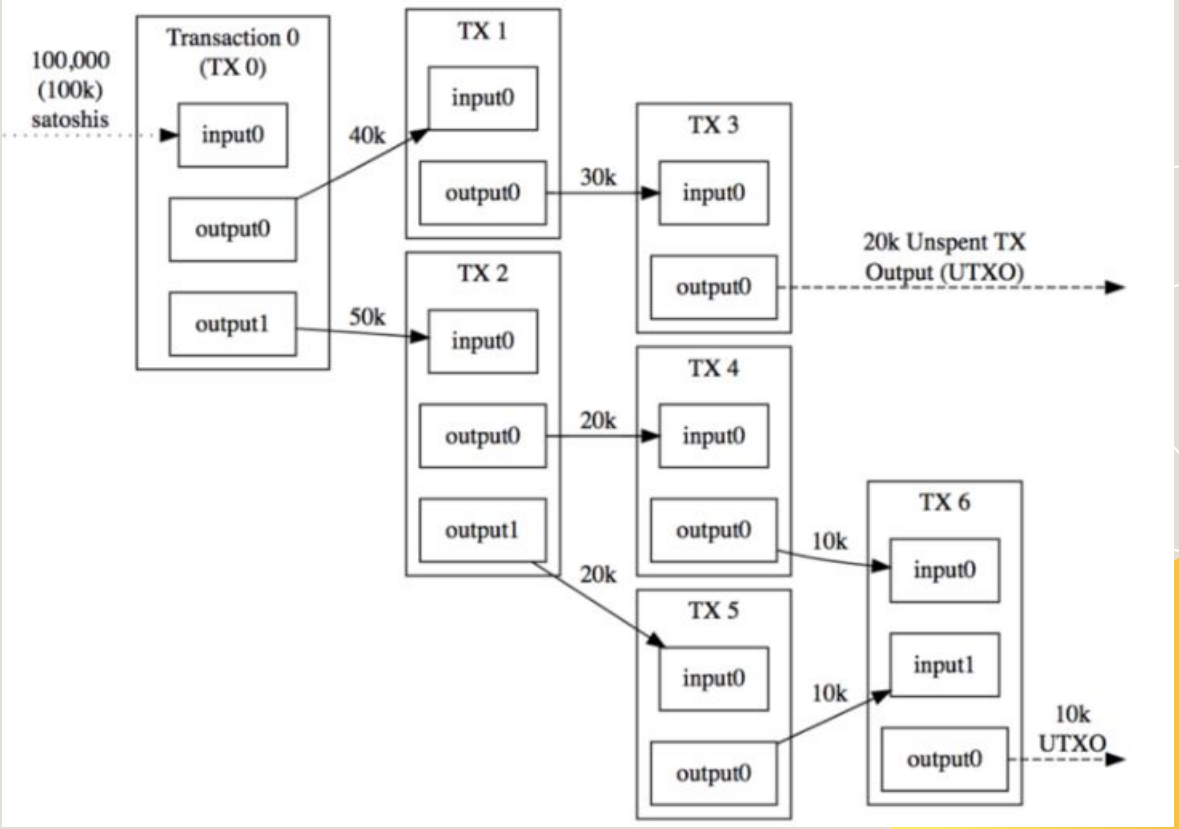
Coin Pool

StateChain

SpaceChain

.....

Transaction Templating

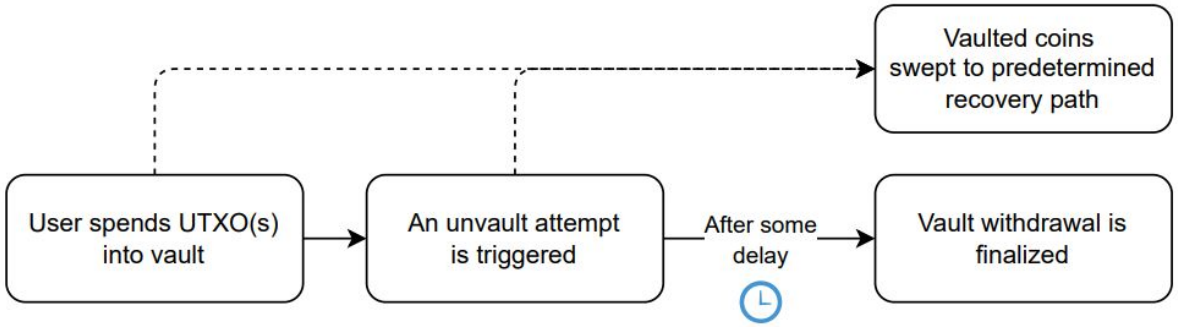


Vault

به جهت امن سازی دارایی

دو نوع تراکنش:

- Vault-commit
- Vault-redeem



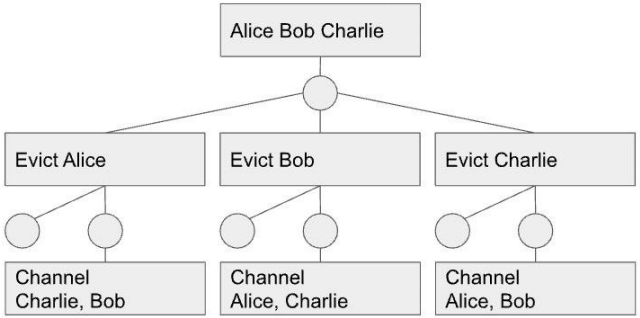
The basic lifecycle of a Bitcoin vault.

Coin Pool

(Payment pool)

What is a payment pool?

A multiparty payment channel which any participant can pull out their UTXO at any time, creating one UTXO for the rest and one UTXO for the evicted.



حل مسائل:

- کاهش تعداد تراکنش
- حل robust exit

Congestion Control

زمانی که تعداد تراکنش های زیادی داریم، و کارمزد شبکه نیز بالا میباشد، از covenant ها به عنوان راه حل مشکل کارمزد استفاده میکنیم. تا همزمان متعهد به تراکنش باشیم و هم تراکنش انتقال هنگام کاهش کارمزد شبکه انجام شود.

پیاده‌سازی‌های پیشنهادی

در حال حاضر تعداد زیادی روش پیشنهادی برای پیاده‌سازی Covenant ها در شبکه Bitcoin وجود دارد:

- ANYPREVOUT
- CTV
- OP_VAULT
- TLUV
- TXHASH
- OP_TX
- OP_CCV
- OP_CAT

- حتی برخی از افراد ادعا می‌کنند که شاید بدون تغییر نیز بتوان Covenant ها را پیاده کرد.

OP_CHECKTEMPLATEVERIFY (CTV)

- معرفی شده در BIP-119
- از Hash یک یا چند Output از پیش مشخص شده برای ایجاد تعهد استفاده می‌کند.
- قابل استفاده برای Vault, Congestion Control و Spacechains
- به خاطر انعطاف کم مورد انتقاد قرار گرفته

CHECKTXHASHVERIFY

- معرفی شده در BIP-346
- بر خلاف CTV که نیاز به تمام داده تراکنش داشت، با پشتیبانی از یک ورودی به نام TxFieldSelector می‌تواند هر قسمتی از تراکنش را انتخاب کند.
- قابل استفاده برای Spacechains, Vault, Congestion Control و Payment Pools

OP_CAT

- دو داده بر روی استک را به هم متصل کرده و دوباره در استک قرار می‌دهد.
- در پیاده‌سازی اصلی Bitcoin وجود داشت اما به خاطر خطرات امنیتی بوسیله ساتوشی حذف شد.
- ایده اصلی: به جای جدا کردن داده‌ها، داده جدا شده را از کاربر گرفته و با اتصال آن‌ها Verify کنیم.
- می‌تواند برای پیاده‌سازی ایده‌های زیادی استفاده شود و به همین خاطر مورد انتقاد قرار گرفته.