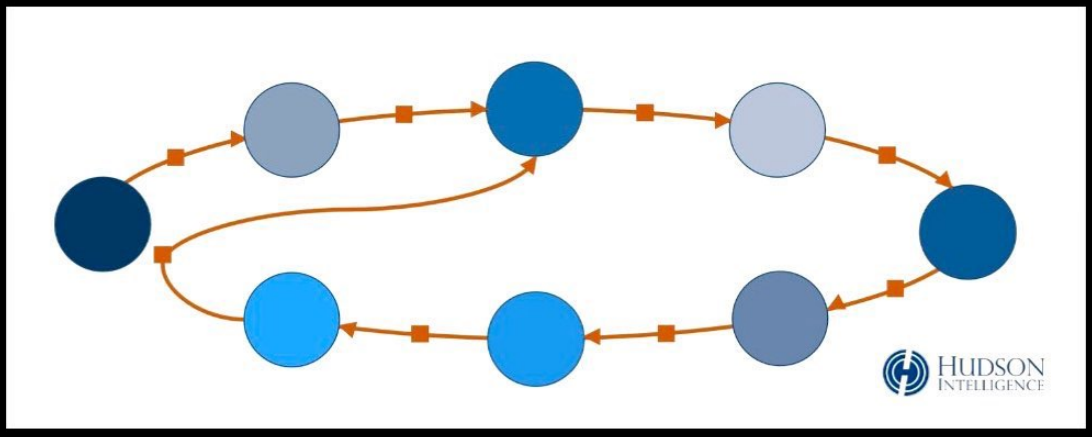
FoC-HW1-97243008

رسا بختیاری

۱-در ابتدا که شبکه بیتکوین ساخته‌شد فقط یک کاربر داشت و شبکه‌ای که در آن یک نفر در آن حضور دارد فقط می‌تواند به عنوان شبکه‌ای عمل کند که در آن چندین کاربر فیک وجود دارد در نتیجه وجود آدرس‌های مختلف برای تست شبکه لازم بود.همچنین استفاده مجدد از یک آدرس امنیت و ناشناس بودن هویت را به خطر می‌اندازد



برای مثال در دیاگرام بالا که مربوط به تراکنش‌های بین چندنفر می‌باشد در آخرین تراکنش مشاهده‌می‌شود که مقصد تراکنش آدرسی است که از آن قبلاً به عنوان مقصد تراکنشی دیگر استفاده شده است و کسانی که بلاکچین را trace و آنالیز میکنند می‌فهمند که هر ۶ آدرس متعلق به یک نفر میباشد و اینگونه پروژه‌های پولشویی و کلاهبرداری را پیدا می‌کنند.

۲-تراکنش جدید انجام داده است چون یک نفر key حساب آن را دارد.