دو احتمال وجود دارد:

1. شخص دیگری (مانند همسرش) به کلید خصوصی او دسترسی دارد. به این ترتیب، صاحب کلید خصوصی می‌تواند به راحتی تراکنش‌های جدیدی را در شبکه بلاک چین ارسال کند.
2. صاحب کلید scriptSig و scriptPubKey را صادر کرده است، اما آن را به یک ماینر ارسال نکرده است و یا آن را به ماینر ارسال کرده است، اما ماینر تصمیم گرفته است چند سال بعد آن را در یک بلاک قرار دهد، یا آن را به شخص دیگری تحویل داده است و آن شخص چند سال بعد از آن استفاده کرده است.

توضیح:

- private key: یک عدد رمزنگاری شده است که به صاحب آن اجازه می دهد تا بیت کوین خود را خرج کند.
- scriptSig: یک قطعه کد است که حاوی امضای صاحب کلید خصوصی است.
- scriptPubKey: یک قطعه کد است که مشخص می کند چه کسی می تواند بیت کوین را خرج کند.

مثال:

فرض کنید علی 1 بیت کوین دارد و می خواهد آن را به حسن بفرستد. علی باید ابتدا یک تراکنش ایجاد کند. این تراکنش شامل اطلاعات زیر است:

- آدرس بیت کوین علی
- آدرس بیت کوین حسن
- مقدار بیت کوینی که علی می خواهد ارسال کند
- امضای علی (که با استفاده از کلید خصوصی وی ایجاد شده است)

علی سپس باید تراکنش را به یک ماینر ارسال کند. ماینر تراکنش را تأیید کرده و آن را به بلاک چین اضافه می کند. پس از آن، بیت کوین علی به حسن منتقل می شود.

در این مثال، فرض کنید علی تراکنش را ایجاد کرده است، اما آن را به یک ماینر ارسال نکرده است. در این صورت، علی دو گزینه دارد:

1. او می تواند تراکنش را به یک ماینر ارسال کند. ماینر تراکنش را تأیید کرده و آن را بعدا به بلاک چین اضافه می کند. پس از آن، بیت کوین علی به حسن منتقل می شود.
2. علی می تواند تراکنش را به شخص دیگری تحویل دهد. آن شخص می تواند تراکنش را به یک ماینر ارسال کند و بیت کوین علی را به حسن منتقل کند.

اگر علی تراکنش را به شخص دیگری تحویل دهد، آن شخص می تواند چند سال بعد از آن استفاده کند. این به این دلیل است که تراکنش‌های بیت کوین منقضی نمی‌شوند.