CRYPTOCURRENCY TRADING

Bitcoin

Ali Zamani

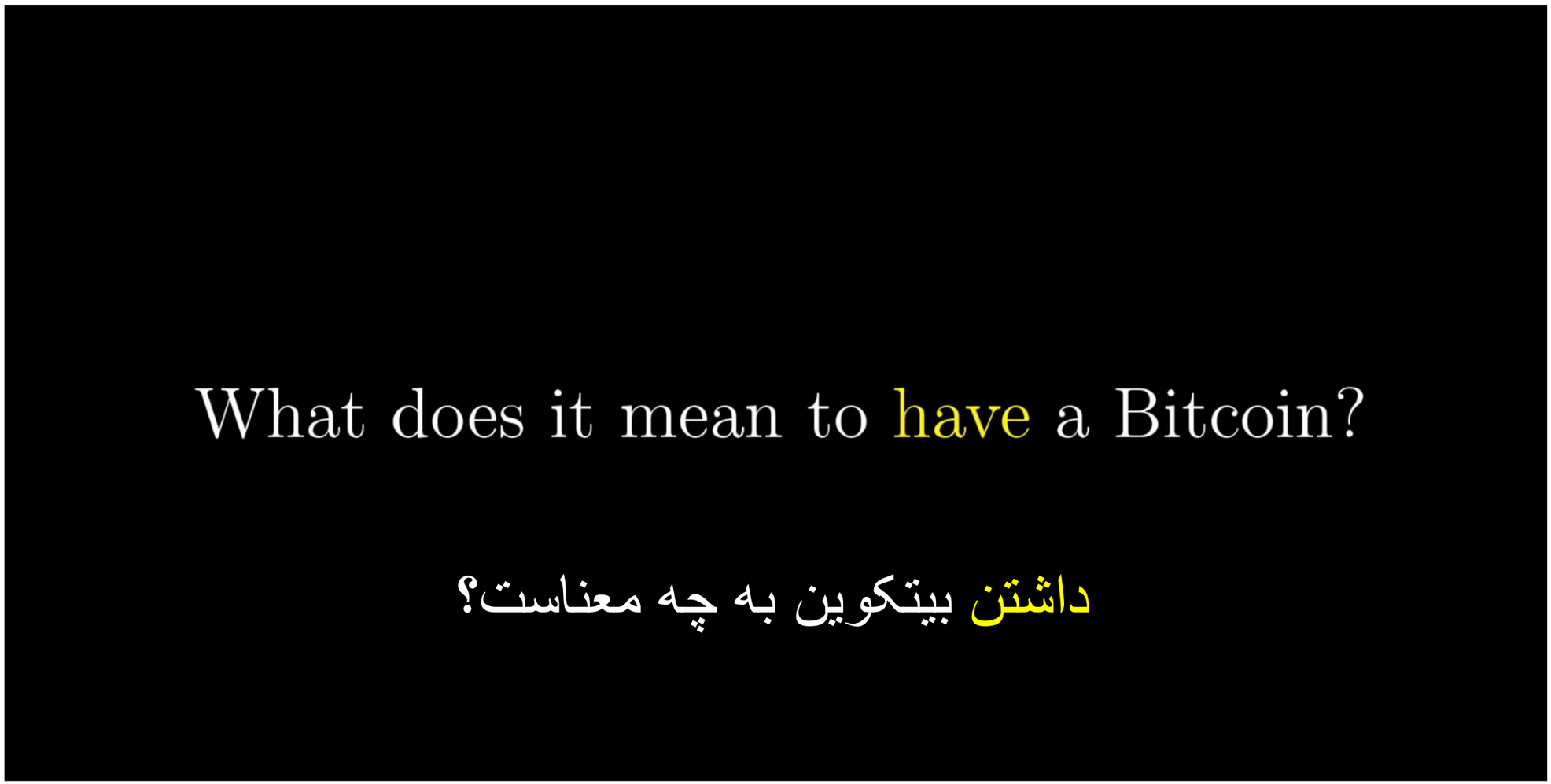
Instagram ID: @361.degree.trading

Clubhouse ID: @alizamanim

Kohan_Fx

KohanFx.com

KohanFx



Digital

یک ارز دیجیتال که :

- ✓ به هیچ دولتی جهت چاپ یا تاییدیه نیاز ندارد
- ✓ به هیچ بانکی جهت مدیریت حسابها یا تایید تراکنشهای مالی نیاز ندارد

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Who is this?

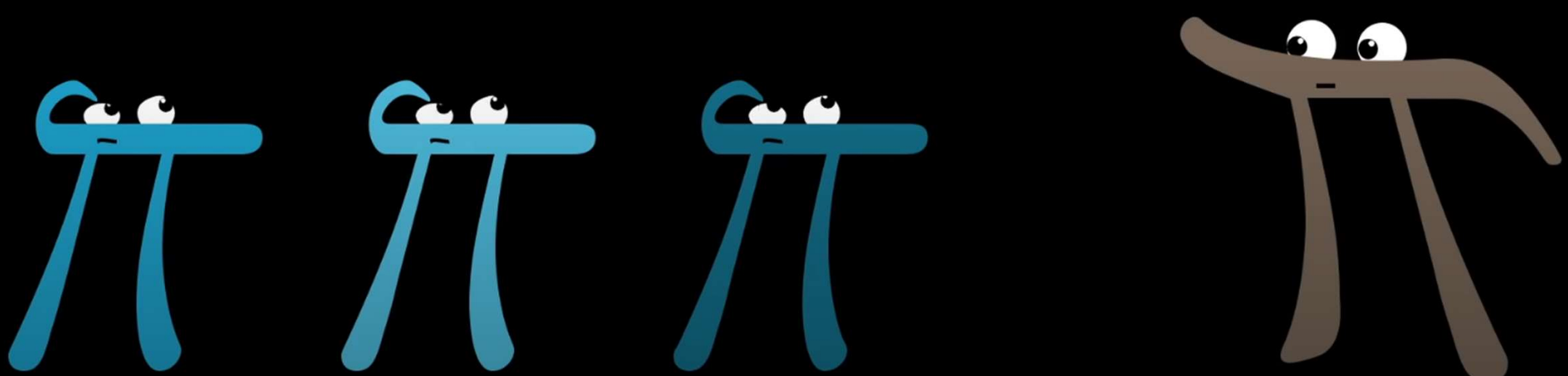
همچنین کسی نمی داند چه شخصی یا اشخاصی آن را ابداع کردند

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Digital signatures, Proof of work, Cryptographic hash functions, . . .

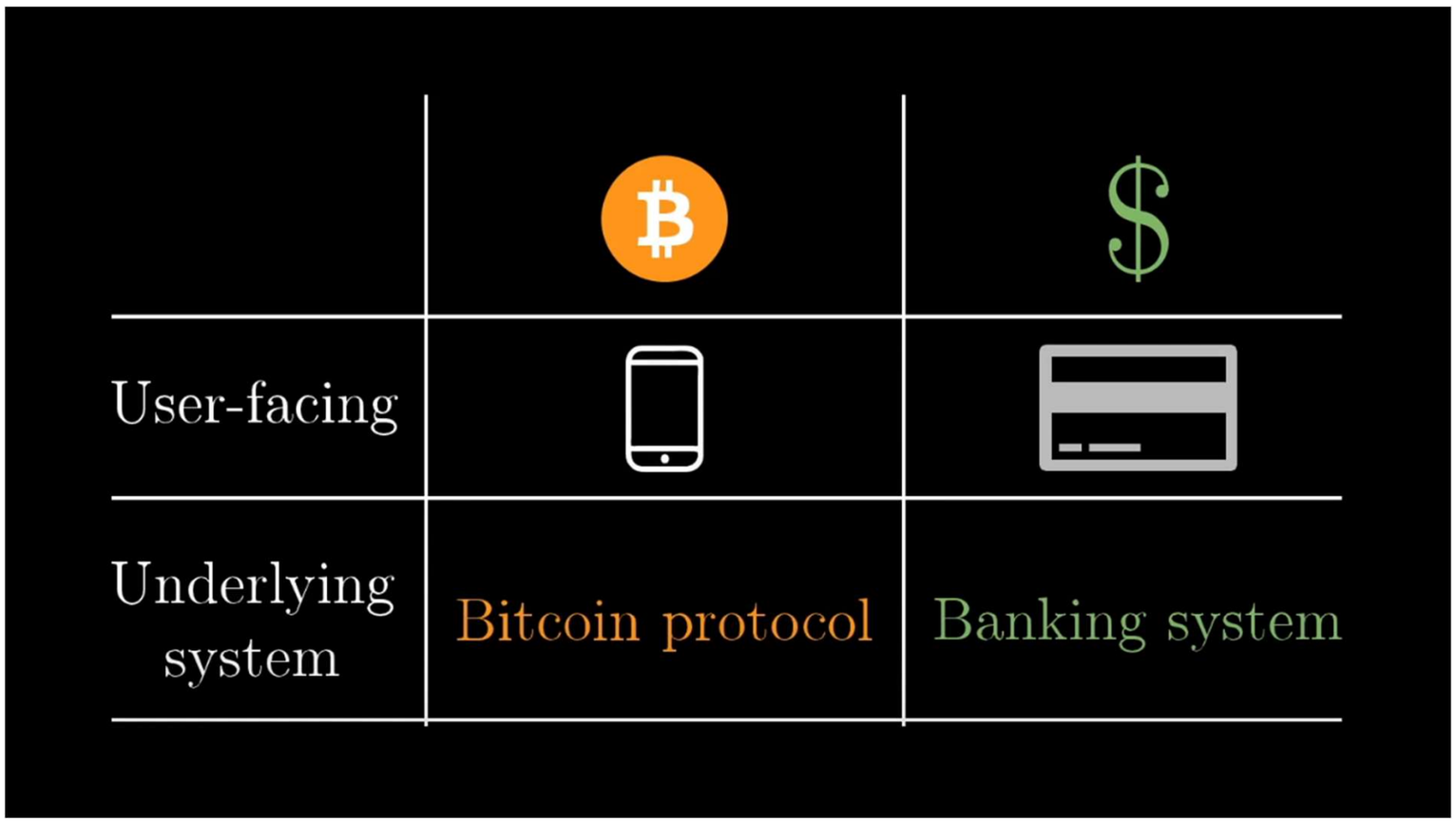
جهت درک بهتر موضوع و آشنایی با مفاهیم کلیدی
نحوه ابداع و کارکرد بیتکوین را بصورت قدم به قدم بررسی میکنیم

What does it mean to have a Bitcoin?



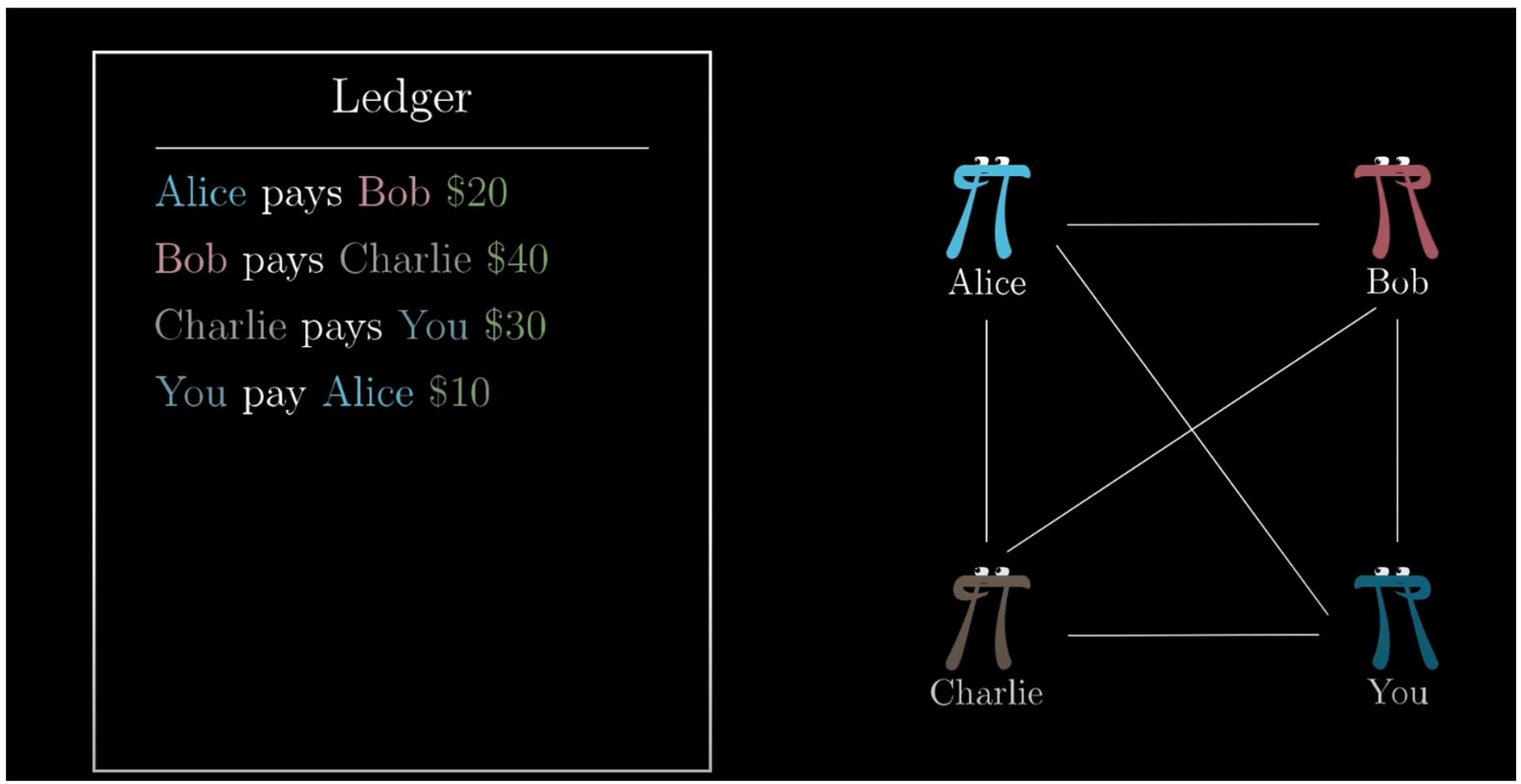
لازم به ذکر است که جهت استفاده از بیتکوین (خرید یا انجام تراکنش) نیازی به دانستن نحوه کارکرد آن
و مفاهیم تکنیکی نمی باشدهمانگونه که برای استفاده از
حساب بانکی یا کارت اعتباری نیازی به دانستن نحوه کارکرد بانک نیست

از طرفی جهت شناخت بازار رمز ارزها و انتخاب رمز ارزهای مناسب جهت سرمایه گذاری
و کاربردهای دیگر لازم است که با مفاهیم تکنیکی آنها آشنایی کافی داشت

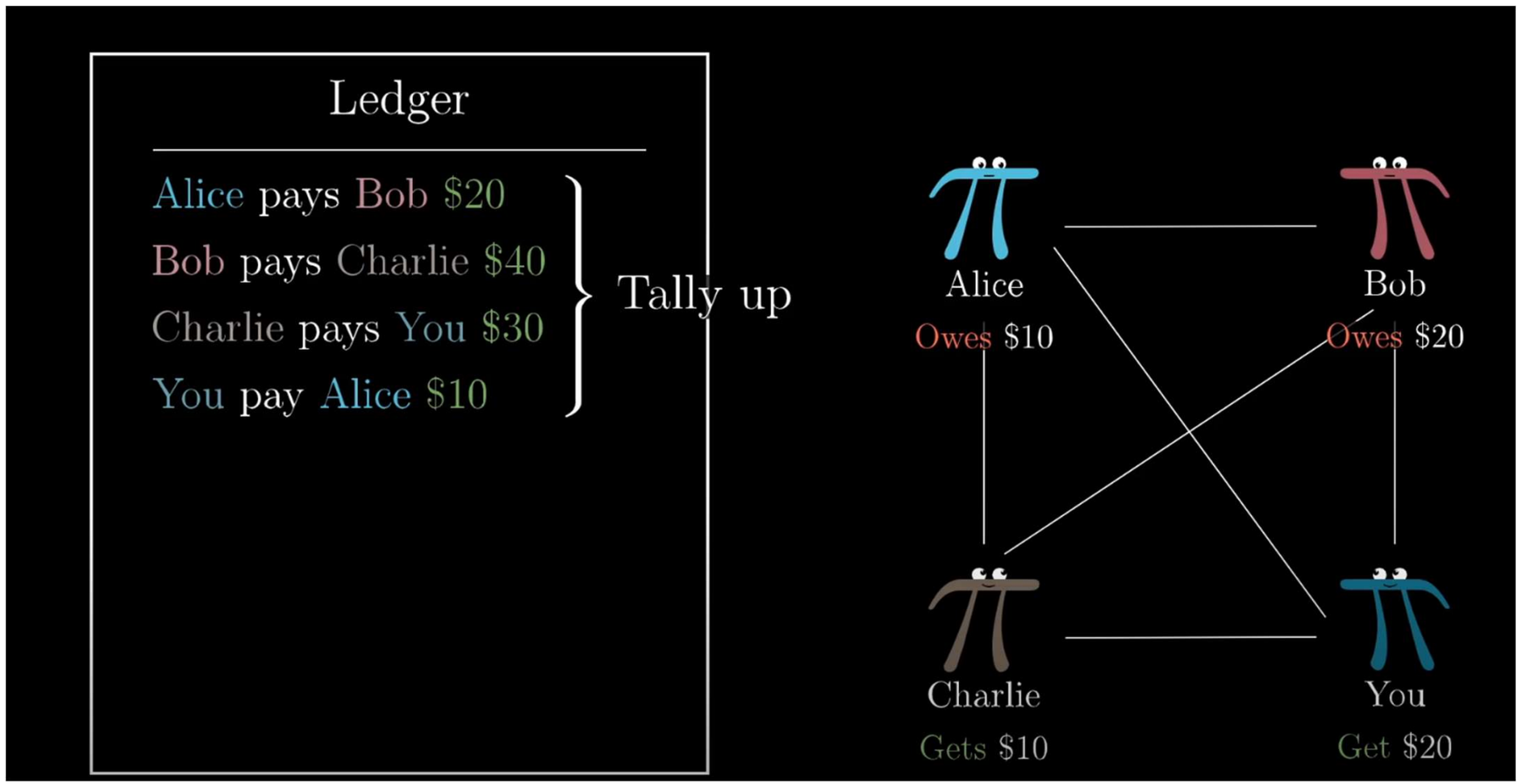


برای شروع کار بیتکوین و رمزارزها را از ذهن خود پاک کرده
و تنها با مفاهیم پیش پا افتاده همچون
دفتر کل و امضای دیجیتال شروع میکنیم

در صورتی که با دوستانتان هزینه های مشترک دارید رد و بدل کردن پول بطور مداوم دردسرهای بسیاری دارد
از این رو جهت دانستن حساب و کتاب مشترک، تراکنشهای انجام شده و یا بدهی های پرداخت نشده
همچون سهم هر نفر از شام، اجاره خانه، هزینه آب برق و ...
را در یک دفتر کل عمومی و قابل دسترس همه (Public Ledger) یادداشت نموده تا سر ماه حسابها رسیدگی شود



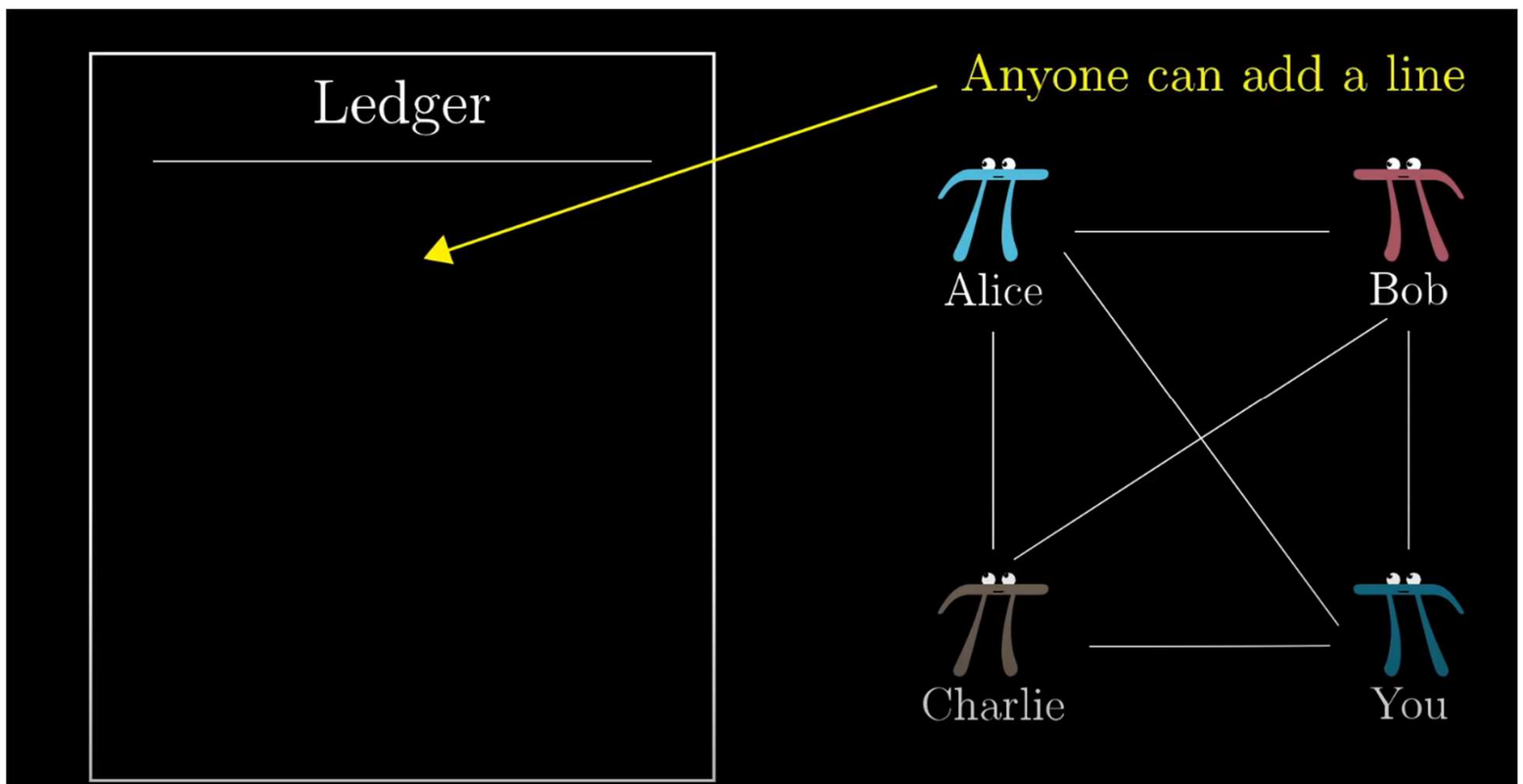
در پایان هر ماه به حسابها رسیدگی کرده و هر نفر
در صورت بدهکار شدن مبلغ بدهی را در حساب مشترک قرار داده
و در صورت بستانکار شدن مبلغ طلب را از حساب مشترک برداشت می کند



شرایط استفاده از دفتر کل:

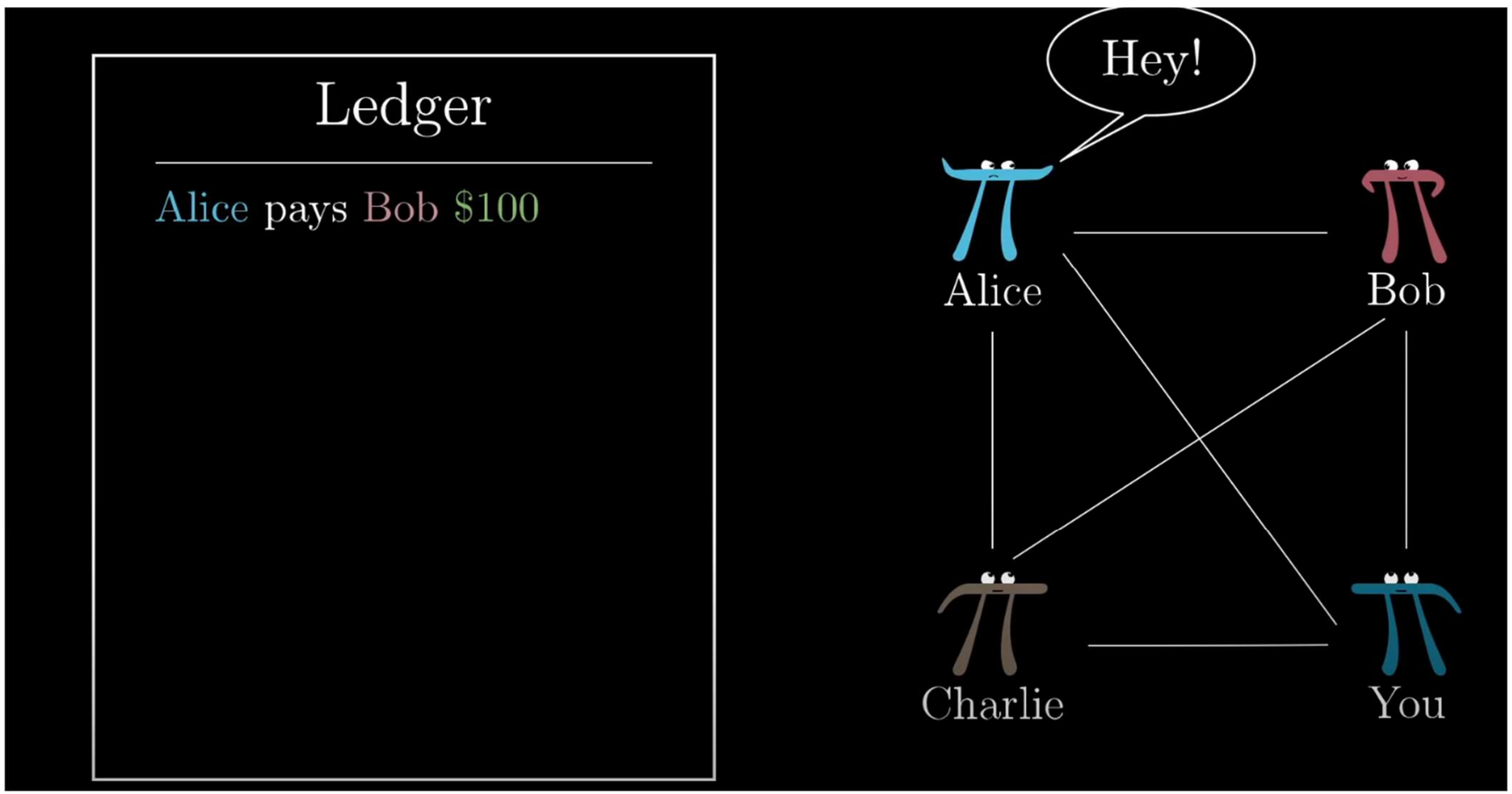
هر کسی می تواند در دفتر تراکنش وارد کند
در پایان هر ماه حسابها رسیدگی شده و صفر گردد

یکی از مشکلات اصلی چنین دفتر کل عمومی این است که هر شخصی می تواند در دفتر تراکنش وارد کند



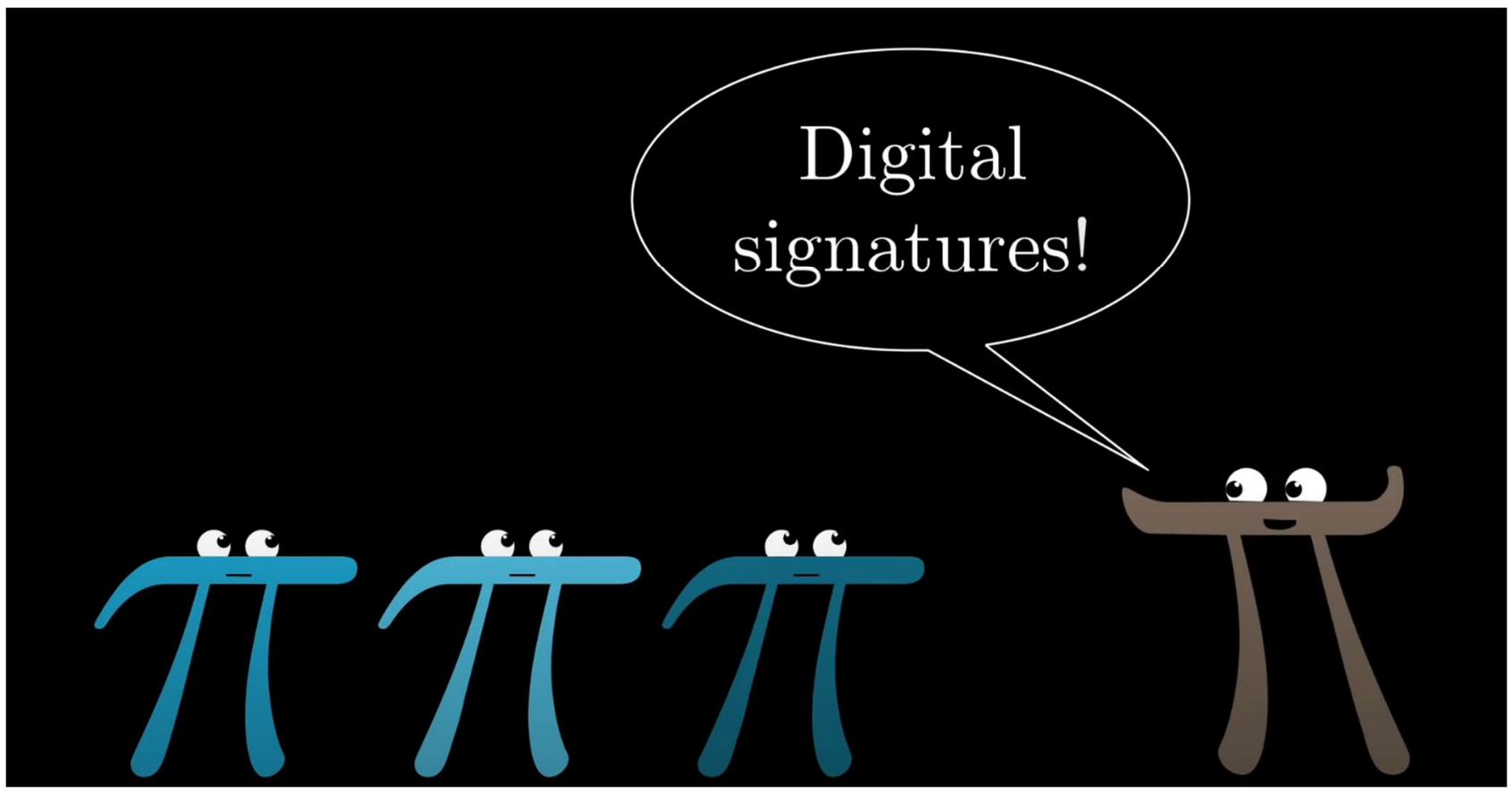
بنابر این محدودیتی وجود ندارد که مانع وارد کردن تراکنشهای خلاف واقع در دفتر کل شود

بنابر این چگونه میشود به چنین دفتر کلی اعتماد کرده و صحت تراکنشهای وارد شده را پذیرفت؟

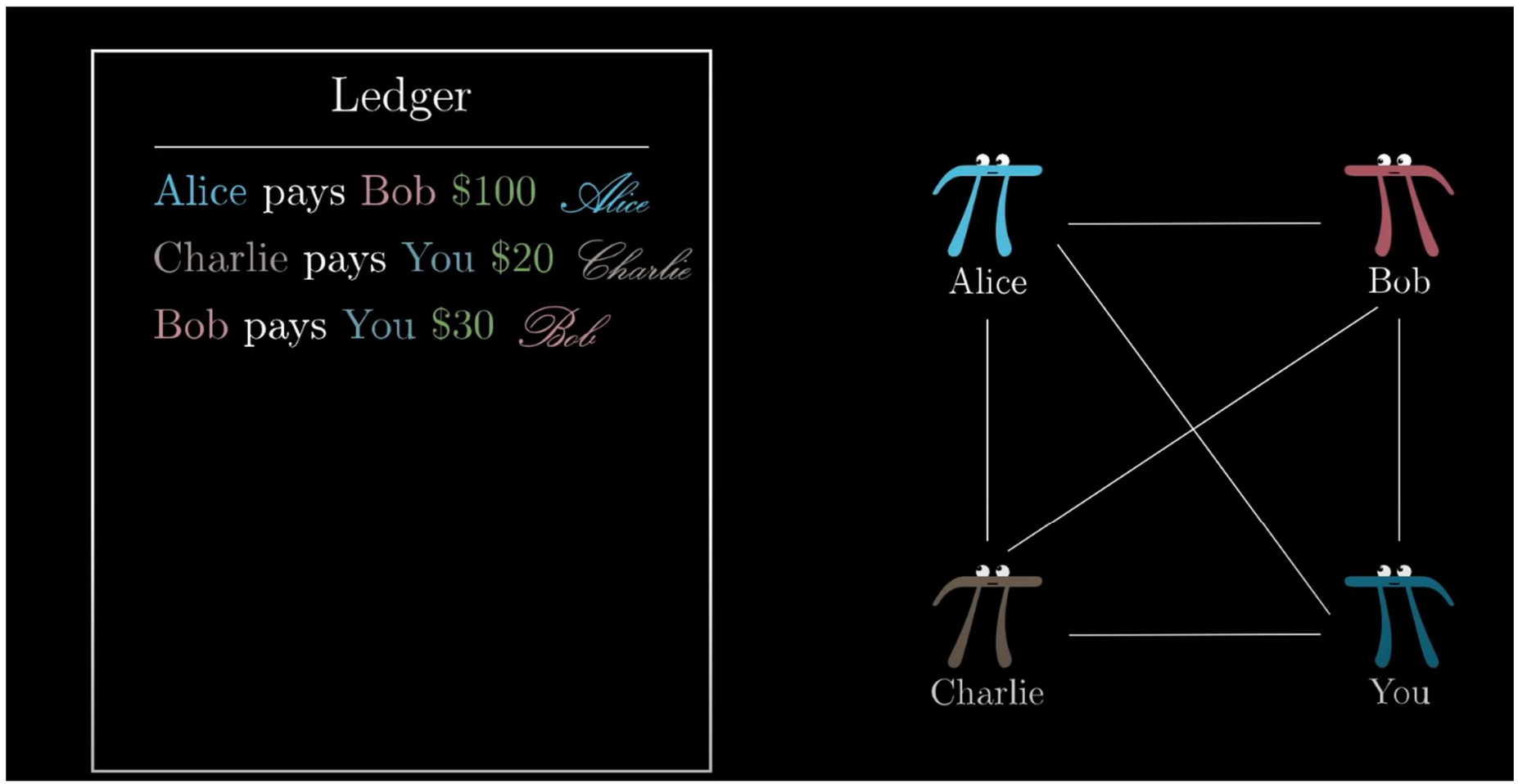


در اینجاست که کریپتوگرافی وارد امور دفتر کل می شود

امضای دیجیتال

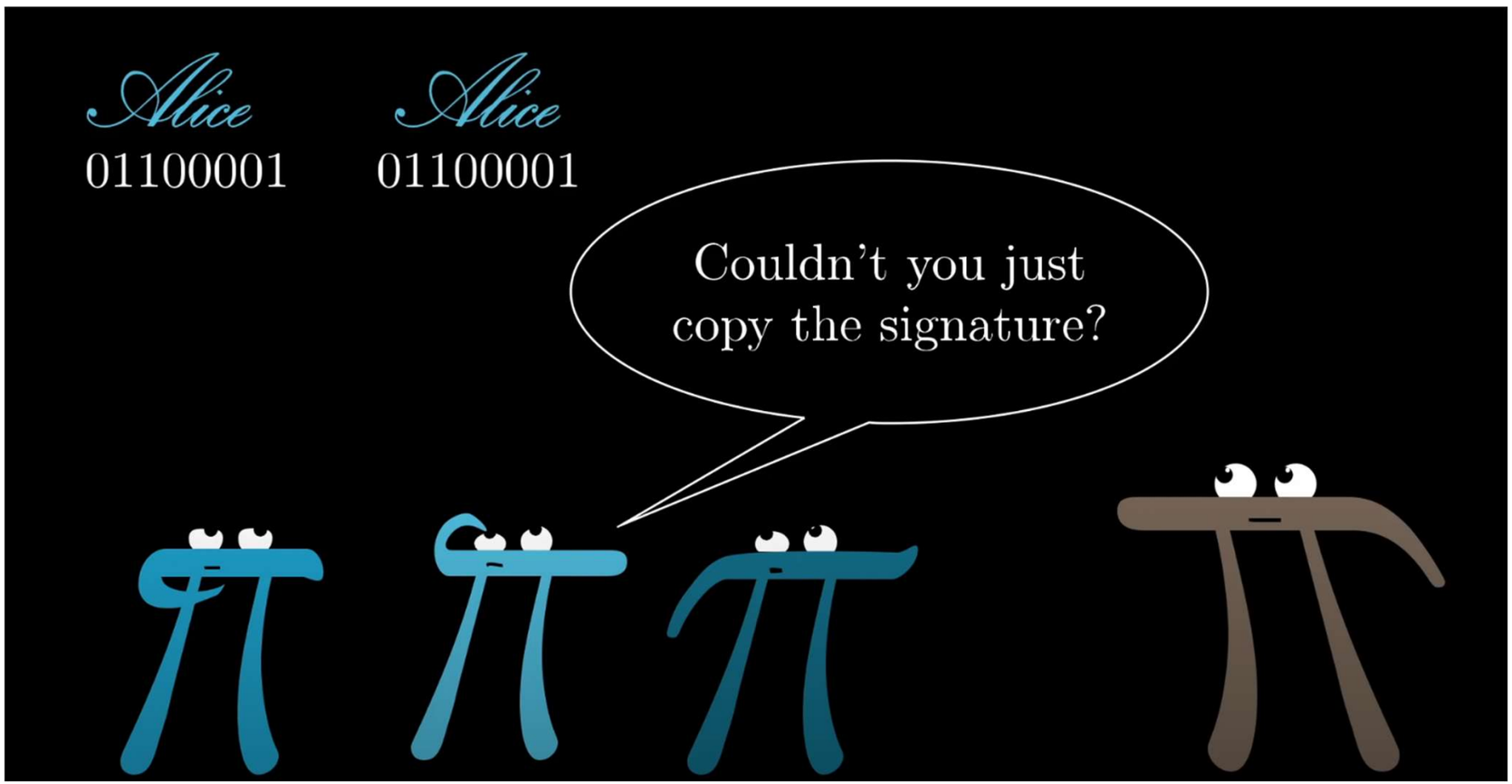


همچون امضای دستنویس، هر شخص میتواند در کنار تراکنشی که در دفتر کل وارد میشود
از امضای دیجیتال جهت تایید صحت آن استفاده کند
بنابراین Bob بدون امضا و تاییدیه Alice نمیتواند در دفتر کل بنویسد که
Alice $100 به Bob باید پرداخت کند

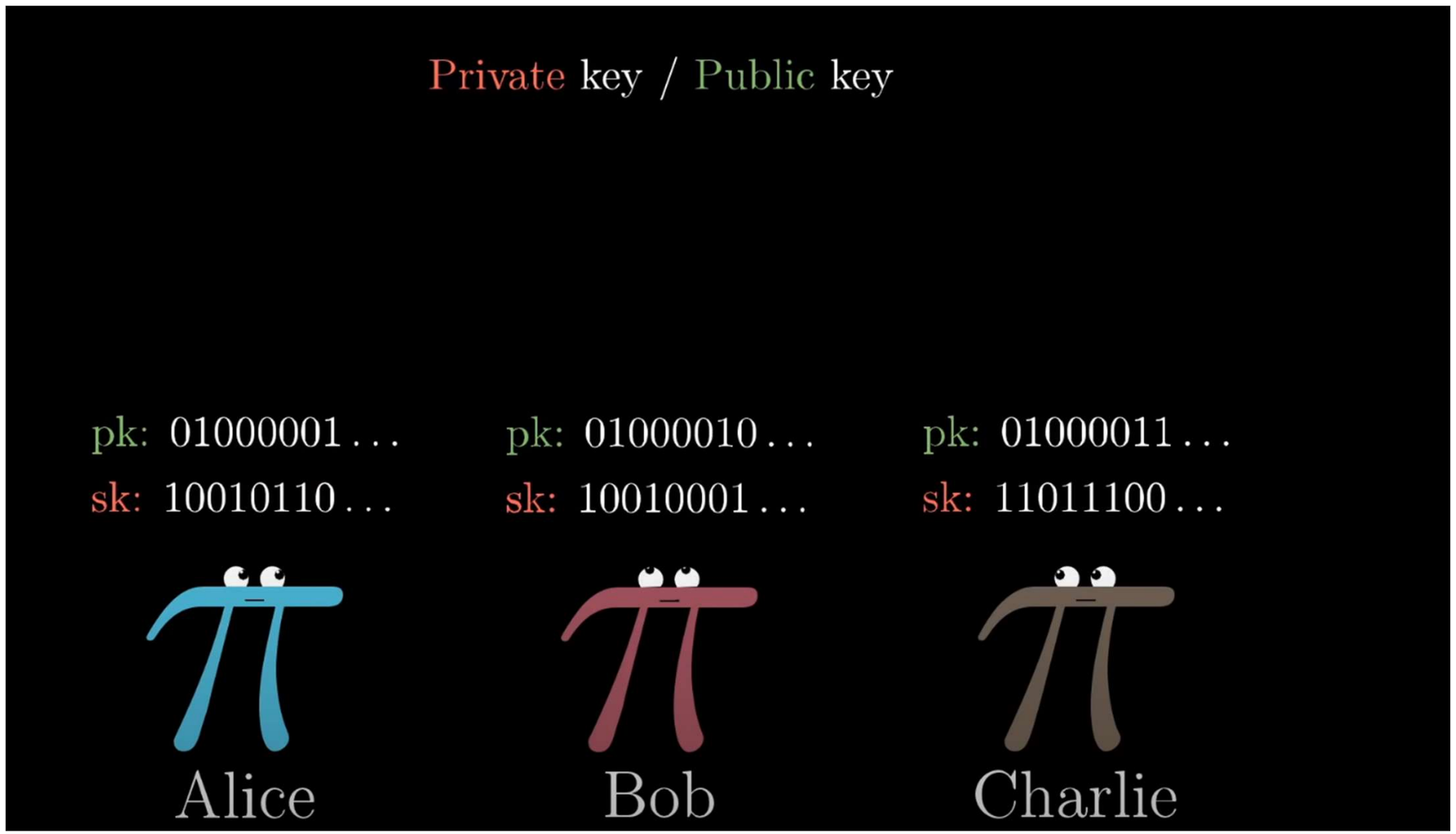


در ابتدا این تصور وجود دارد که امضای دیجیتال قابل کپی کردن میباشد
بنابراین هر کسی میتواند امضای دیگری را کپی کرده و تراکنشهای خلاف واقع را تایید کند

پس چگونه میتوان از جعل پیشگیری کرد؟



نحوه کار به این شکل است هر شخص یک جفت کلید عمومی (Public Key)
و یک کلید خصوصی (Private Key) خواهد داشت

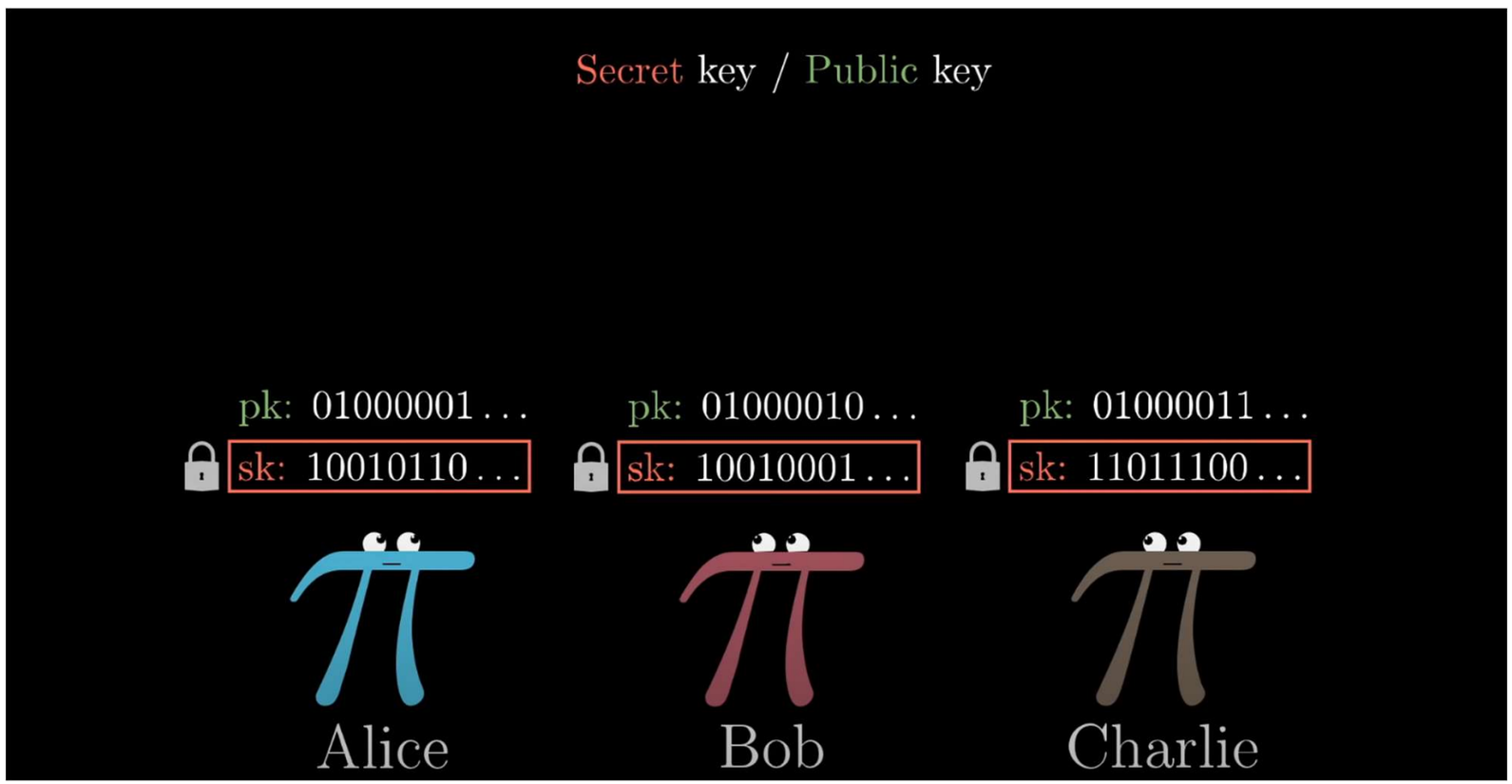


برای راحتی بجای Private Key از واژه Secret Key استفاده میکنیم

Public Key: PK

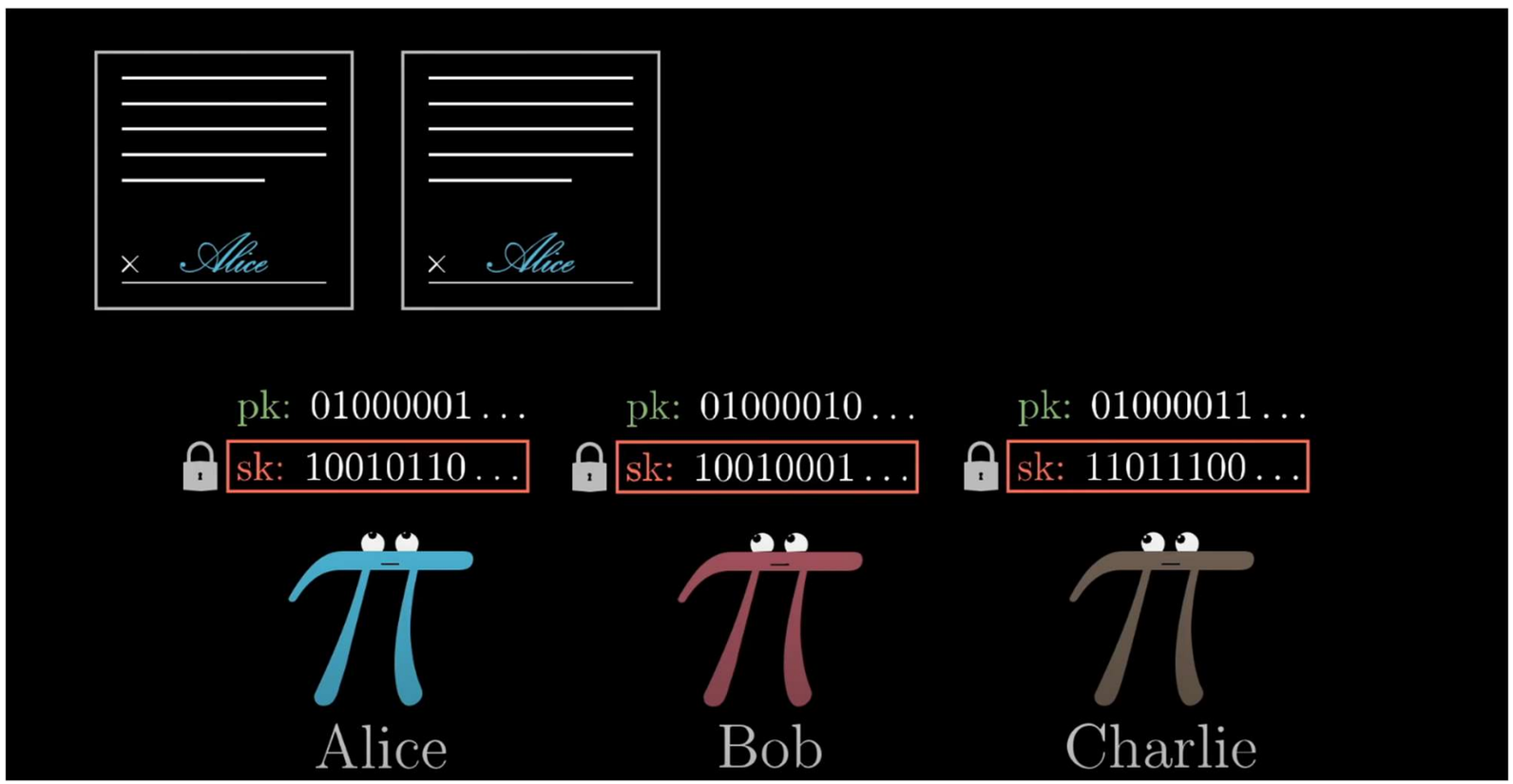
Secret Key: SK

همانگونه که اسم آن مشخص است Secret Key
را باید مخفی و تنها نزد خود نگه دارید

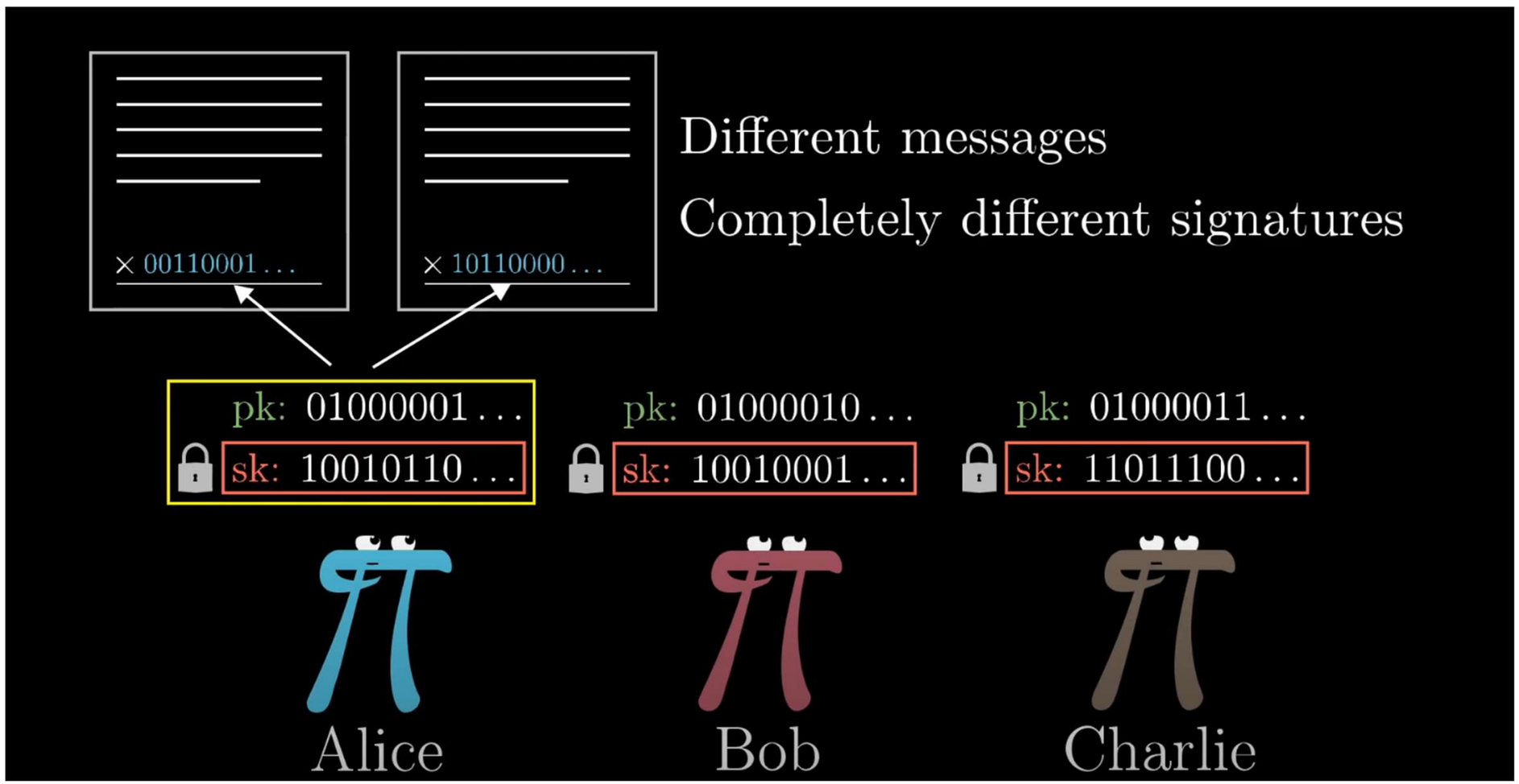


در دنیای واقعی امضای دستنویس شما برای امضای تمام اسناد و مدارک یکسان می باشد

این در حالی است که امضای دیجیتال عملکرد متفاوتی داشته و برای هر پیام، سند یا متنی شکل متفاوتی دارد



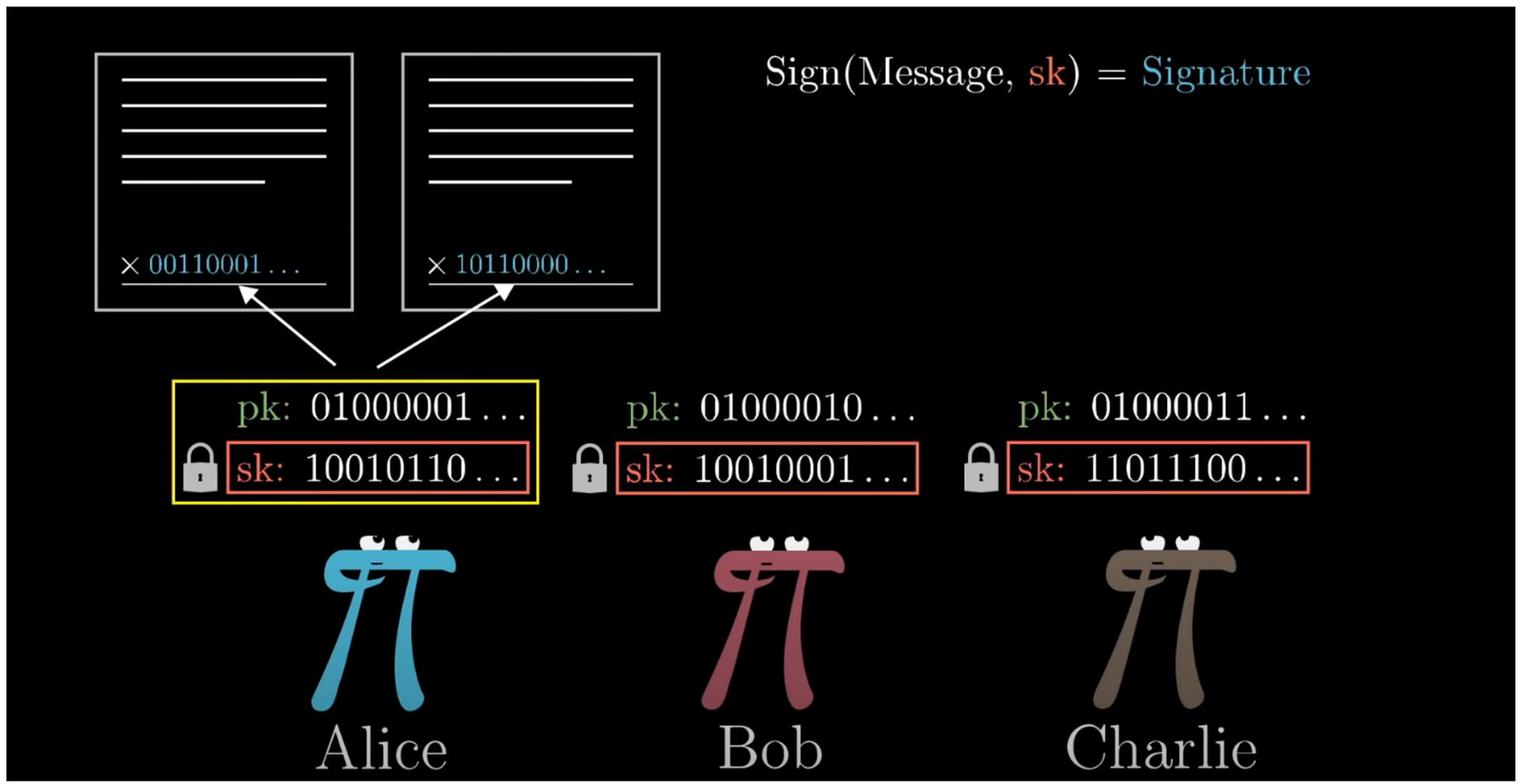
امضای دیجیتال رشته ای از صفر و یک است که برای هر متن ترکیب خاص و متفاوتی داشته
که با کوچکترین تغییر در متن کاملا تغییر میکند



بنابراین امضای دیجیتال نیاز به یک فانکشن یا تابع دارد که ورودی آن متن سند و کلید خصوصی می باشد

> بنابراین بدون داشتن کلید خصوصی نمیتوان امضای دیجیتال را تولید کرد

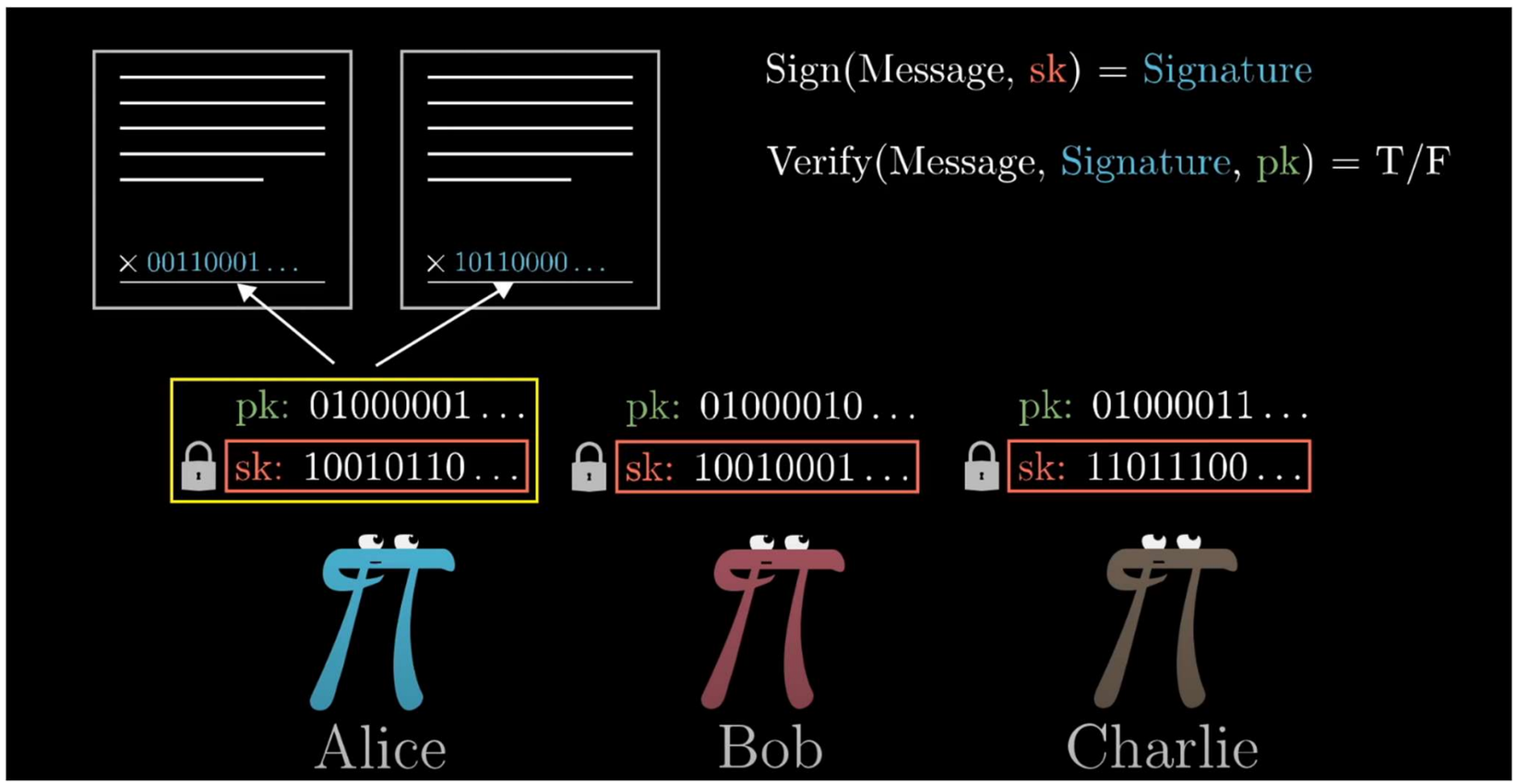
همچنین این پروسه باعث می شود کسی نتواند امضای دیجیتال شما را کپی کرده و در جای دیگر استفاده کند



در کنار تابع تولید امضای دیجیتال، تابع دیگری نیز وجود دارد که کار آن تایید صحت امضا میباشد و در اینجاست که کلید عمومی نقش خواهد داشت

ورودی این تابع متن سند، امضای دیجیتال و کلید عمووی می باشد

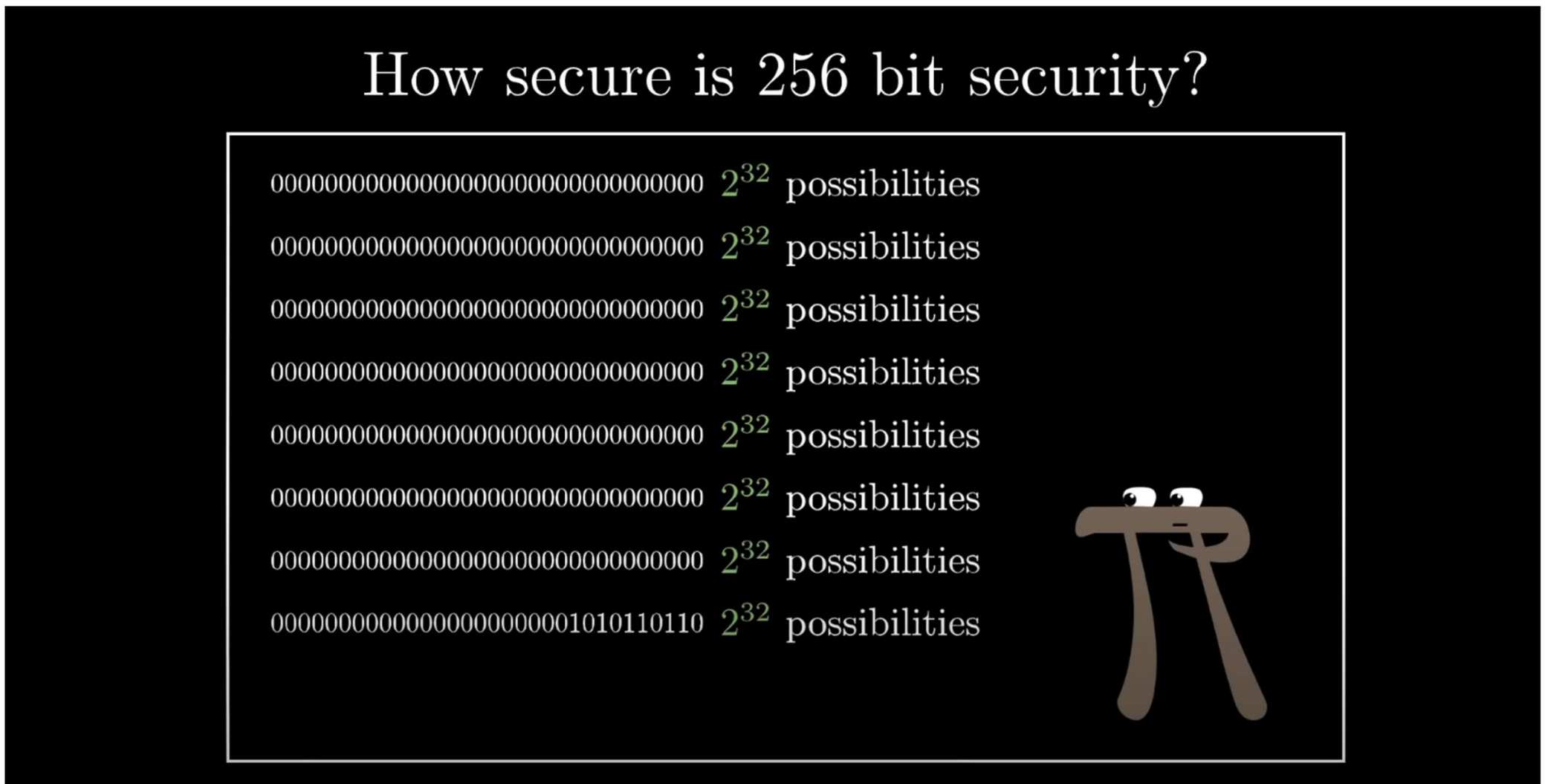
و خروجی آن تنها تایید استفاده از کلید خصوصی وابسته به این کلید عمومی در تولید این امضای دیجیتال است



موضوع مهم این است که بدون داشتن کلید خصوصی امکان تولید امضای صحیح برای یک سند وجود ندارد
و تنها راه آن امتحان کردن تمام ترکیبهای ممکن و حدس و خطا است

تعداد امضاهای ممکن برای یک رشته 256 بیت؟

امنیت رشته امنیتی 256 بیت چقدر است؟



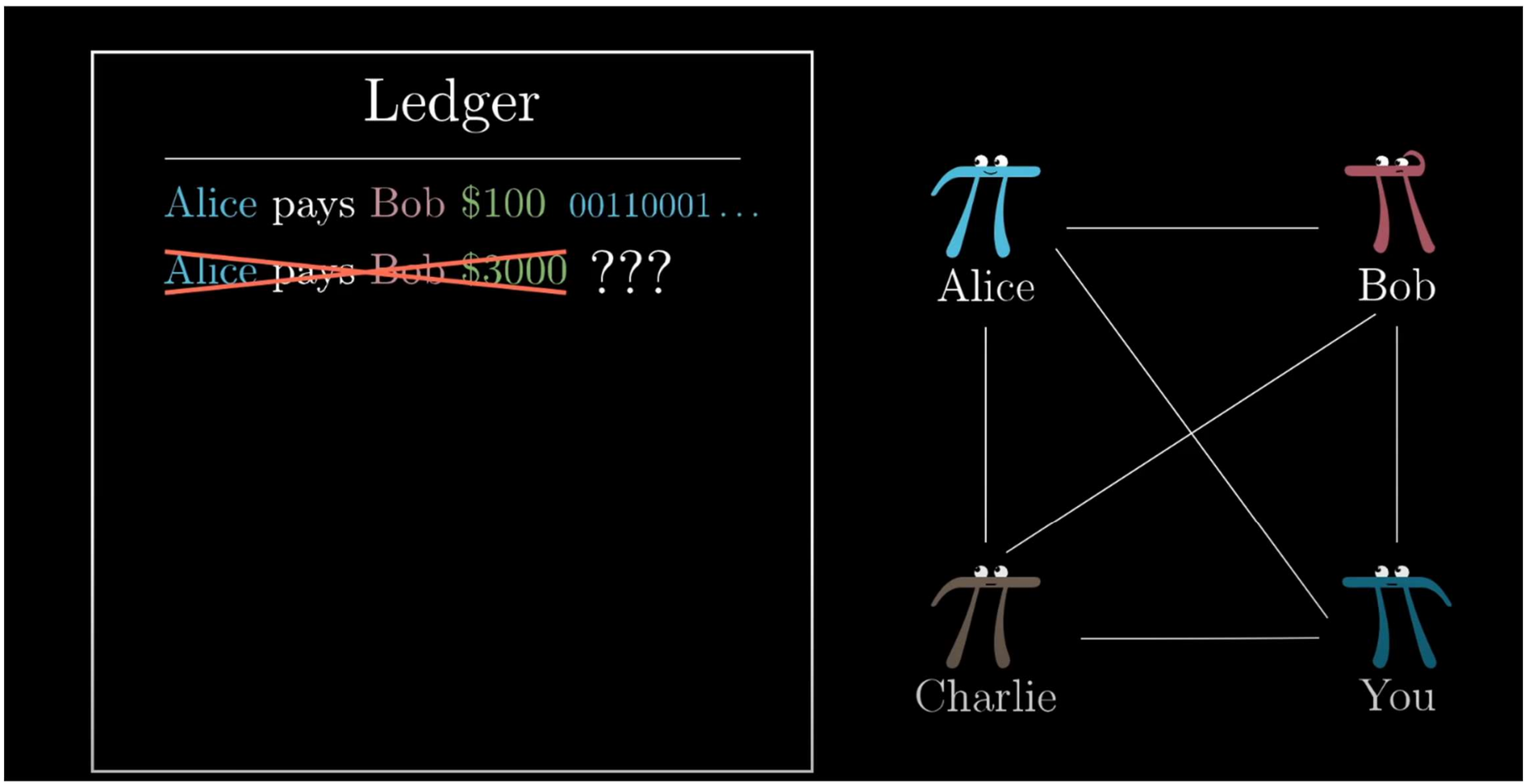
How secure is 256 bit security?

00000000000000000000000000000000	4 Billion possibilities
00000000000000000000000000000000	4 Billion possibilities
00000000000000000000000000000000	4 Billion possibilities
00000000000000000000000000000000	4 Billion possibilities
00000000000000000000000000000000	4 Billion possibilities
00000000000000000000000000000000	4 Billion possibilities
00000000000000000000000000000000	4 Billion possibilities
00000000000000000000001101000110	4 Billion possibilities

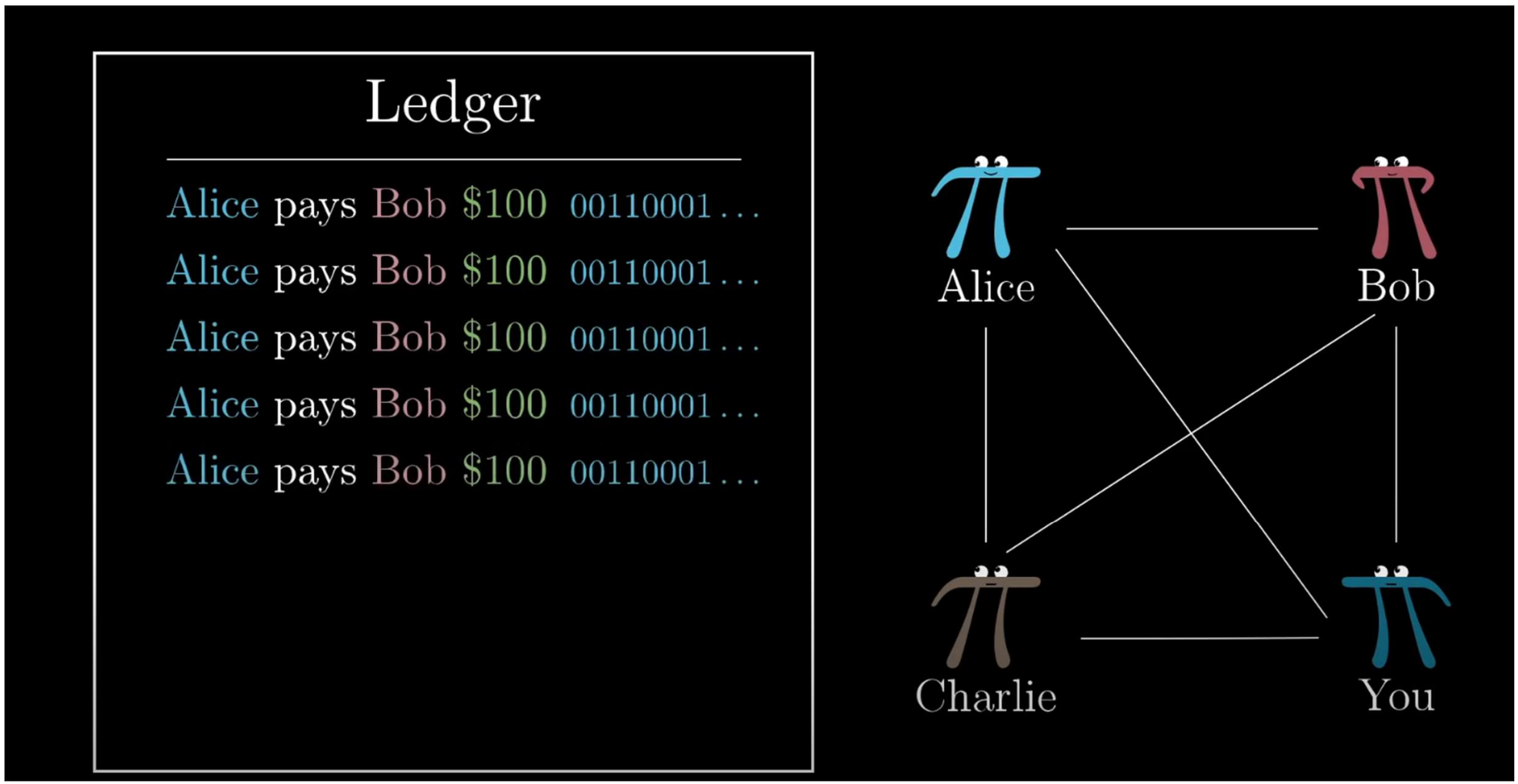
بنابراین در صورتی که تابع تایید امضا صحت آن را اعلام کرد میتوانید با اطمینان خاطر آن را بپذیرید
چرا که تنها راه تولید این امضا داشتن کلید خصوصی وابسته به این کلید عمومی است

اکنون با وجود امضای دیجیتال کسی نمیتواند تراکنش جدیدی را بدون تاییدیه پرداخت کننده در دفتر کل وارد کند

اما مشکل دیگری وجود دارد

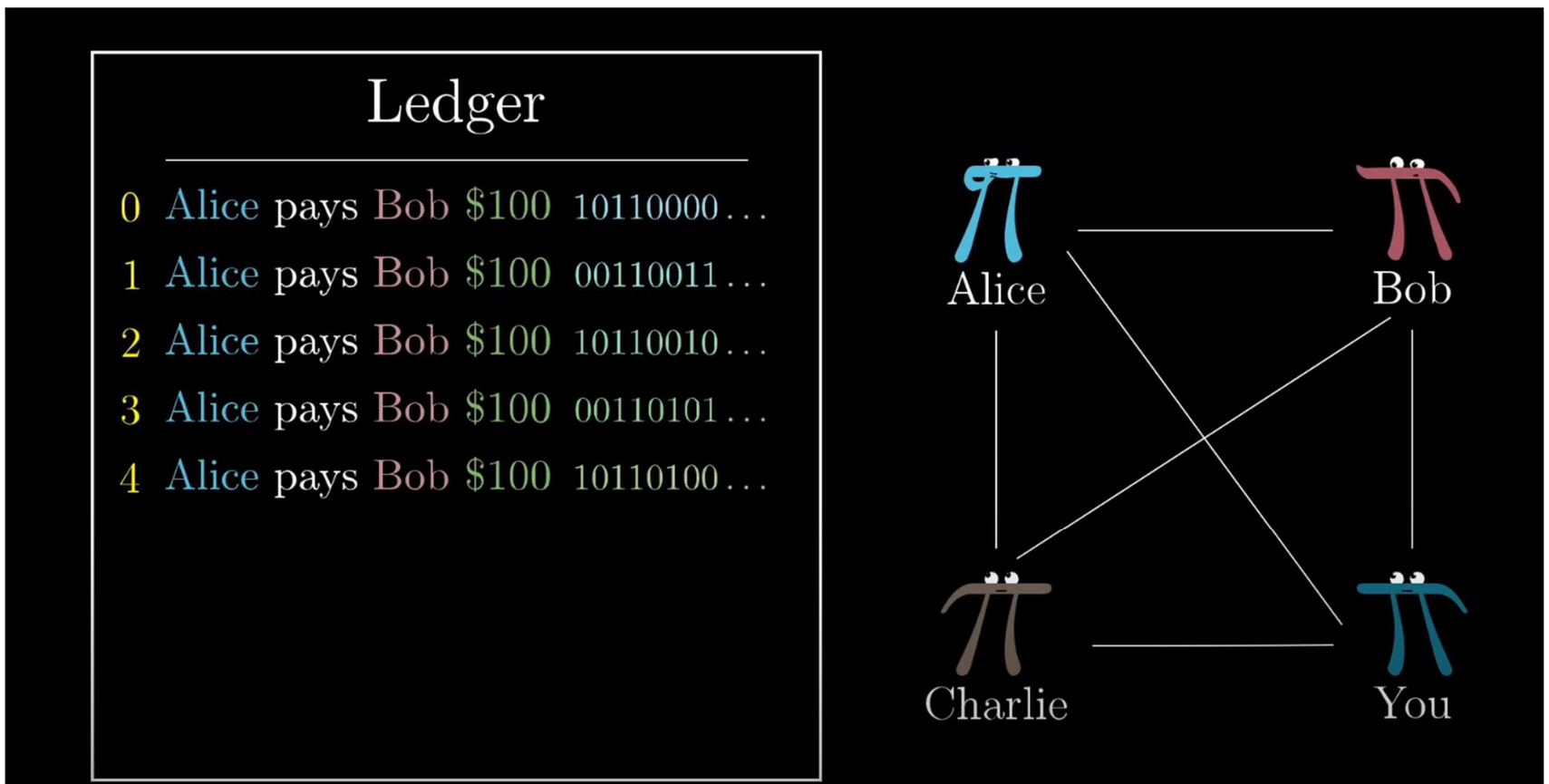


با وجود اینکه بدون داشتن کلید خصوصی نمیتوان تراکنش جدیدی را وارد دفتر کرد
اما میتوان یک تراکنش را به همراه امضای دیجیتال آن کپی کرده و چندین بار وارد دفتر کرد



برای رفع این مشکل به هر تراکنش یک شناسه اختصاص داده میشود
بنابراین تراکنش جدید حتی اگر مبلغ و طرفین یکسانی هم داشته باشد
باید شناسه متفاوتی داشته باشد

حال به دلیل شناسه جدید و تغییر متن سند نیاز به تولید امضای جدید میباشد
که تنها دارنده کلید خصوصی میتواند این امضا را تولید نماید

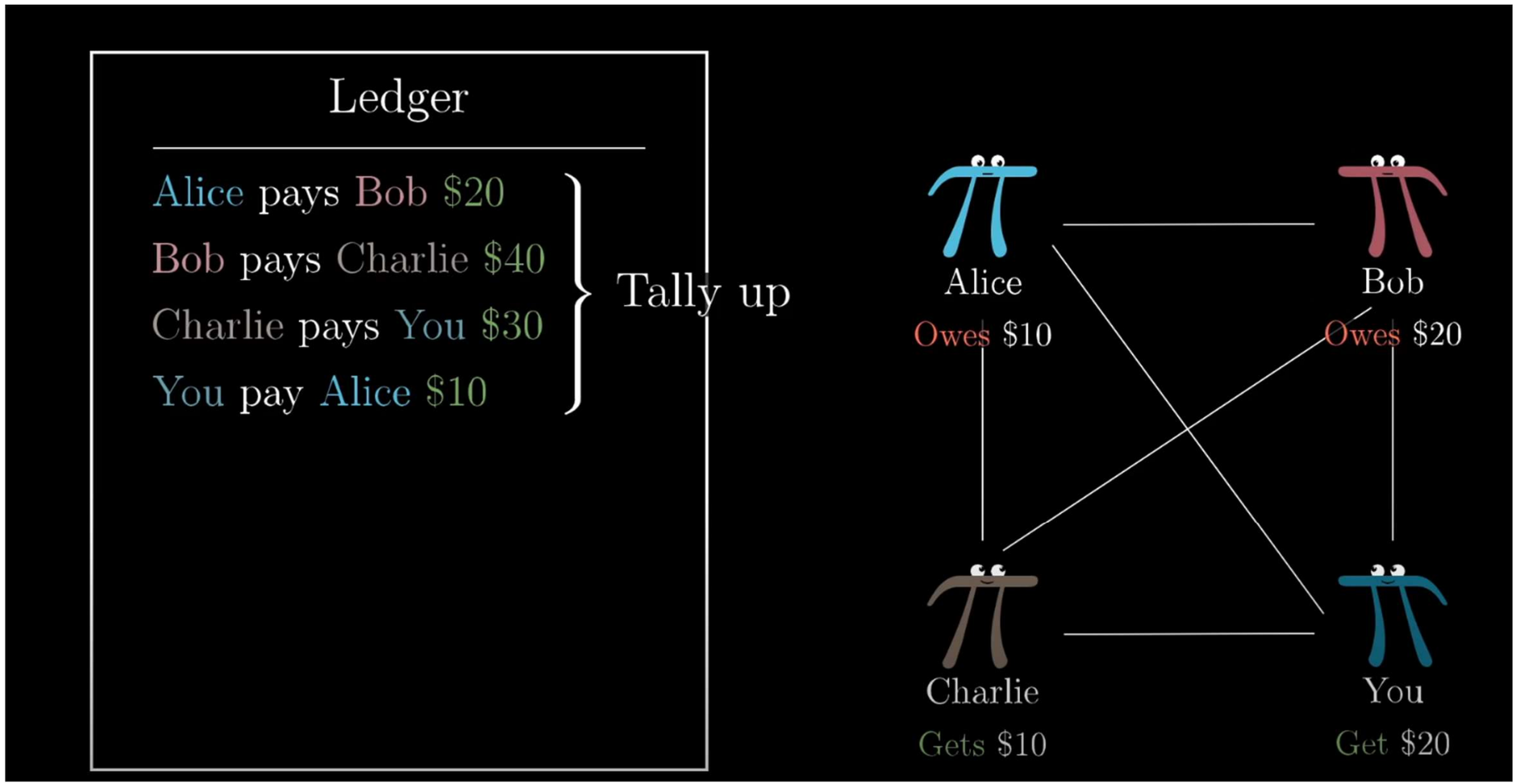


Protocol

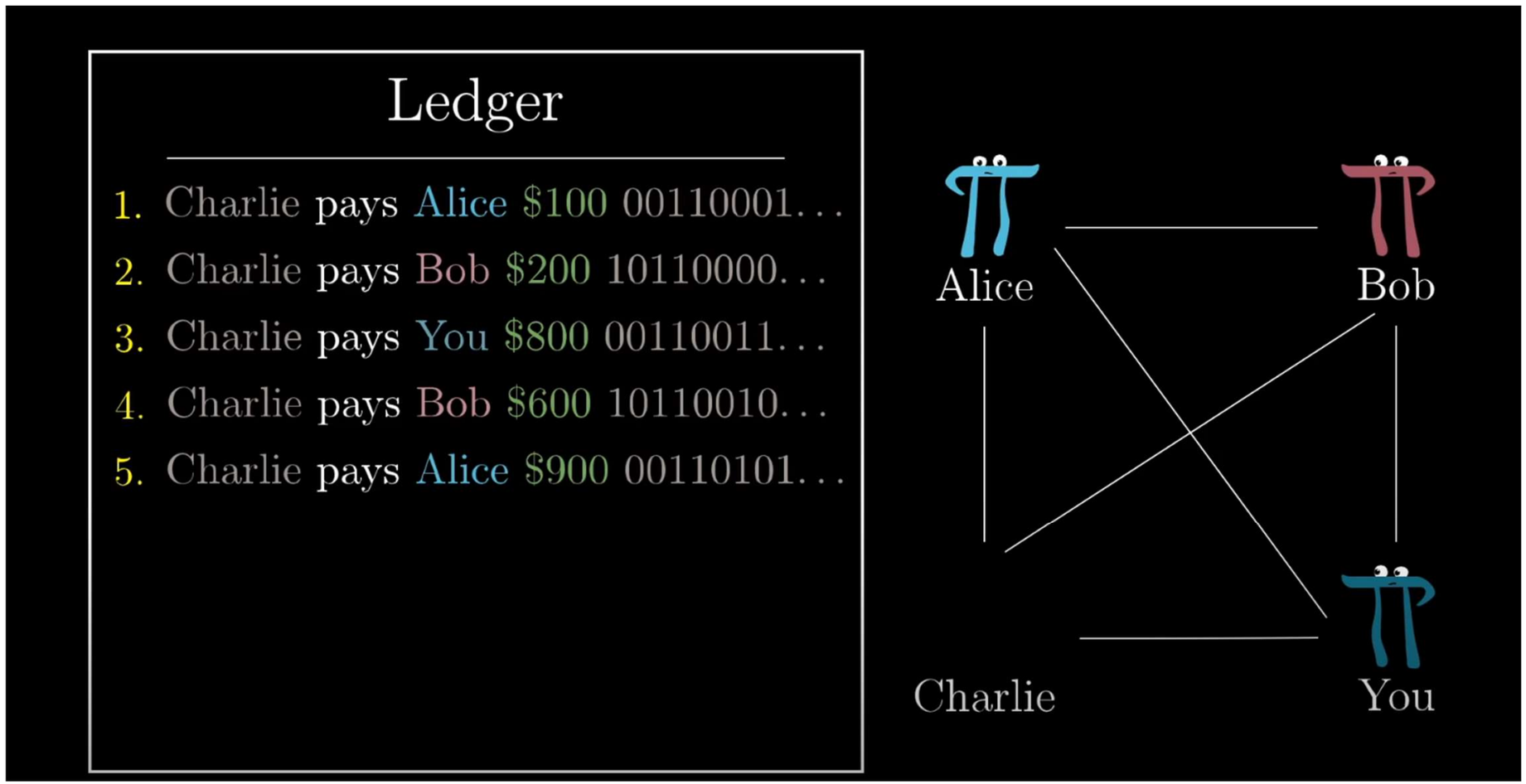
- Anyone can add lines to the Ledger
- Settle up with real money each month
- Only signed transactions are valid

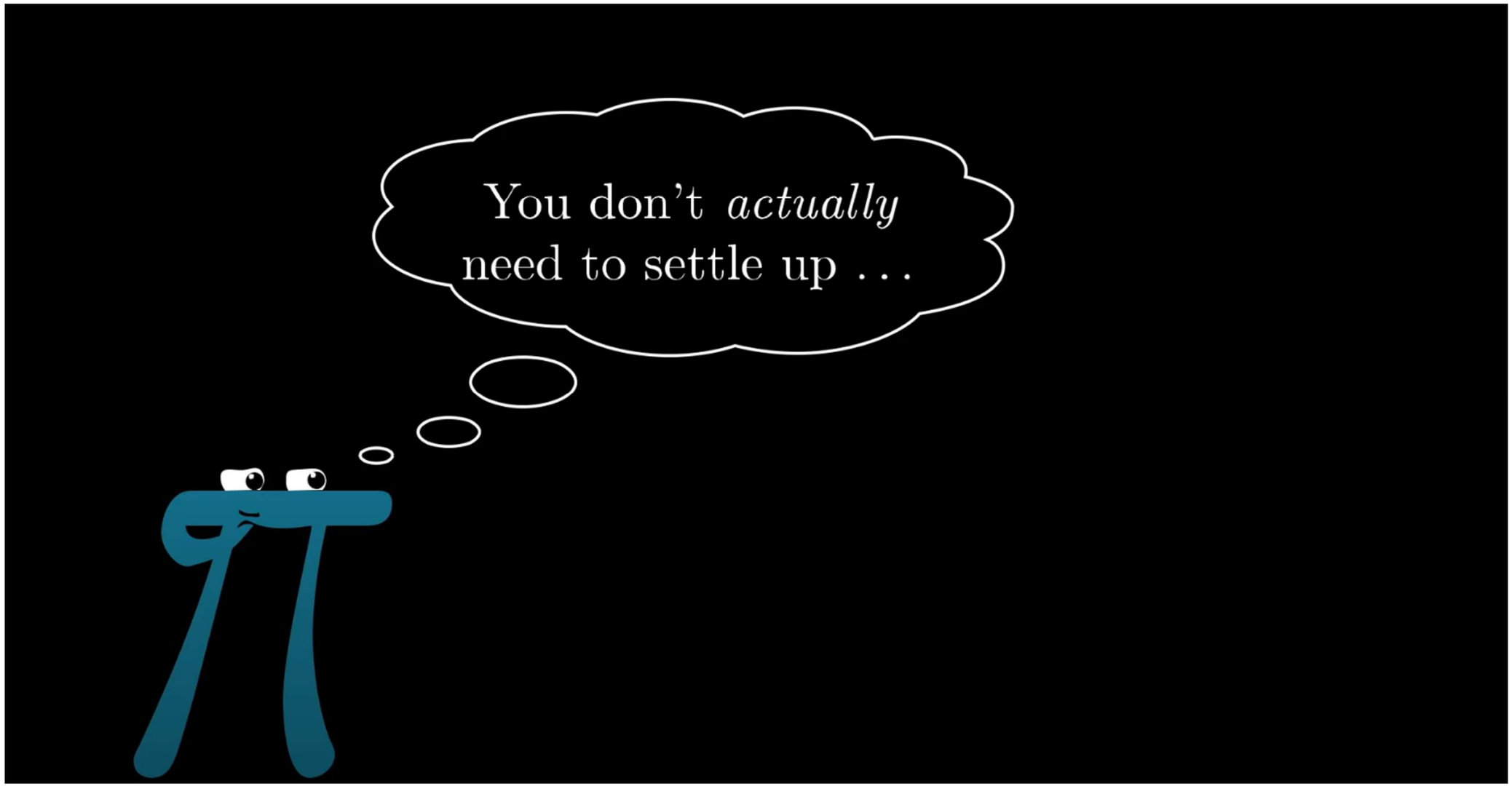
شرایط استفاده از دفتر کل:
هر کسی می تواند در دفتر تراکنش وارد کند
در پایان هر ماه حسابها رسیدگی شده و صفر گردد
تنها تراکنشهای امضا شده معتبر هستند

با وجود تمامی موارد در نظر گرفته شده نیاز به اعتماد به اشخاص همچنان وجود دارد
چرا که این روال در صورتی با مشکل مواجه نمیشود که در پایان ماه همه بدهی خود را پرداخت کنند



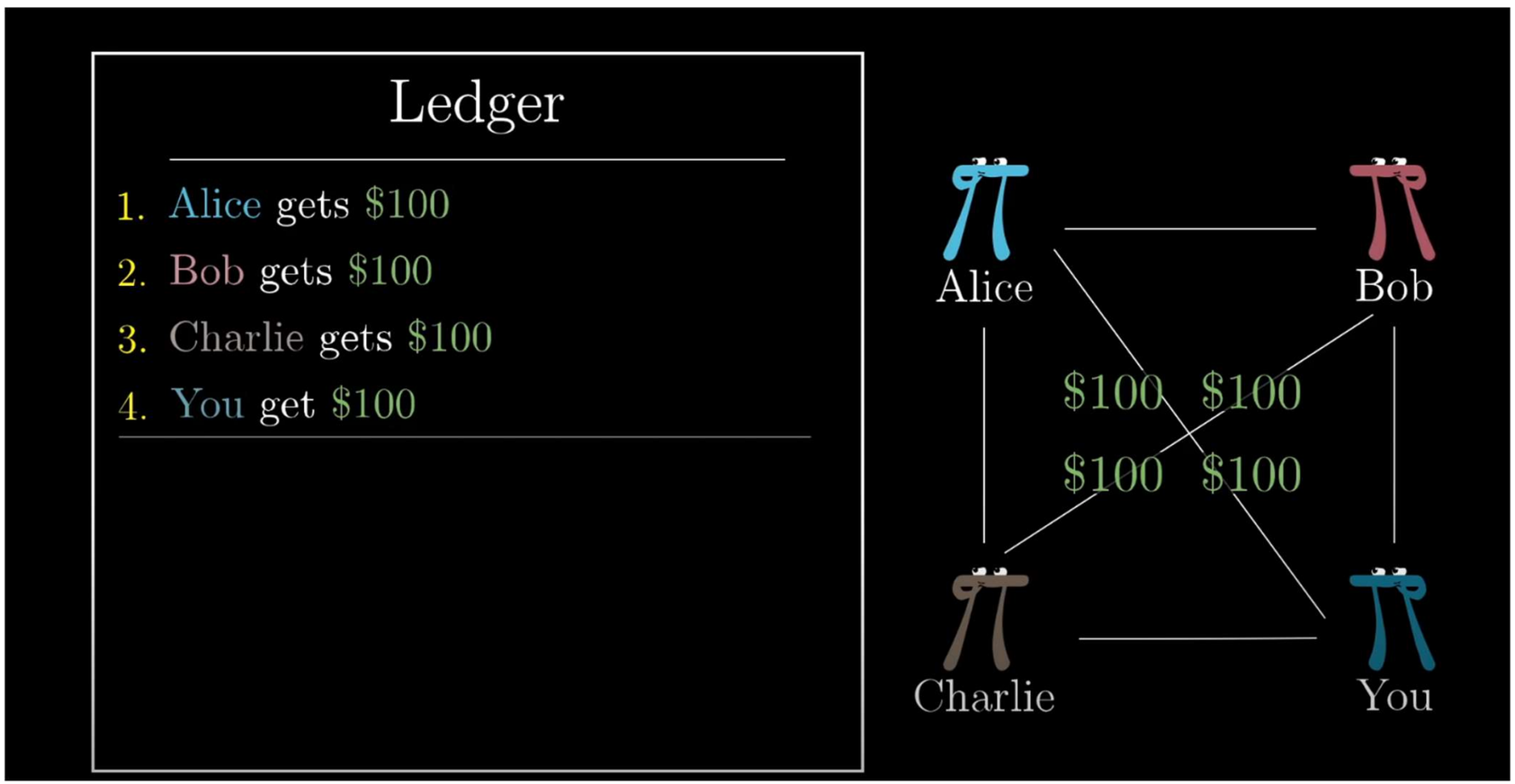
اگر Charlie در طول ماه مدام قرض کرده و در پایان ماه غیب شود چه باید کرد؟





افراد تنها در صورتی که میزان بدهیشان بیشتر از طلبشان باشد امکان فرار و عدم تسویه حساب را دارند

بنابراین اگر در ابتدای ماه هر نفر مبلغی را وارد حساب مشترک نماید
و امکان انجام تراکنش تنها تا سقف مبلغ به اشتراک گذاشته شده باشد
در پایان ماه نیاز به پرداخت بدهی از طرف کسی نمیباشد

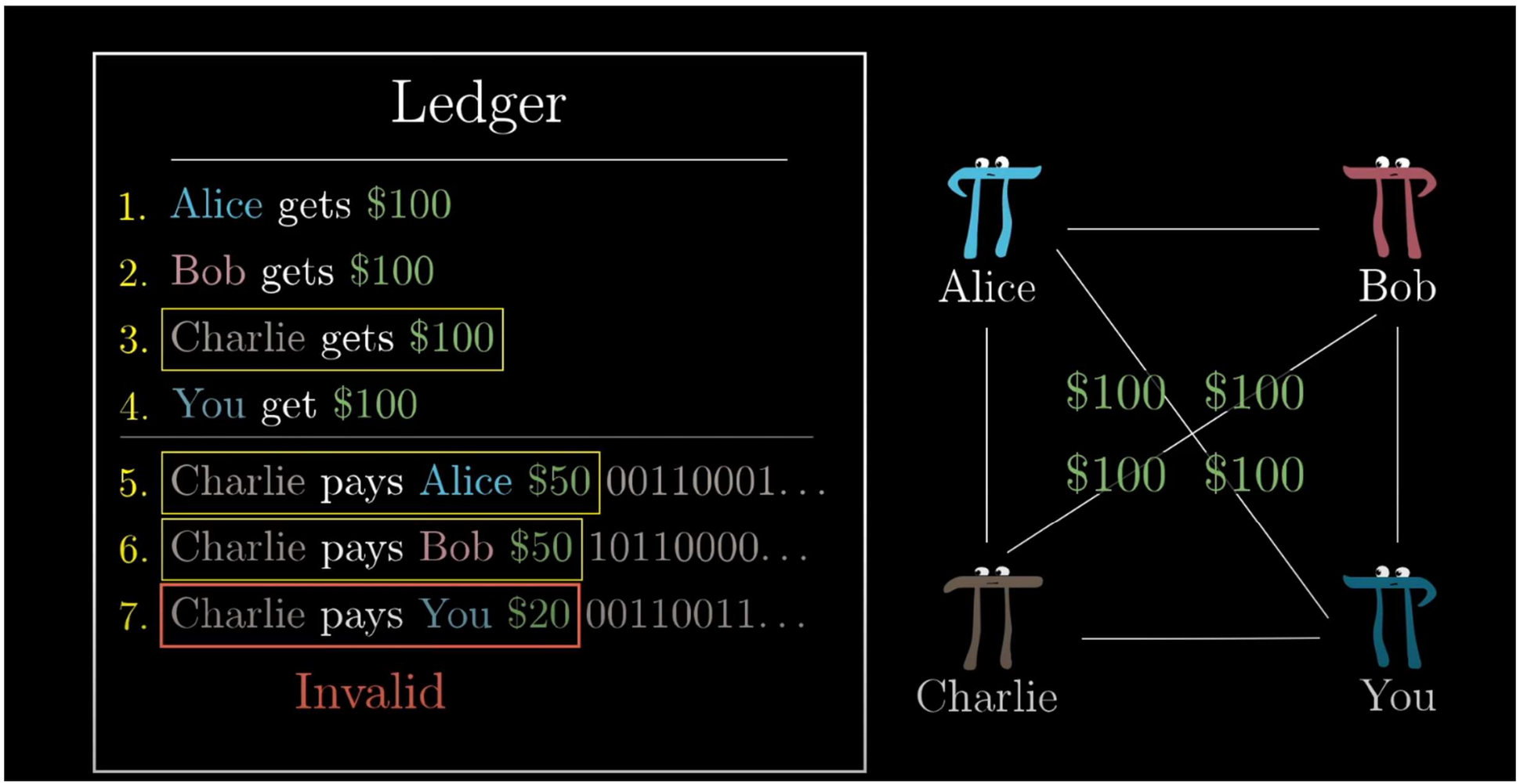


Protocol

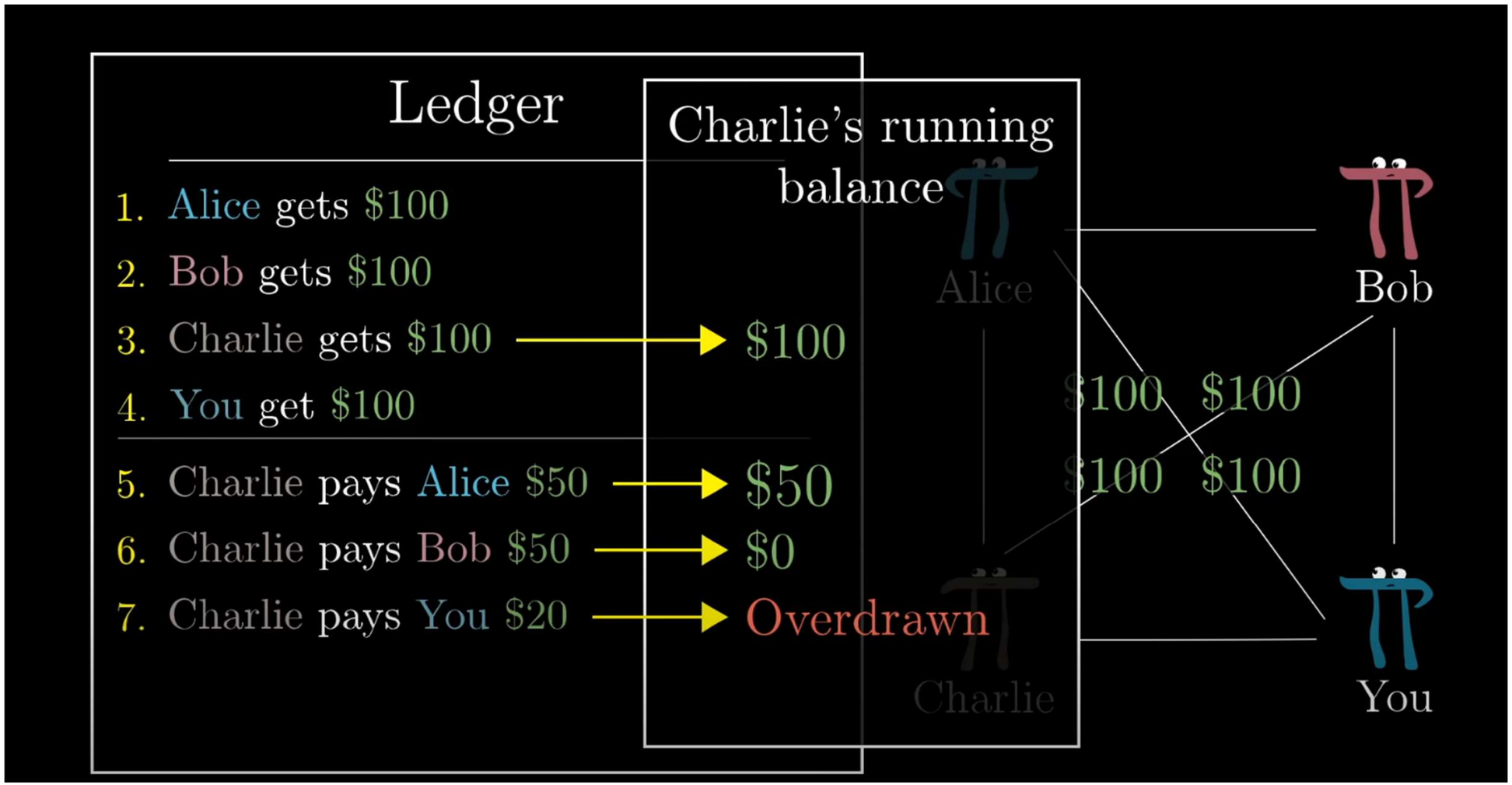
- Anyone can add lines to the Ledger
- Only signed transactions are valid
- No overspending

شرایط استفاده از دفتر کل:
هر کسی می تواند در دفتر تراکنش وارد کند
تنها تراکنشهای امضا شده معتبر هستند
تنها تا سقف موجودی میتوان هزینه کرد

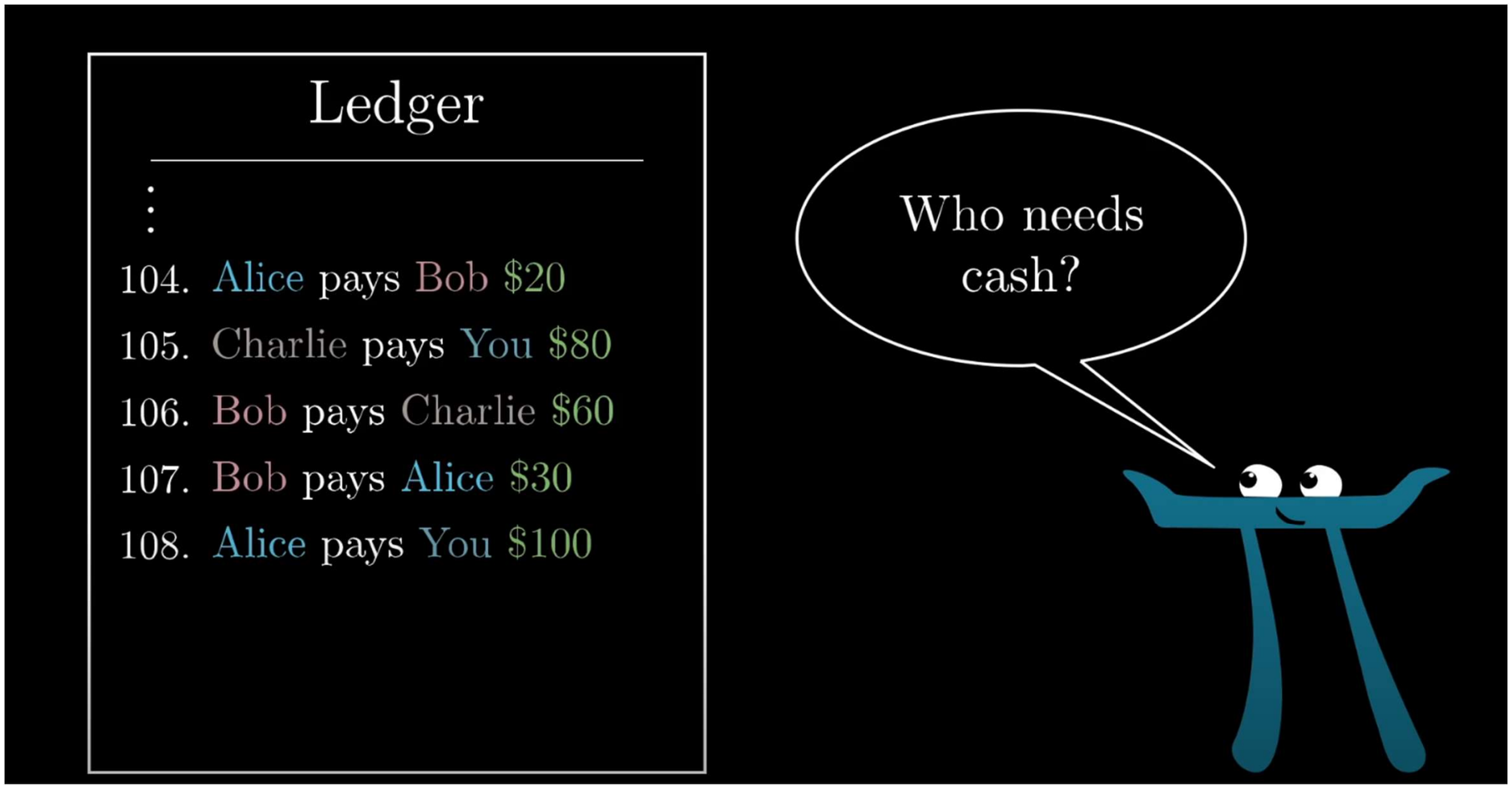
بنابراین در صورتی که طی دو تراکنش اول Charlie تمامی موجودی خود را هزینه کند
تراکنش سوم برای او تایید نمیشود همانند زمانی که امضای او اشتباه باشد



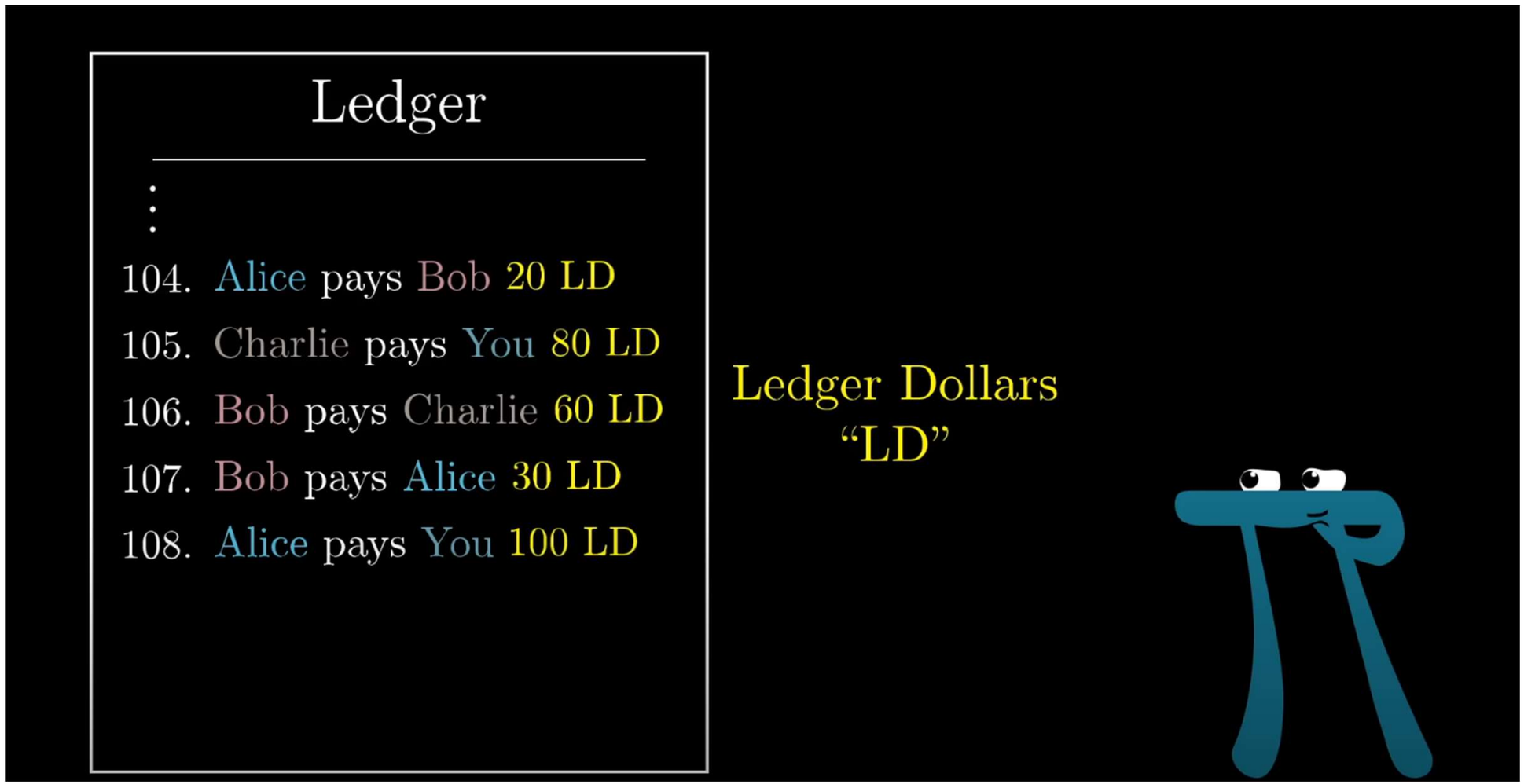
این امر نیازمند دانستن سوابق تراکنشها میباشد تا از موجودی
هر شخص و سقف هزینه او بتوان اطمینان حاصل کرد



این پروسه در صورت استفاده از جانب همه افراد و ادامه داشتن وابستگی خود به $ را از دست می دهد
و دیگر نیازی به تسویه و پرداخت با $ یا هر پول دیگری نیست

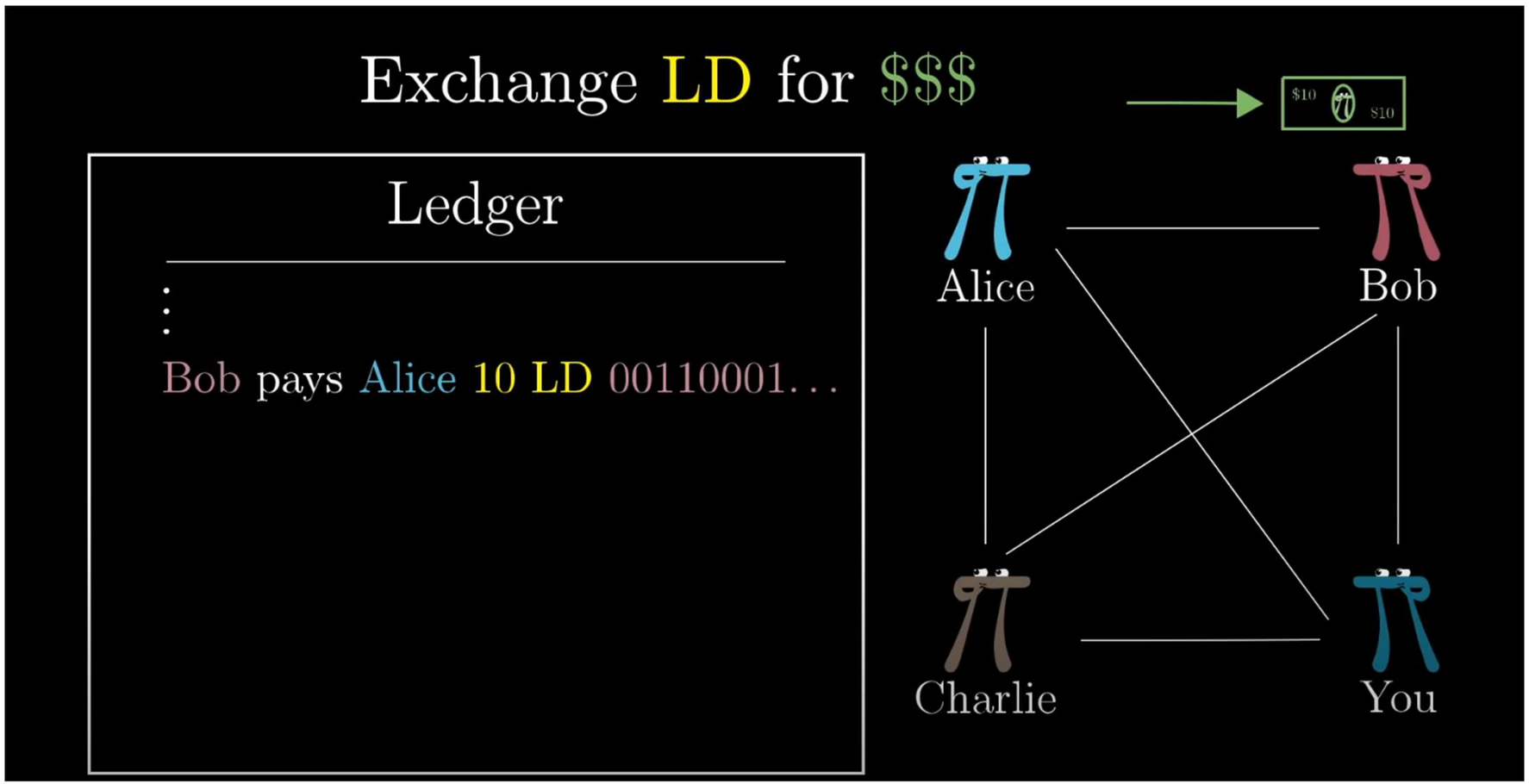


در نتیجه میتوان پول مورد تبادل در دفتر کل را با نامی جدید برچسب زد

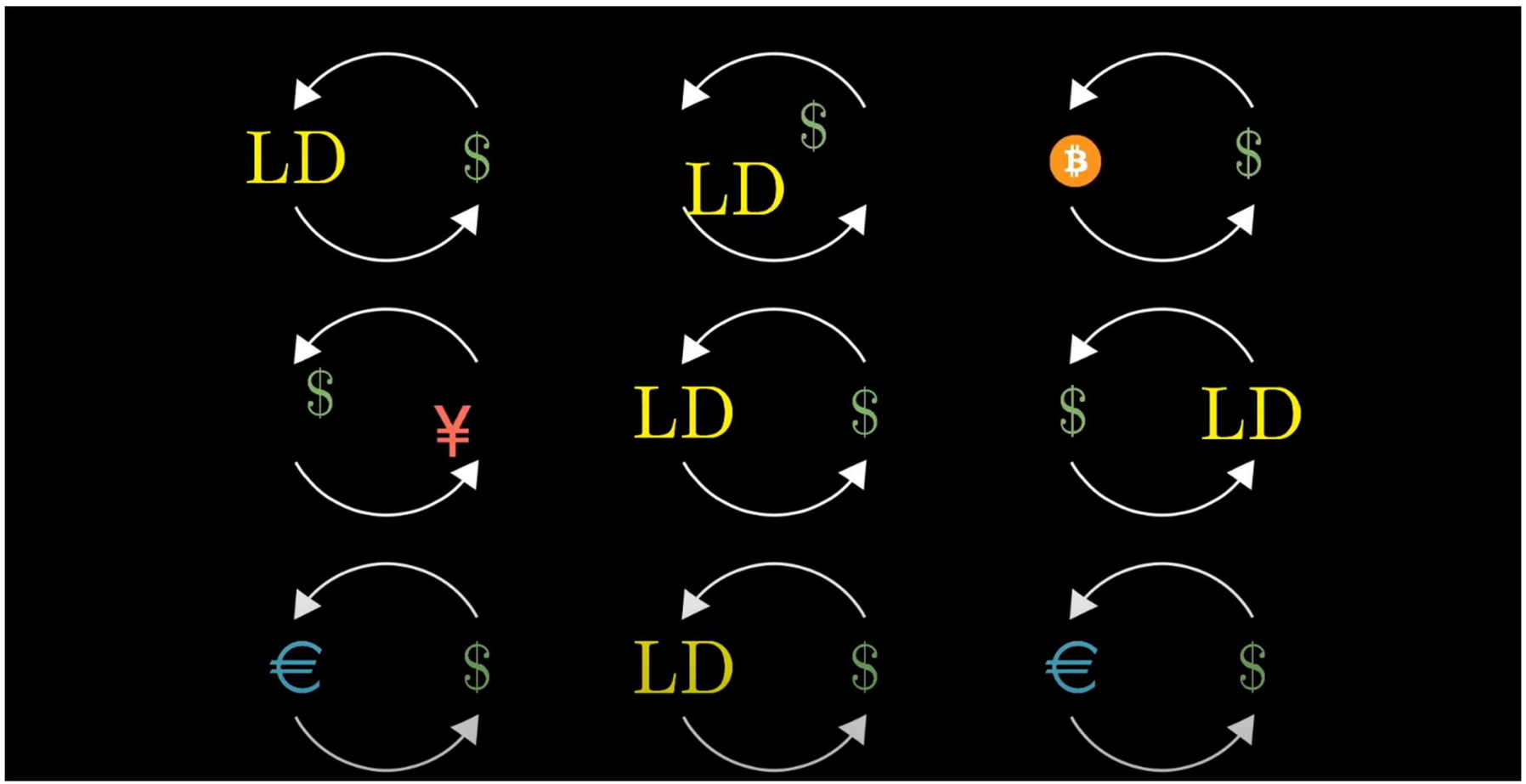


هرچند همچنان میتوان در صورت نیاز پول موجود در دفتر کل را با $ معاوضه کرد

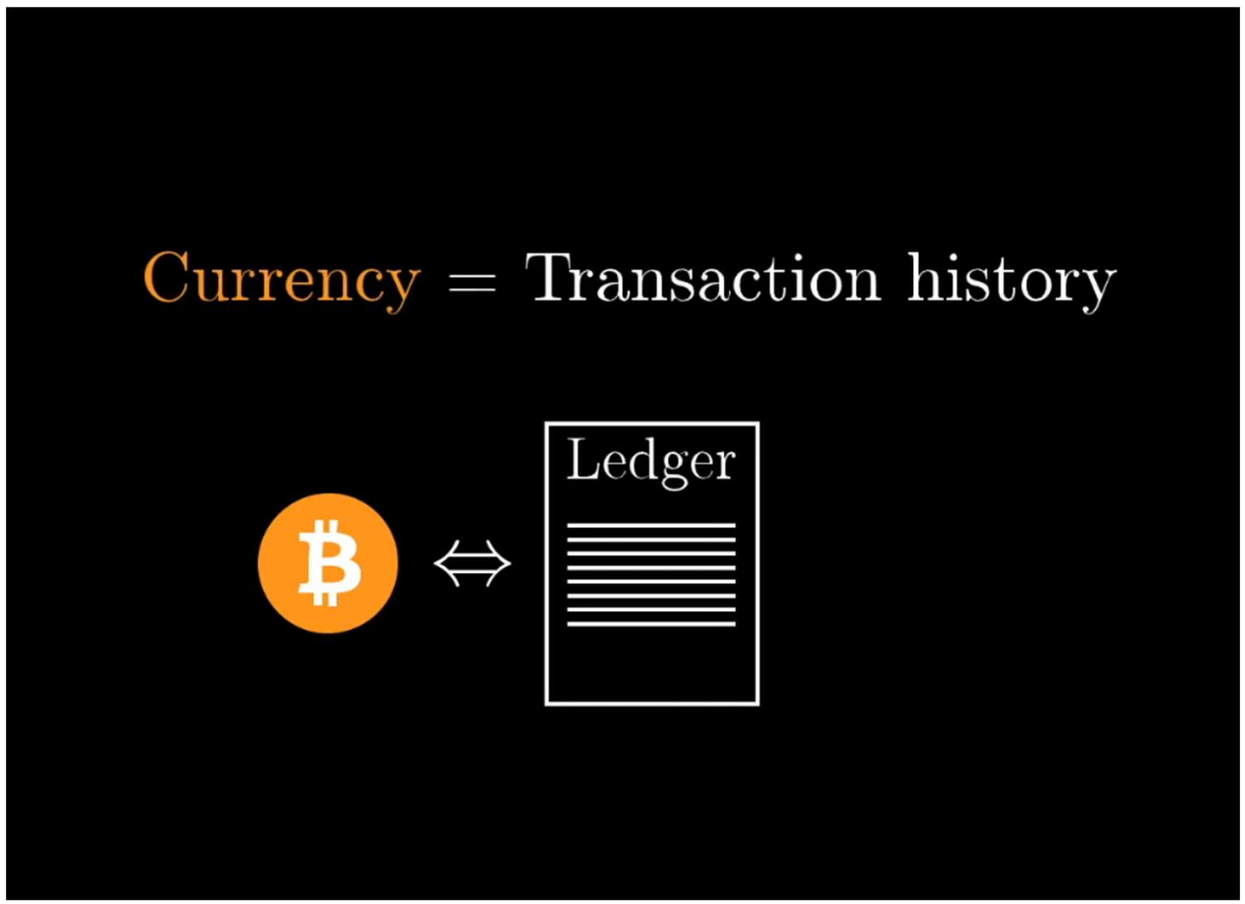
به عنوان مثال Alice میتواند مبلغی در وجه $ به Bob پرداخت کند
و بجای آن معادلش LD دریافت کند و در دفتر کل وارد شود



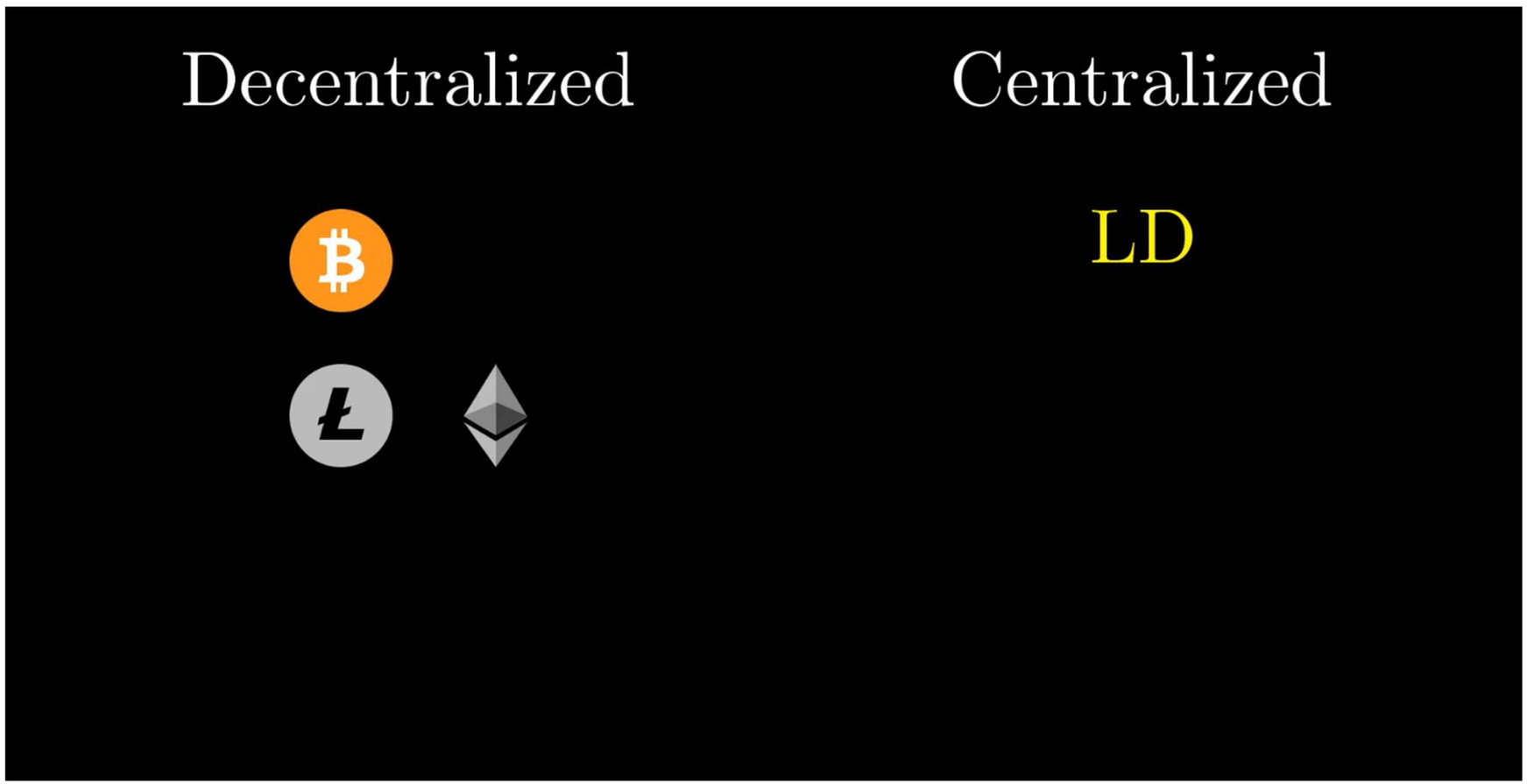
باید به این موضوع توجه داشت که چنین تبادلاتی را پروتوکل تعریف شده نمیتواند تضمین کند
زیرا این تبادل ارز که توسط کارگزاری یا شخصی انجام میشود قوانین خودش را دارد
و از قوانین دفتر کل تبعیت نمیکند



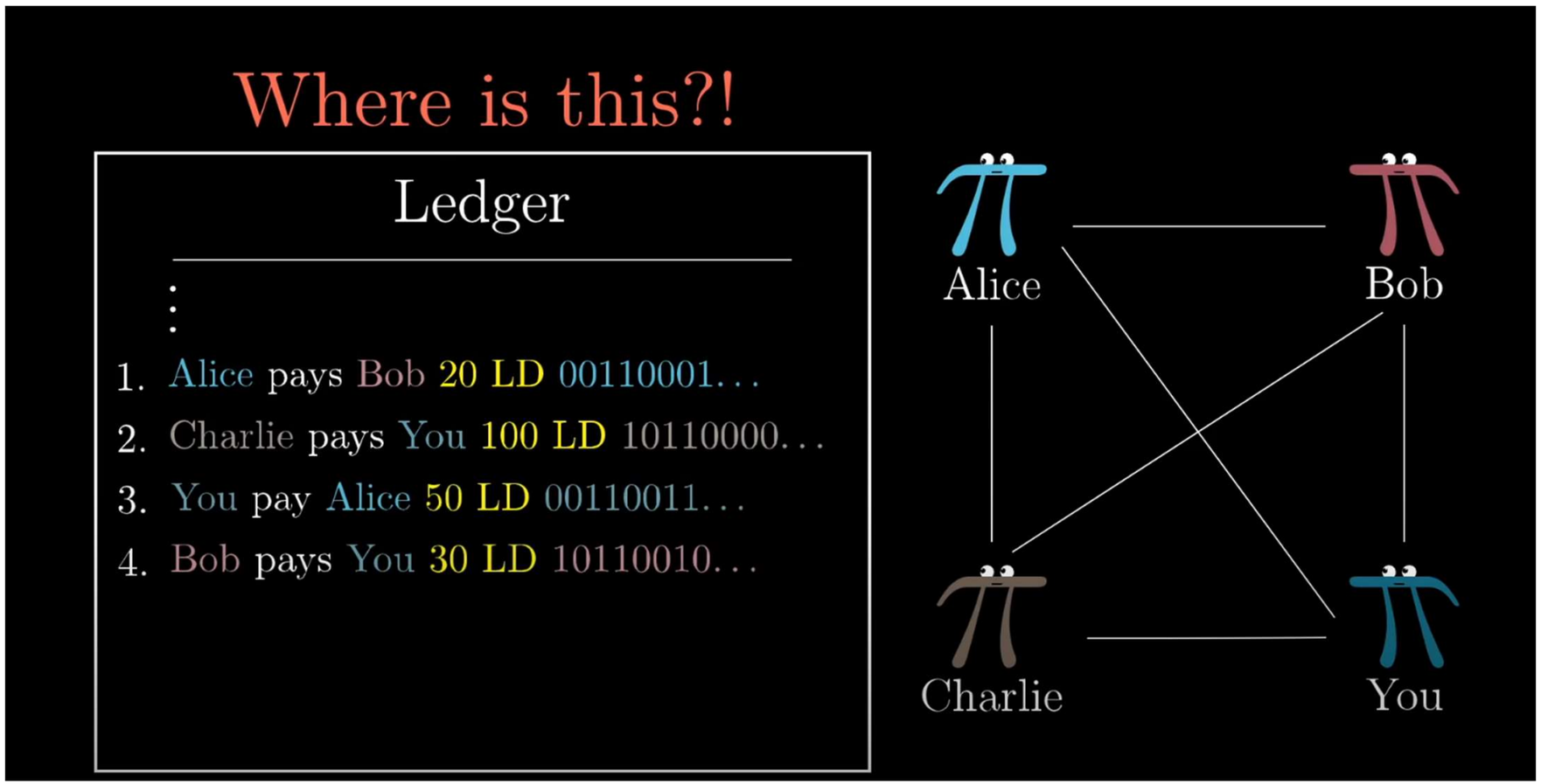
باید توجه داشت که بیتکوین یا بقیه رمزارزها چیزی نیستند جز دفتر کل عمومی
یا به عبارت دیگر سوابق تراکنشها



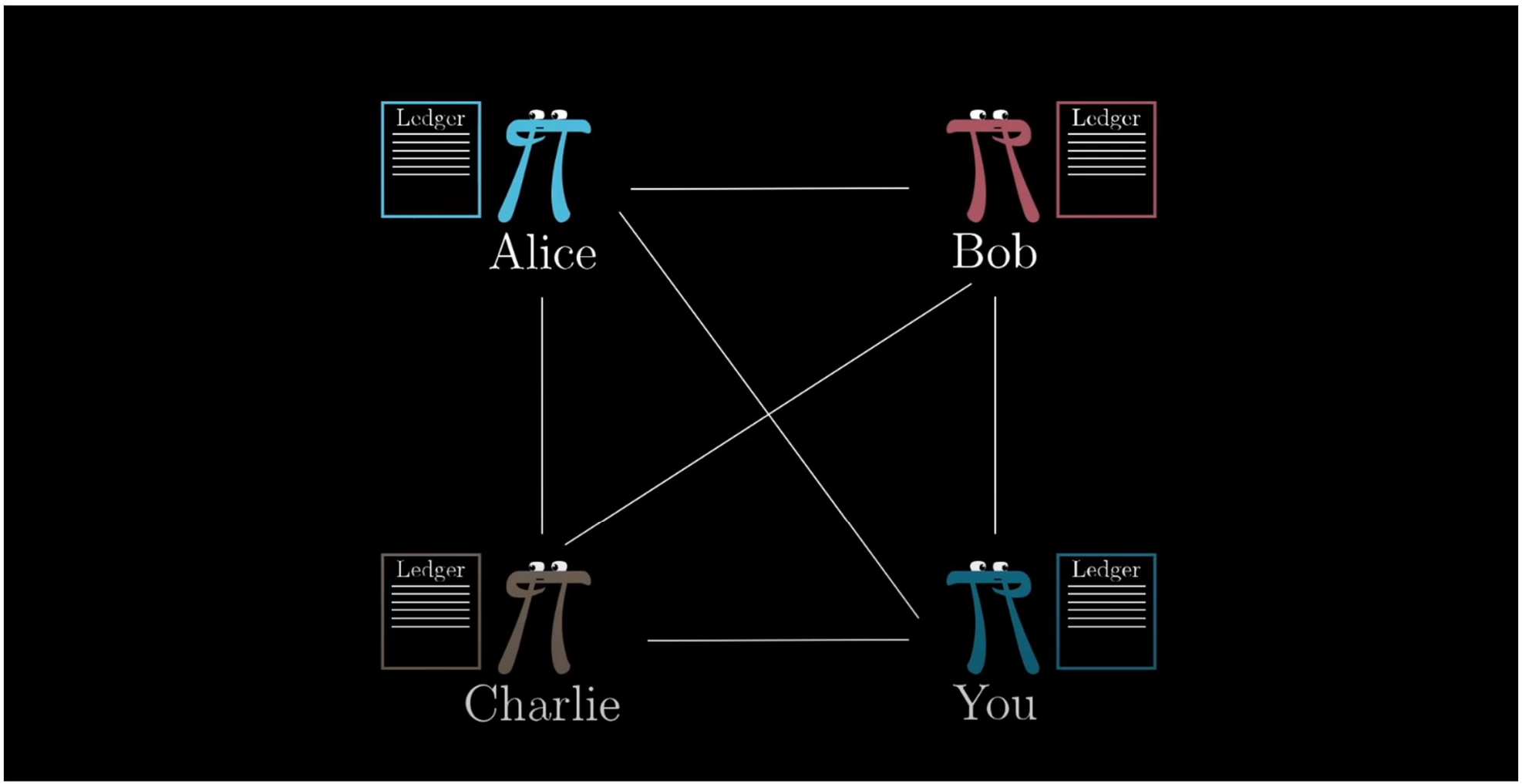
یک تفاوت عمده بین پول رایج و یا حتی پولی که در دفتر کل تعریف کردیم با بیتکوین و رمزارزهای دیگر وجود دارد



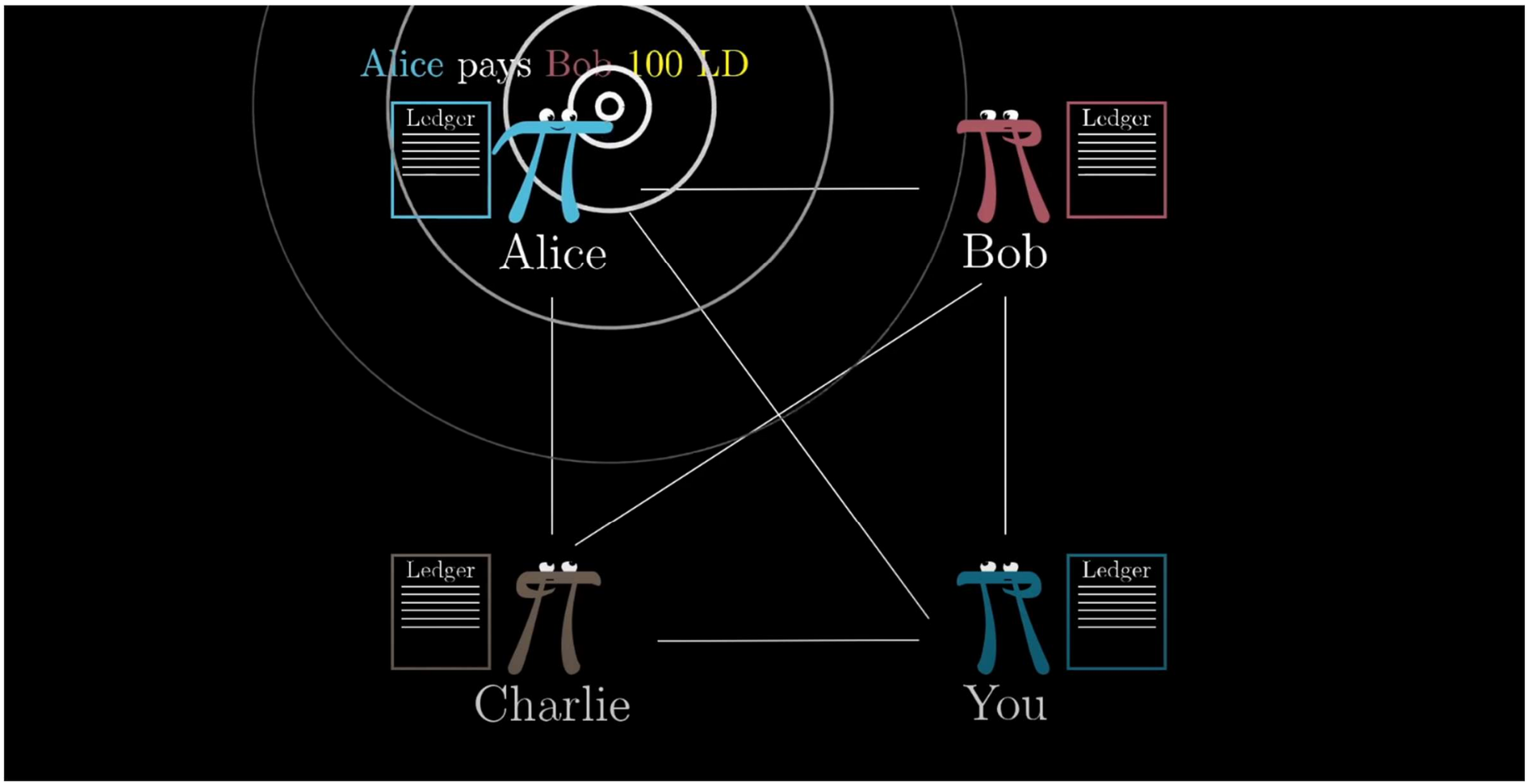
در صورتی که دفتر کل در یک مکان عمومی و در دسترس همه باشد (همچون کتابخانه یا وبسایت و ...)
این امر نیازمند اعتماد به یک مکان ثابت و متمرکز است.
چه کسی وبسایت را کنترل میکند؟
چه کسی قوانین حاکم بر دفتر کل و افزودن تراکنش را کنترل میکند؟
و ...



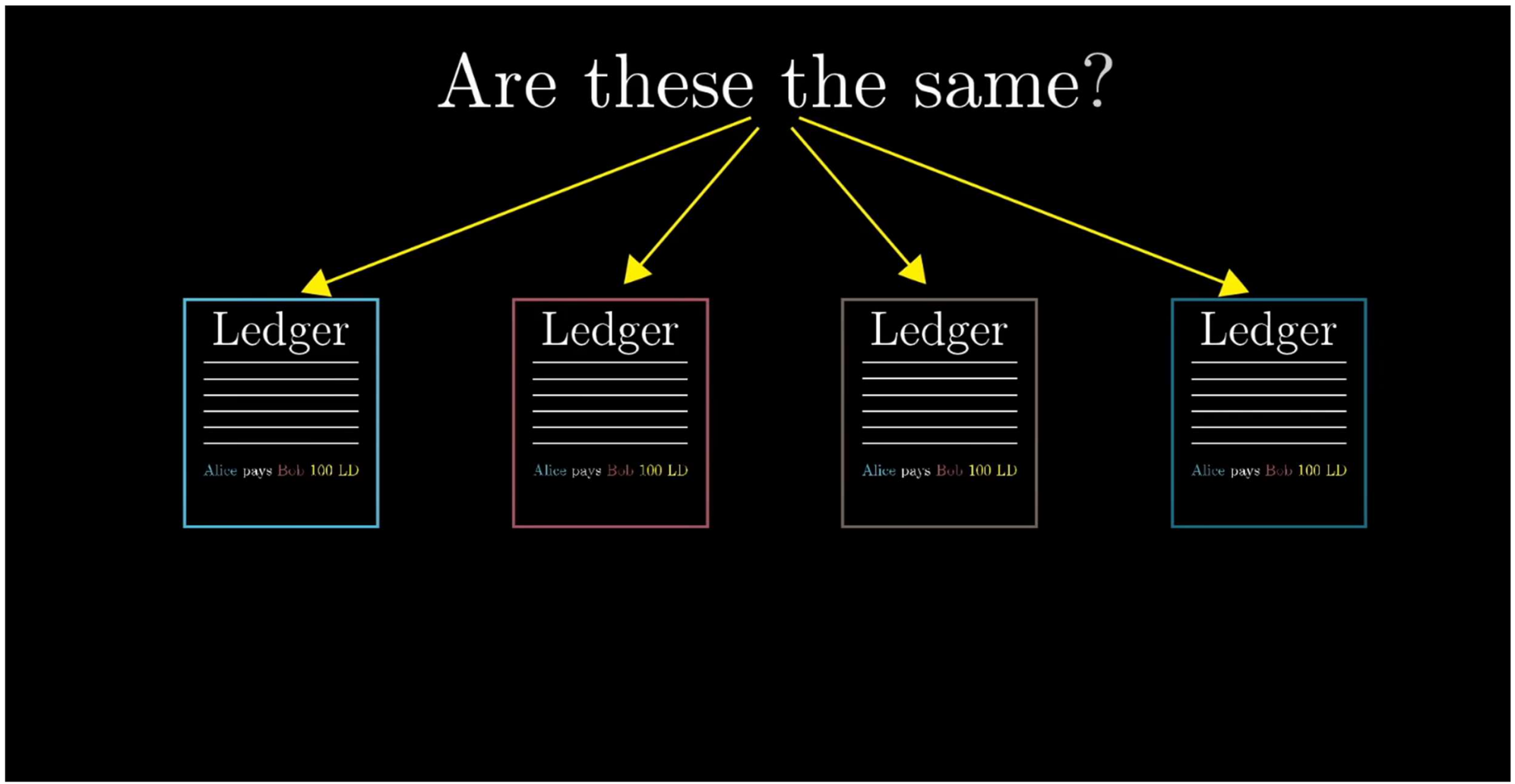
جهت حذف حتی این میزان کم از اعتماد، هر شخصی یک کپی از دفتر کل را نزد خود نگه میدارد



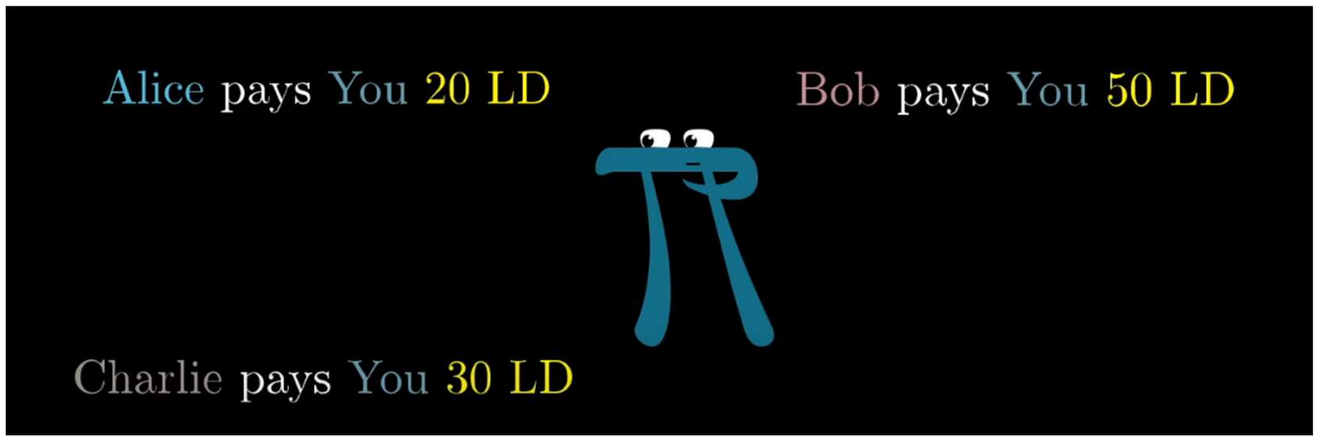
بنابراین هنگام انجام تراکنش، آن را به عموم اعلام میکنیم تا همه
آن را در کپی دفتر کل موجود نزدشان وارد کنند

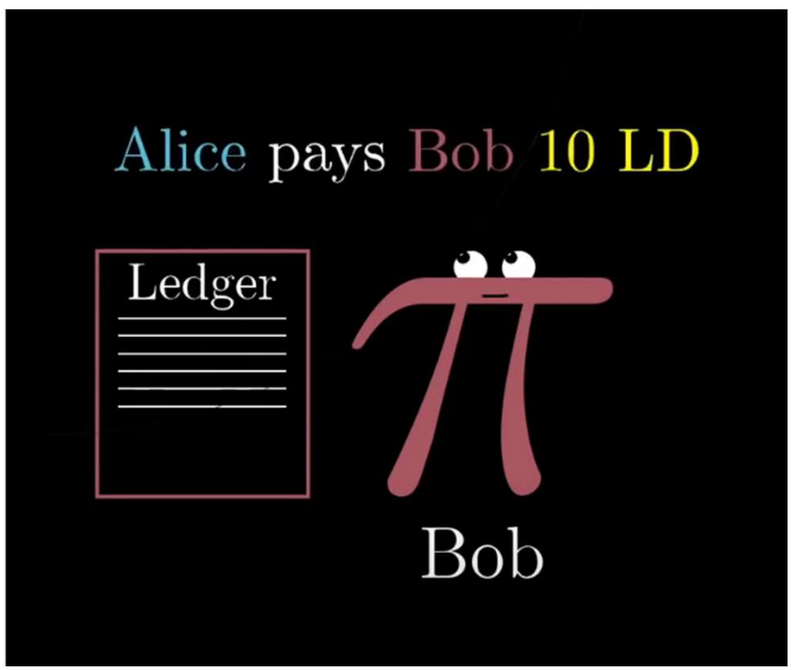


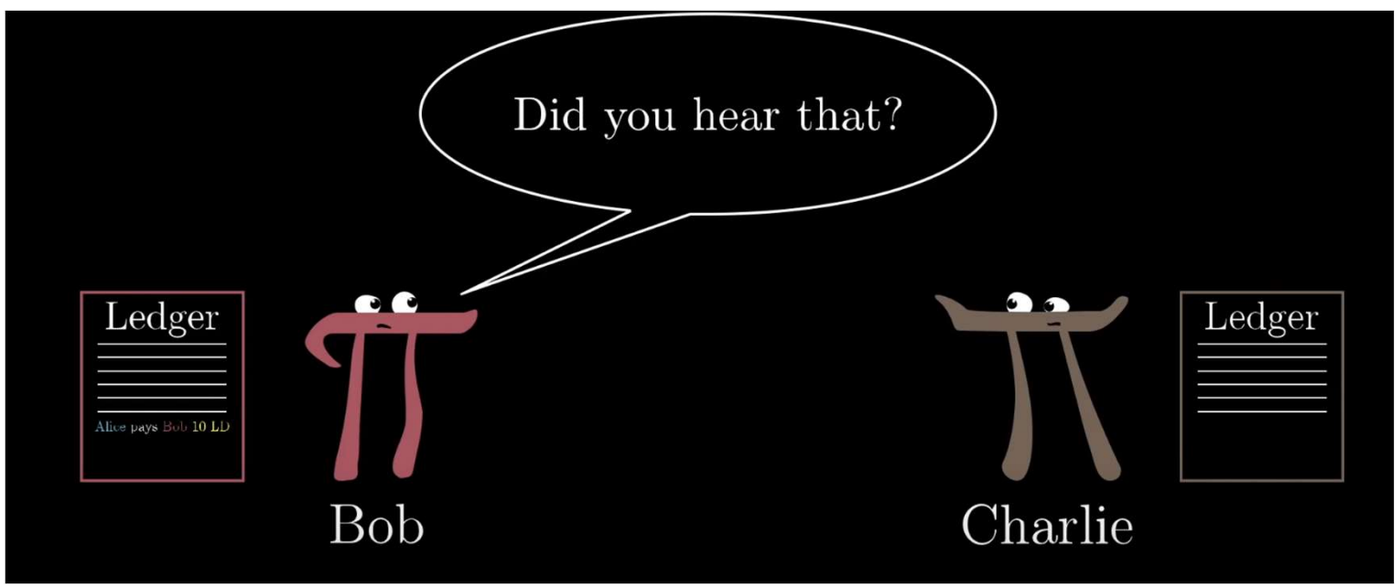
اما چگونه همه به توافق خواهند رسید که کدام کپی از دفتر روزانه درست است؟



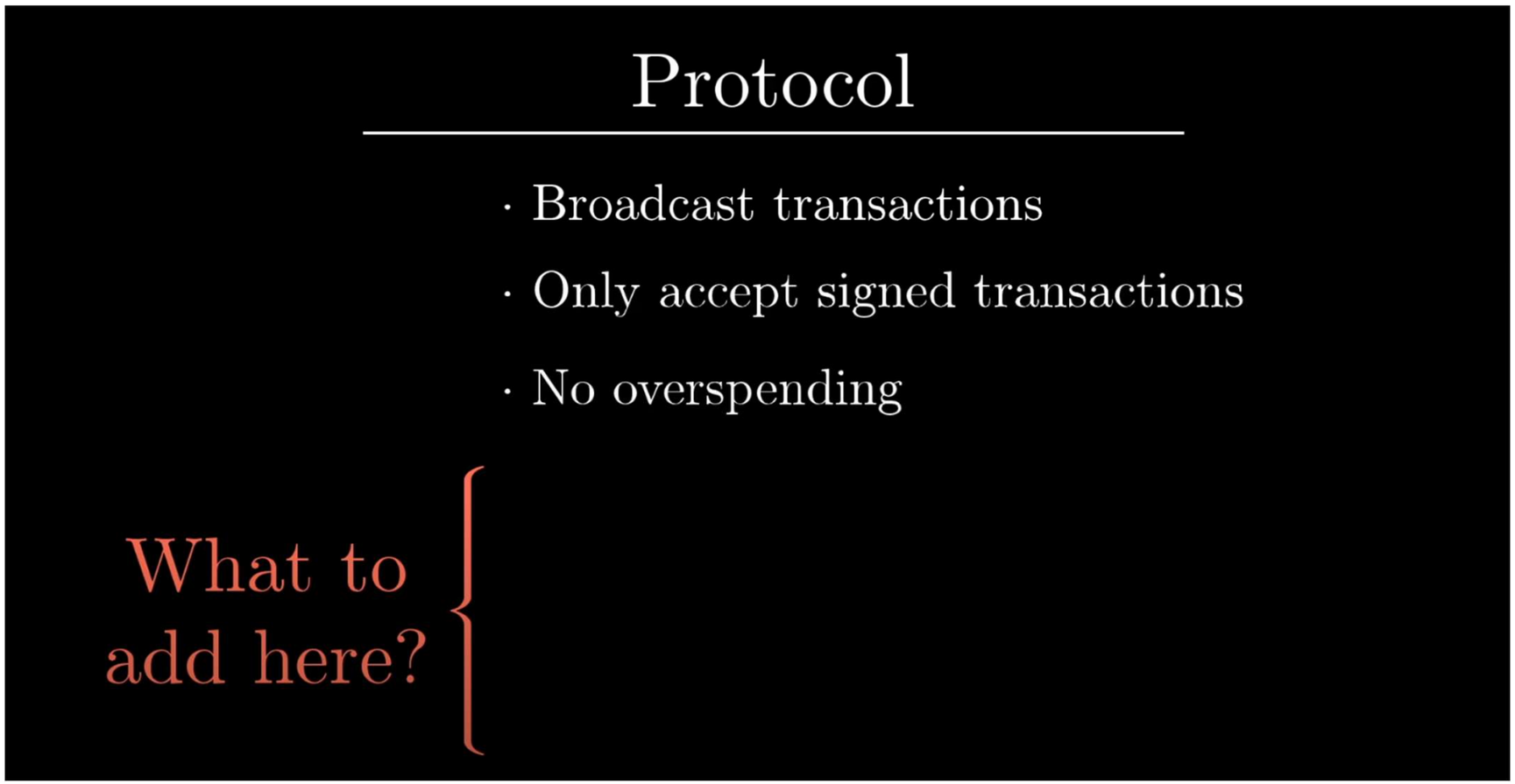
چگونه اشخاص اطمینان حاصل کنند که وقتی یک تراکنش را دریافت میکنند بقیه هم آن را دریافت کرده و با همان ترتیب قبول دارند؟



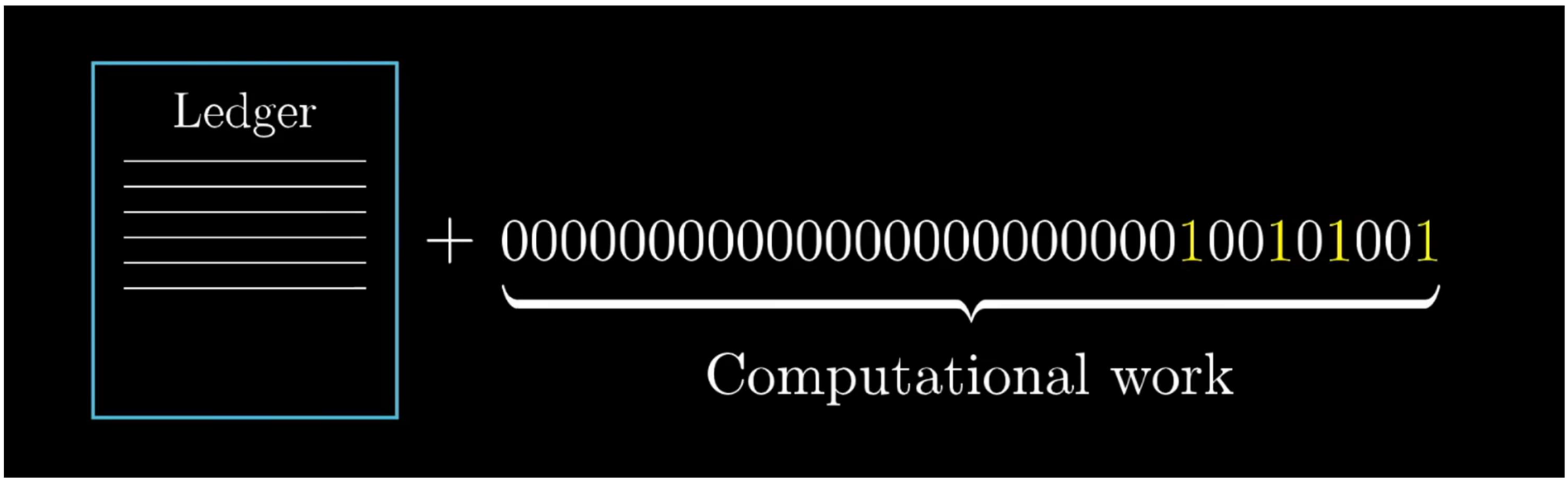


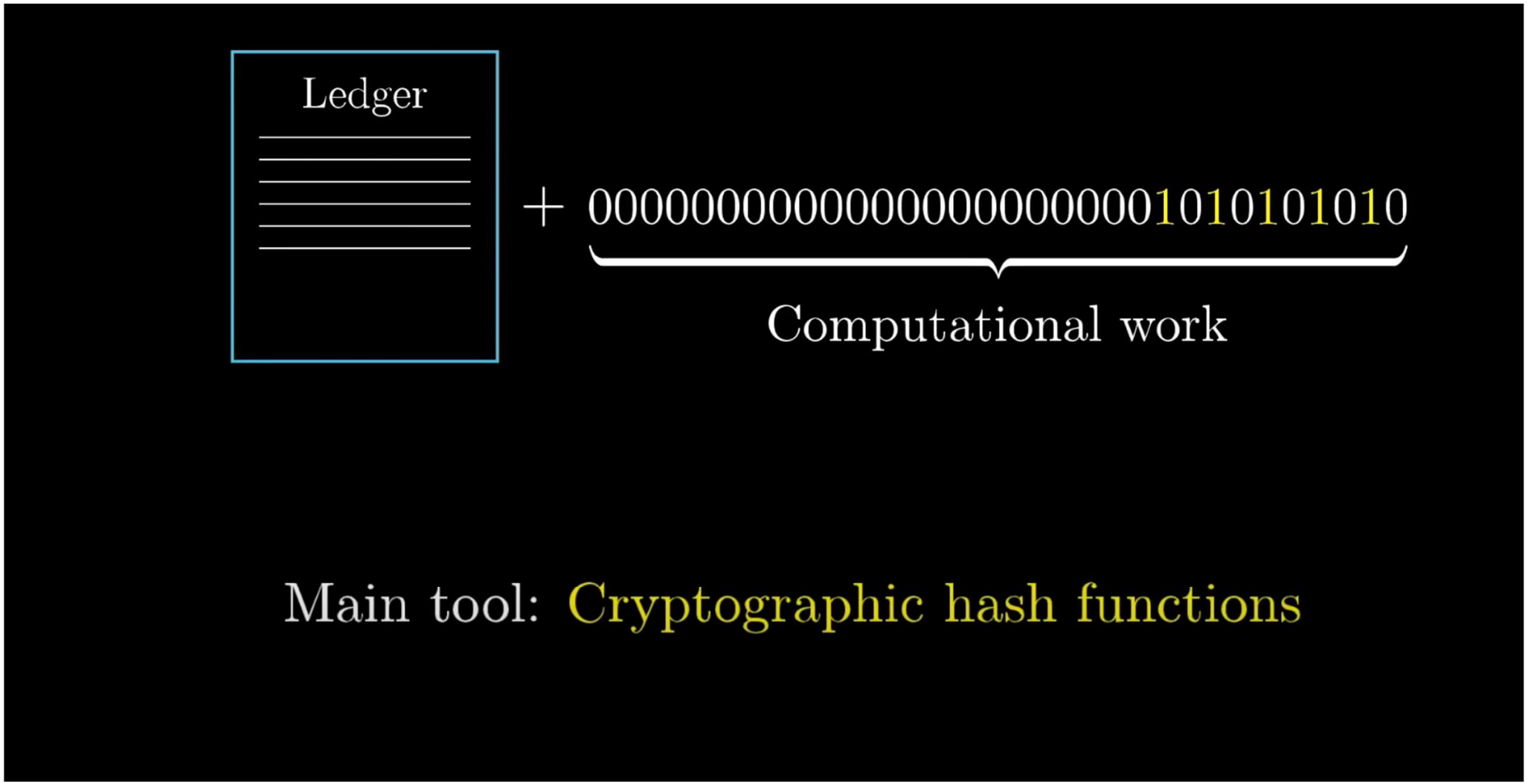


آیا میتوان قانونی اضافه کرد که تایید یا رد تراکنشها و ترتیب آنها را به گونه ای کنترل کند
که زمانی که شما تراکنشی را جهت ثبت در دفتر کل دریافت نمودید مطمعن باشید
که همه افراد دیگر در سراسر جهان قانون یکسانی را پیروی کرده
و دفتر کل آنها نیز دقیقا همانند دفتر کل شماست

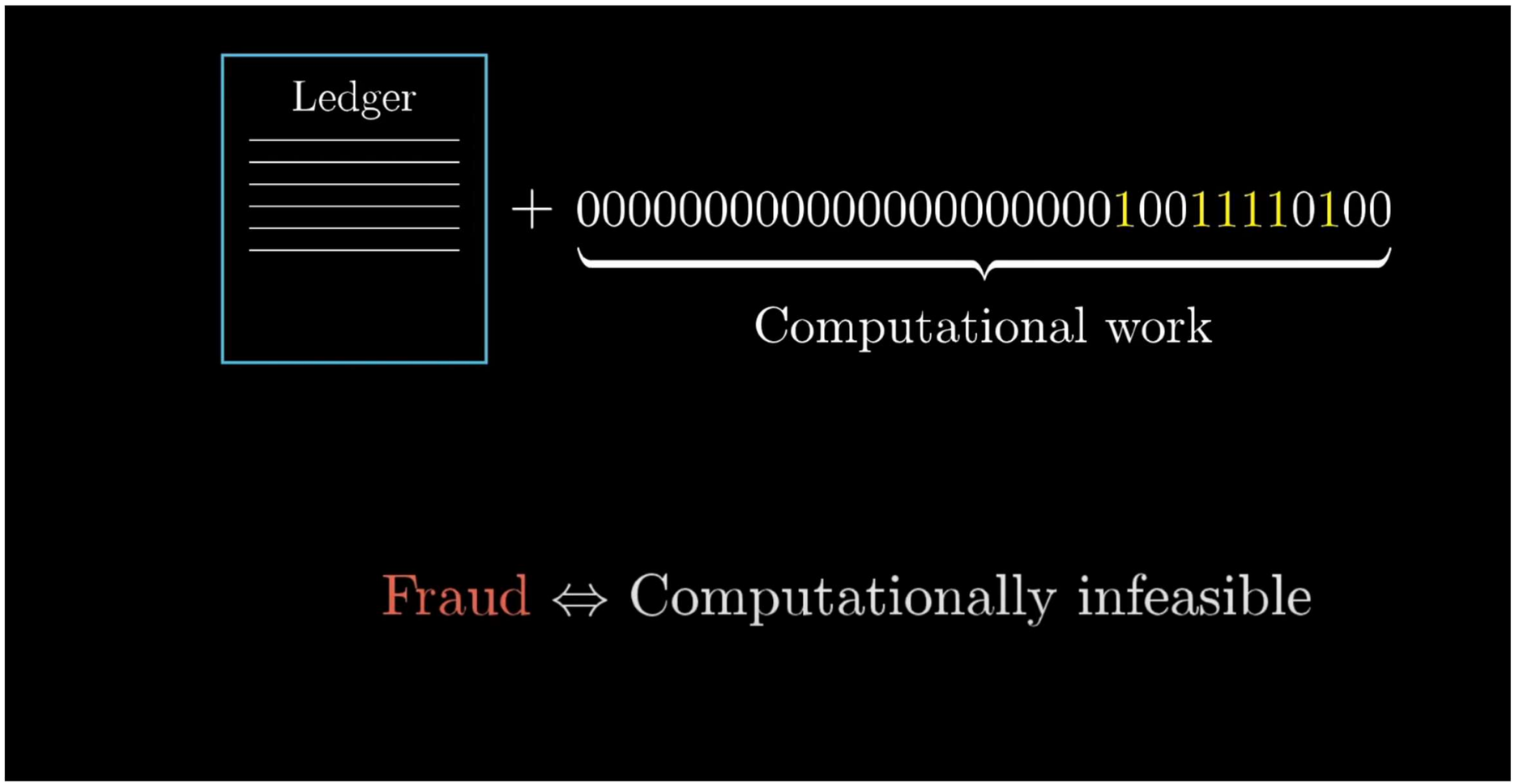


طبق مقاله اصلی بیتکوین (Bitcoin White Paper)
دفتر کلی معتبر است که بیشترین کار محاسباتی را انجام داده باشد

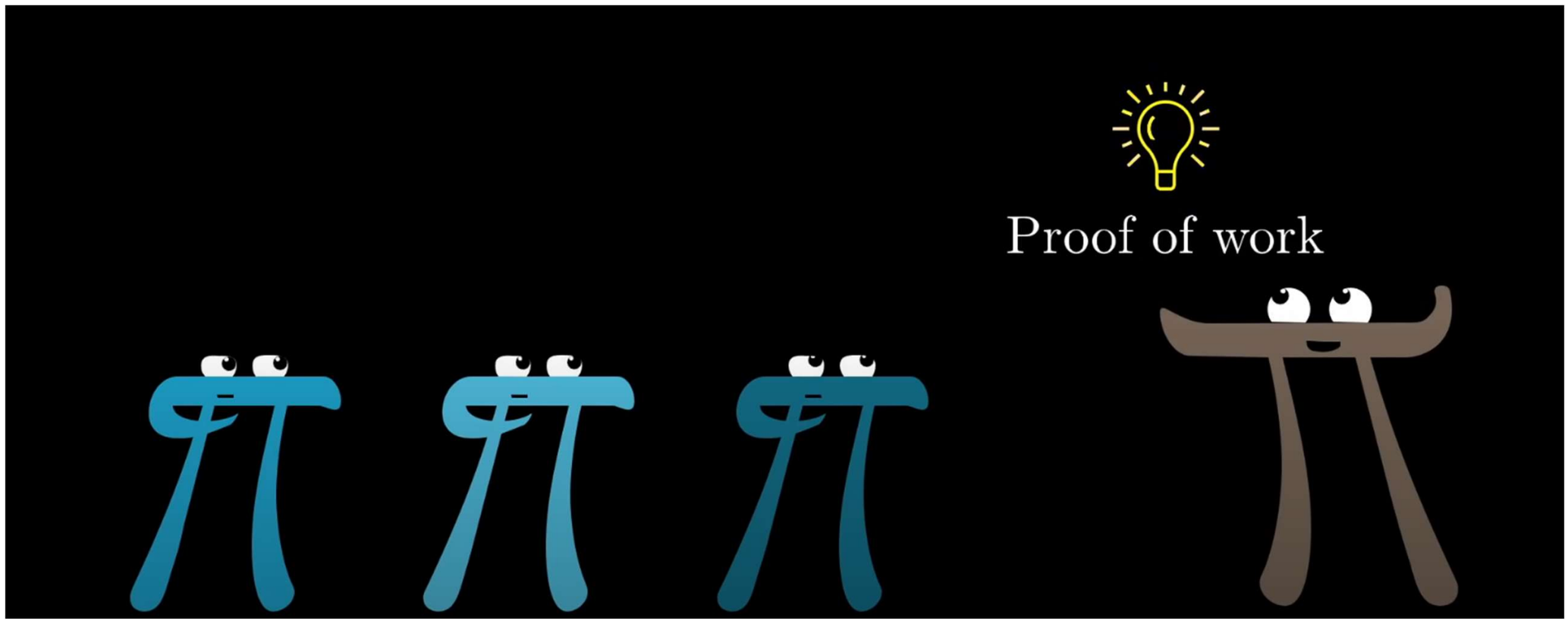




وقتی جهت تایید صحت دفتر کل نیازمند بیشترین کار محاسباتی هستیم
بنابراین هرگونه کلاهبرداری یا وارد کردن تراکنشهای خلاف واقع
نیازمند توان محاسباتی بسیار زیادی میباشد



این رویه Proof of Work نام دارد و قلب تپنده بیتکوین و برخی رمزارزهای دیگر میباشد
این رویه تضمین کننده امنیت شبکه نیز میباشد

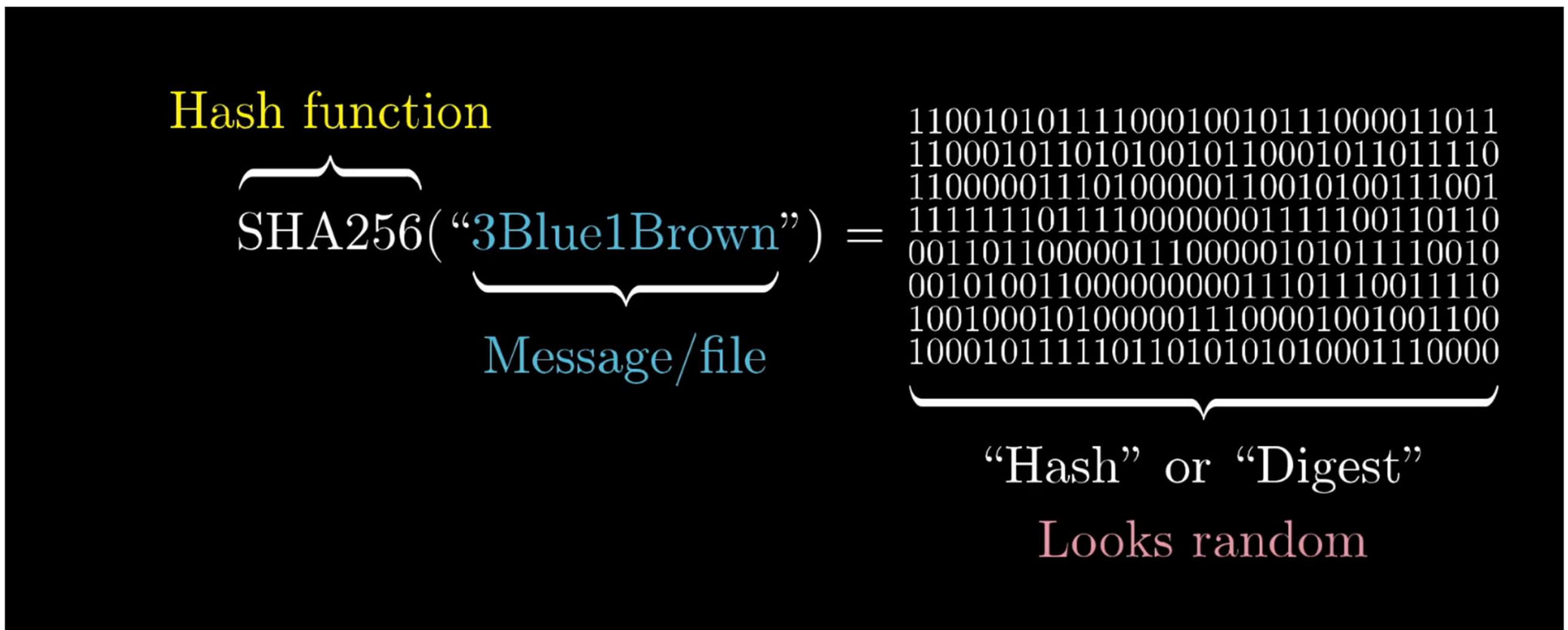


تابع هش چیست؟

تابع هش هر متنی را که دریافت کند یک رشته از صفر و یک با طول مشخص تولید میکند

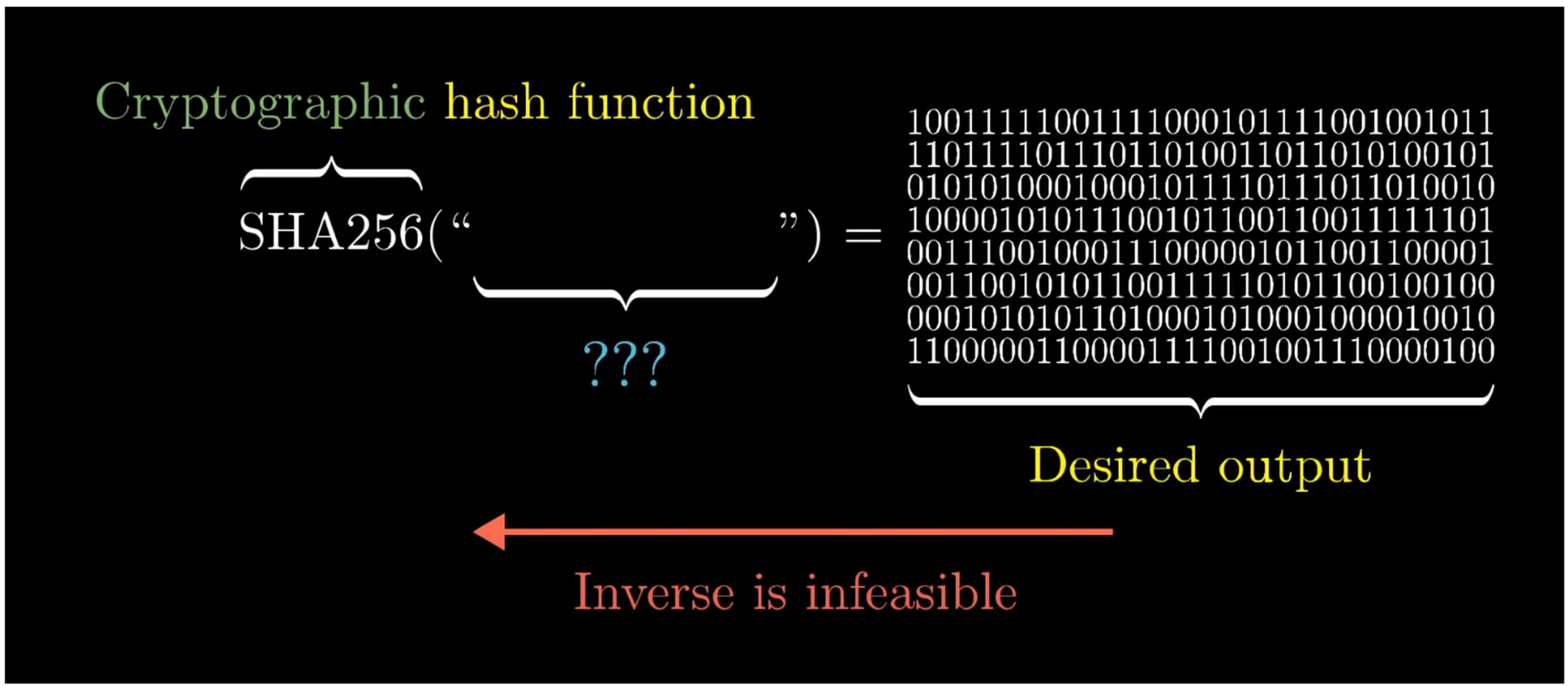
خروجی را هش یا دایجست مینامند

برای یک ورودی ثابت خروجی یکسانی دریافت خواهیم کرد ولی کوچکترین تغییر در ورودی کاملا خروجی را تغییر میدهد

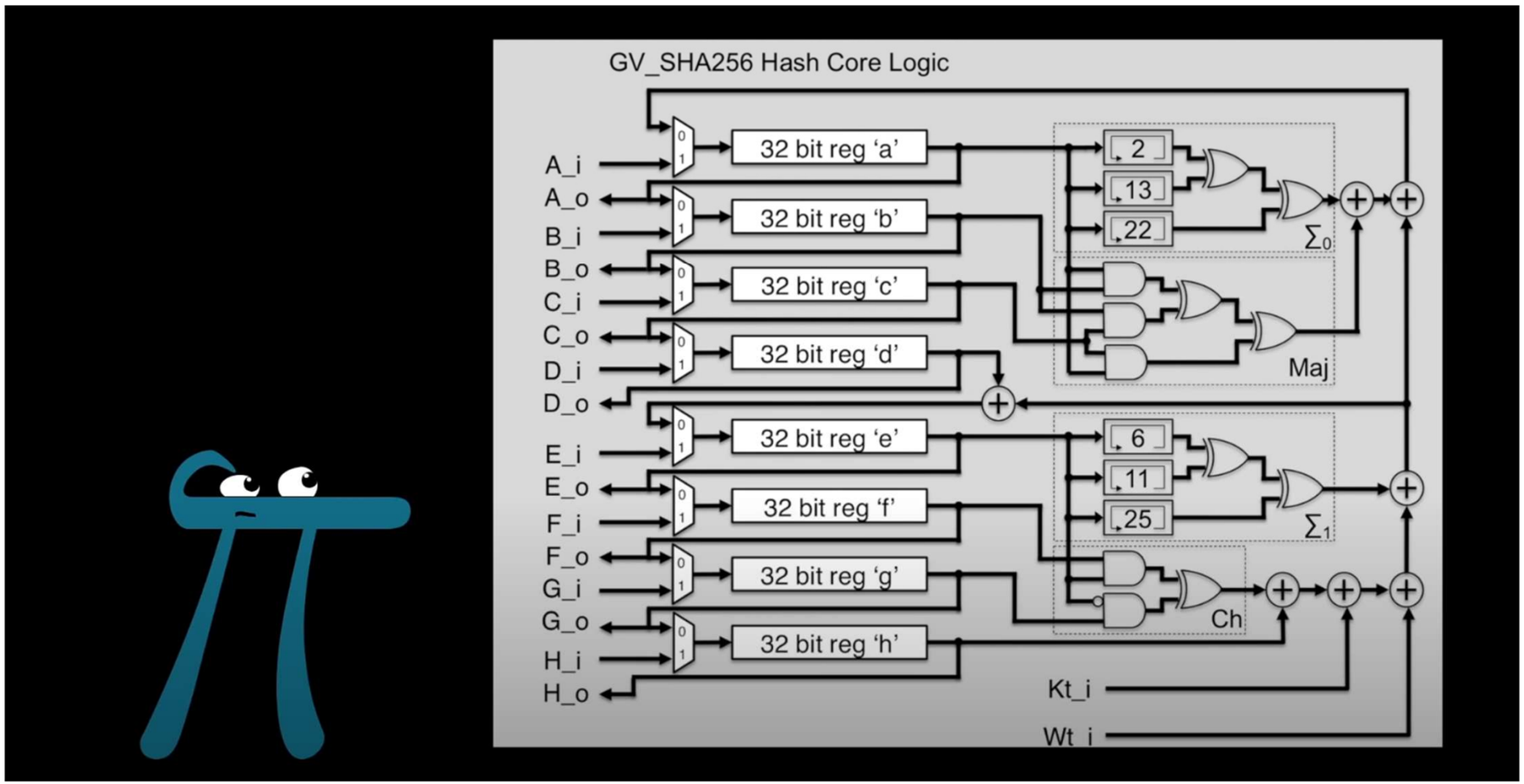


تابع هش کریپتوگرافی تابعی یک طرفه بوده و با داشتن یک هش مشخص نمیتوان متن ورودی را بدست آورد

تنها راه آن حدس زدن تمامی حالتهای ممکن است که عدد بسیار بزرگی میباشد

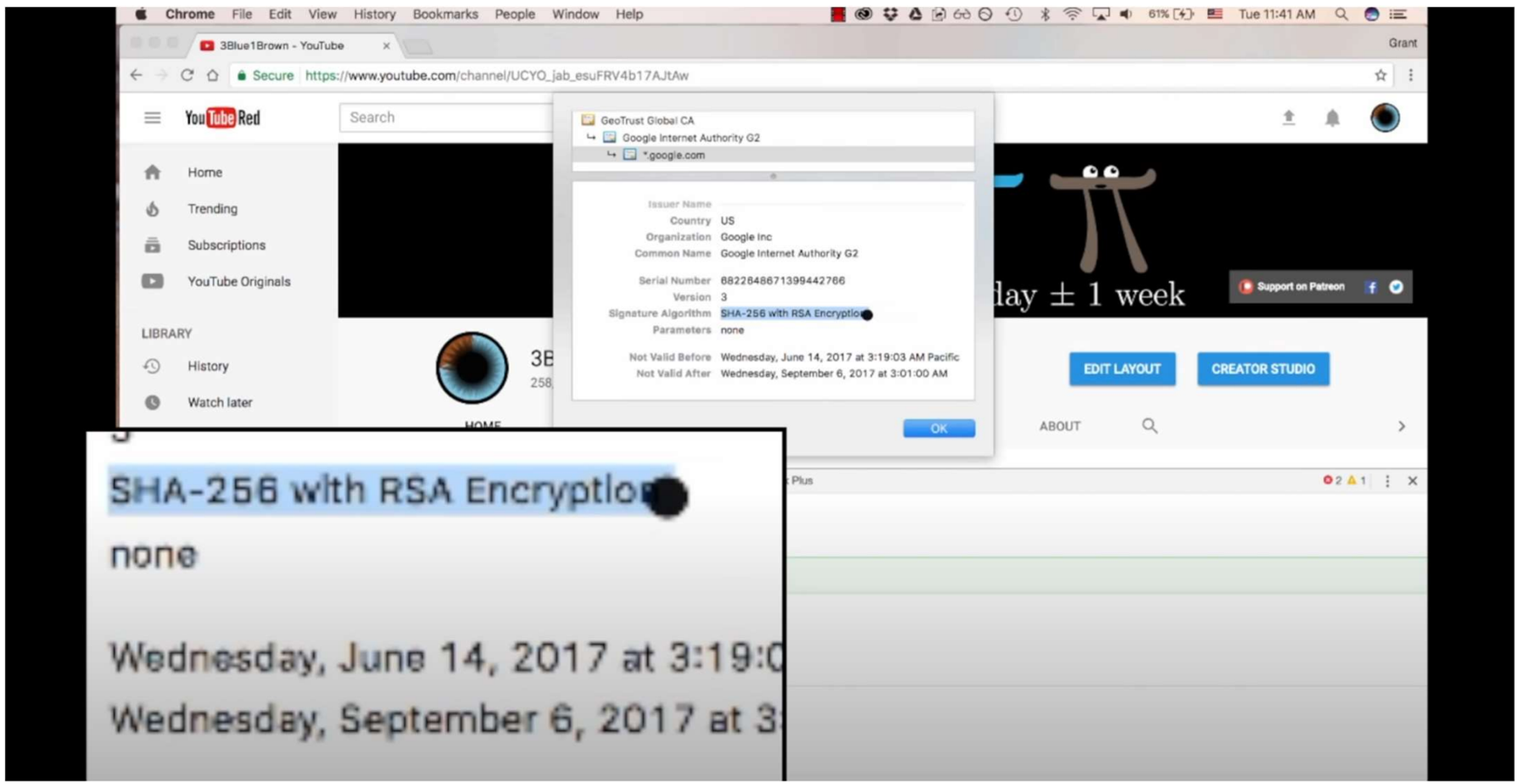


این پروسه تولید هش امکان مهنسی معکوس حتی با مطاله دقیق نحوه کارکرد تابع را ندارد
و تا کنون کسی موفق به انجام آن نشده است

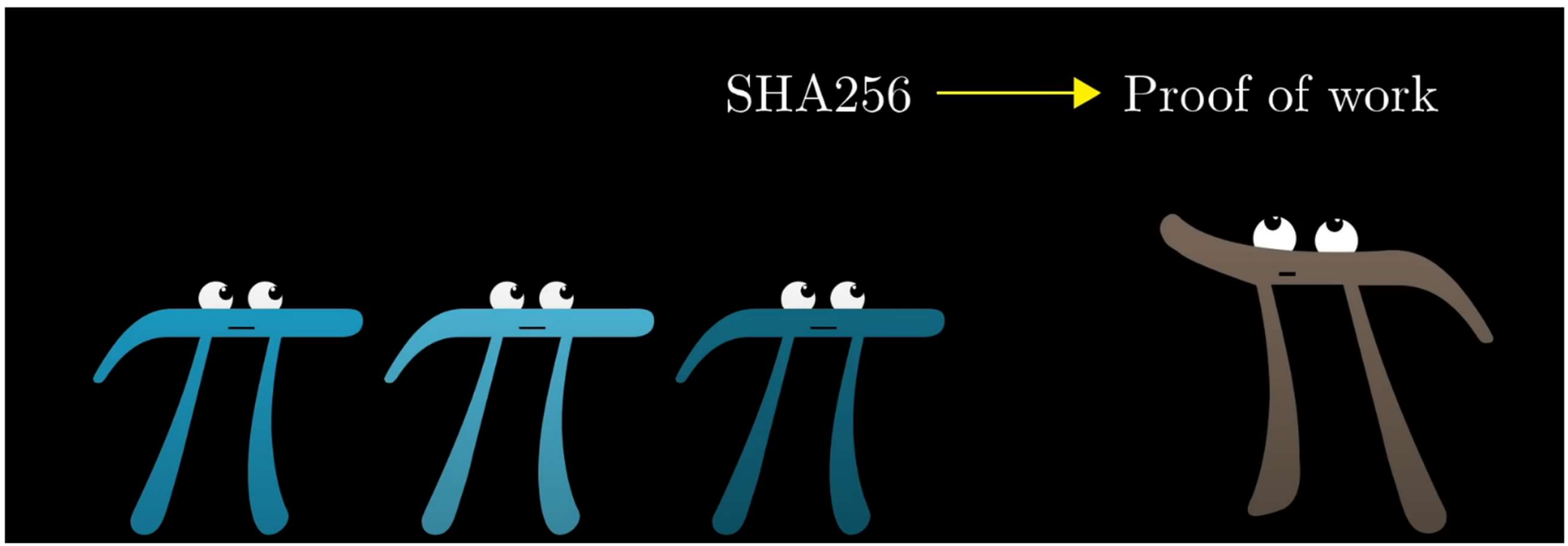


این پروتوکل در اکثر سیستمهای امنیتی اسفاده میشود

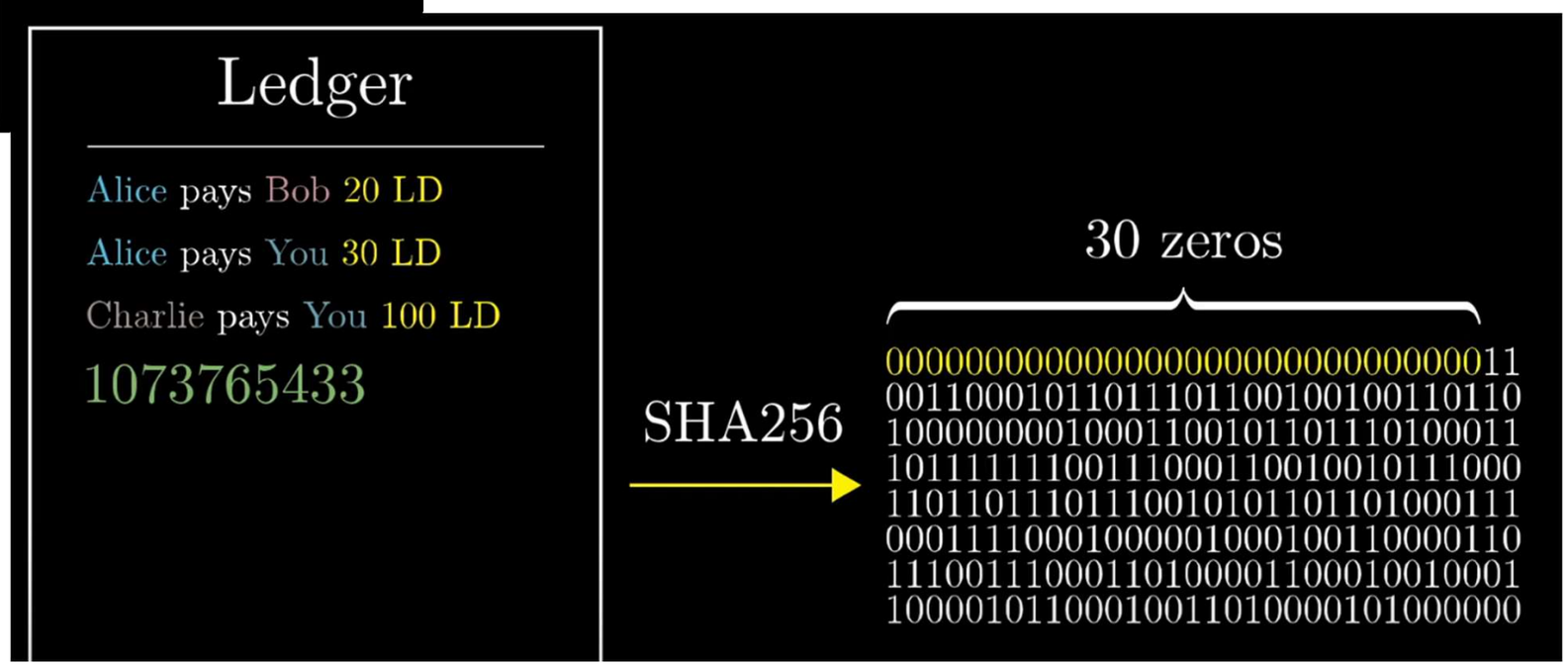
در صورتی که پروتوکل امنیتی یوتیوب و یا وبسایت بانک خود را چک کنید نام SHA256 را خواهید دید



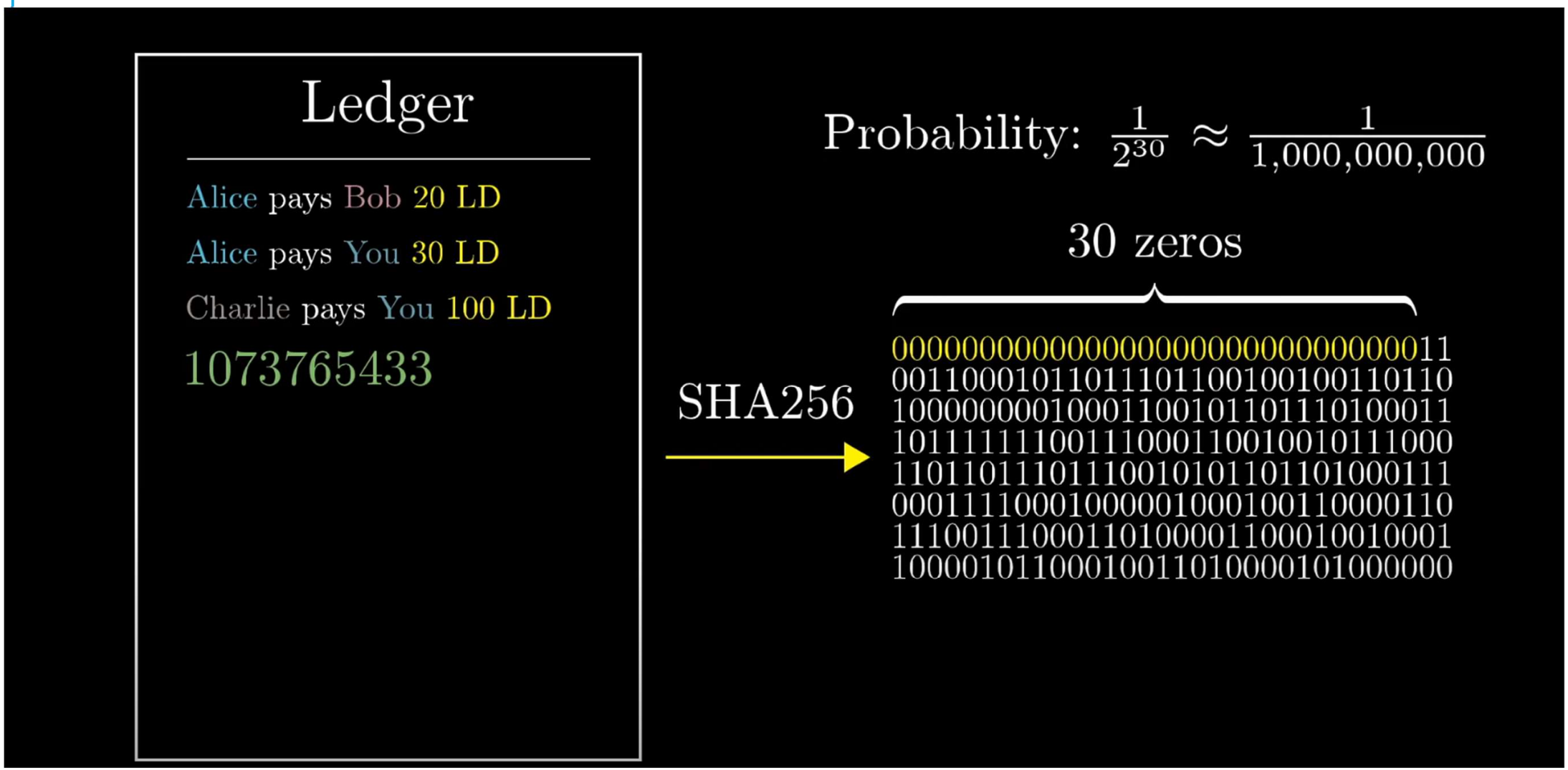
اما این تابع چگونه میتواند نشان دهد که یک لیست از تراکنشها
بیشترین کار محاسباتی را انجام داده است؟



تصور کنید یک نفر به
شما بگوید عدد خاصی
یافته است که وقتی آن را
به انتهای لیست تراکنشها
اضافه کنید 30 بیت اول
هش خروجی صفر
خواهد بود

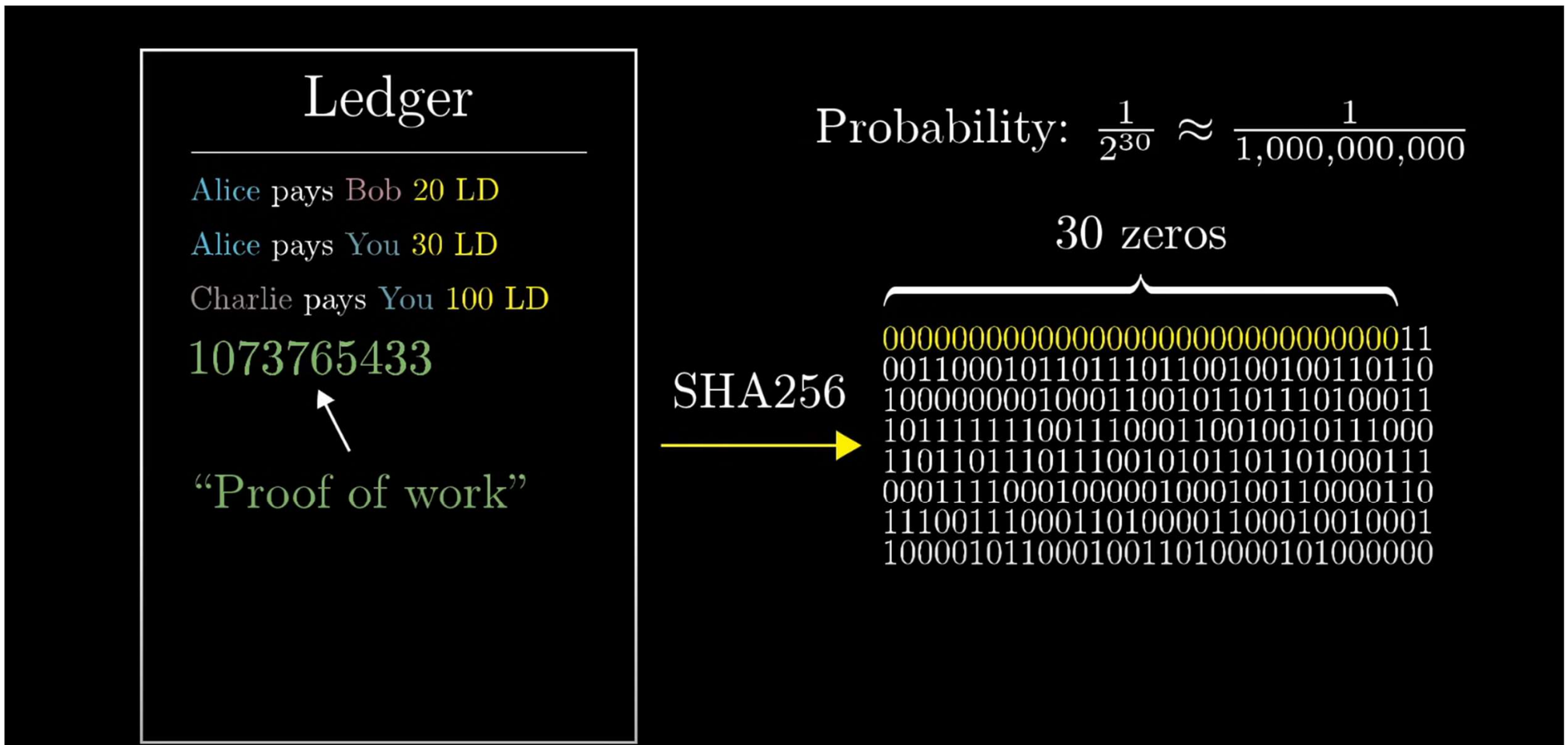


یافتن چنین عددی چقدر دشوار است؟



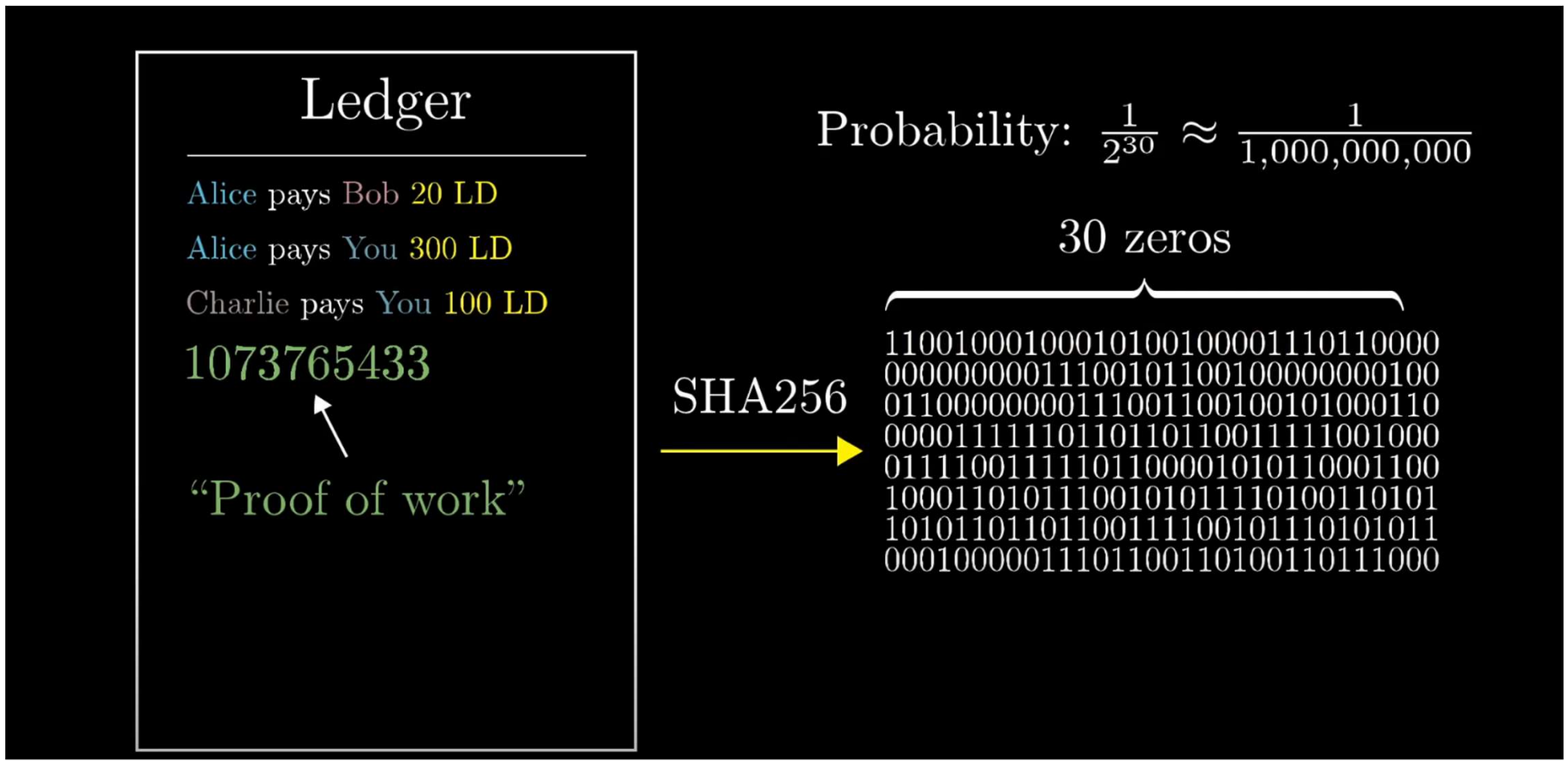
از آنجا که تابع هش کریپتوگرافی یکطرفه میباشد
پس تنها راه یافتن این عدد حدس زدن و امتحان کردن آن میباشد تا زمانی که عدد مورد نظر پیدا شود

اما زمانی که عدد مورد نظر یافت شد امتحان کردن آن کار راحتی میباشد
آن را به انتهای متن اضافه کرده و هش خروجی را چک میکنیم



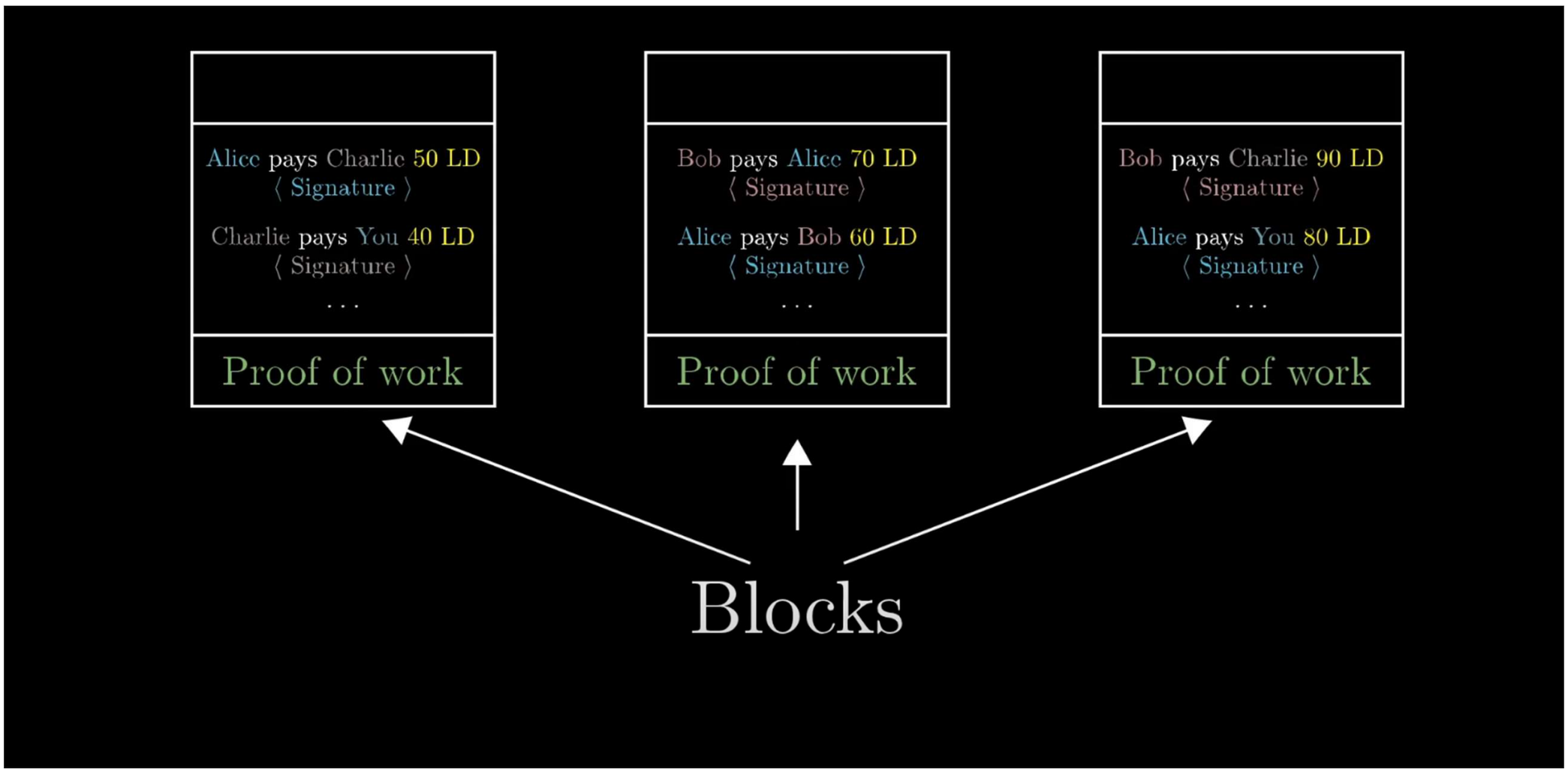
بنابراین کسی که این عدد مخصوص را یافته است مطمعنا کار محاسباتی بسیاری انجام داده (Proof of Work)
و شما با داشتن آن عدد بدون انجام این کار سنگین به راحتی میتوانید صحت آنرا چک کنید

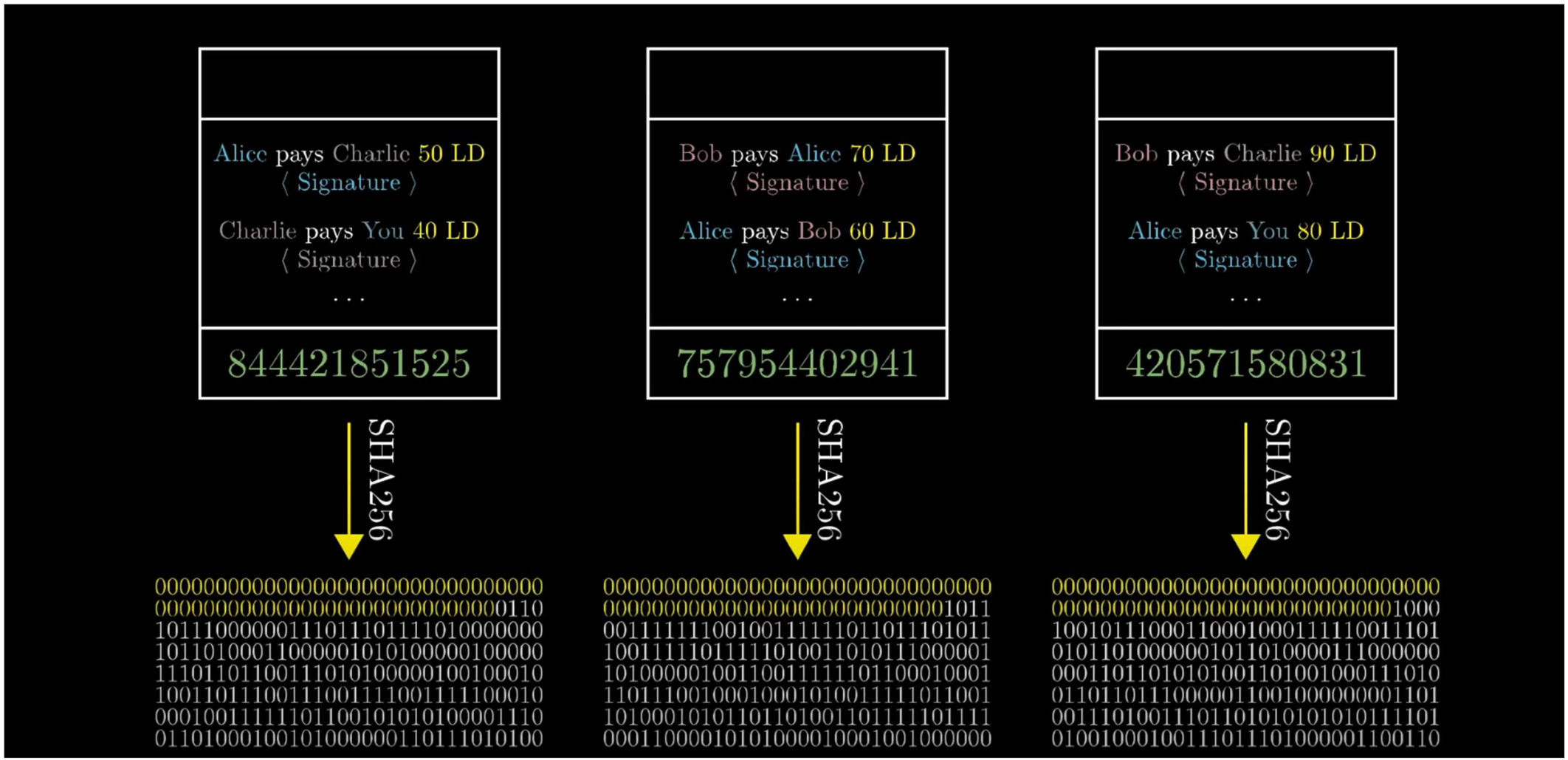
همچنین اگر کوچکترین تغییری در متن ایجاد کنید
مجبور خواهید بود مجددا این کار محاسباتی سنگین را انجام داده و عدد مربوطه جدید را حدث بزنید



در ادامه اولین کاری که انجام میدهیم دفتر کل را در دسته هایی جداگانه مرتب میکنیم و هر یک را یک بلاک مینامیم

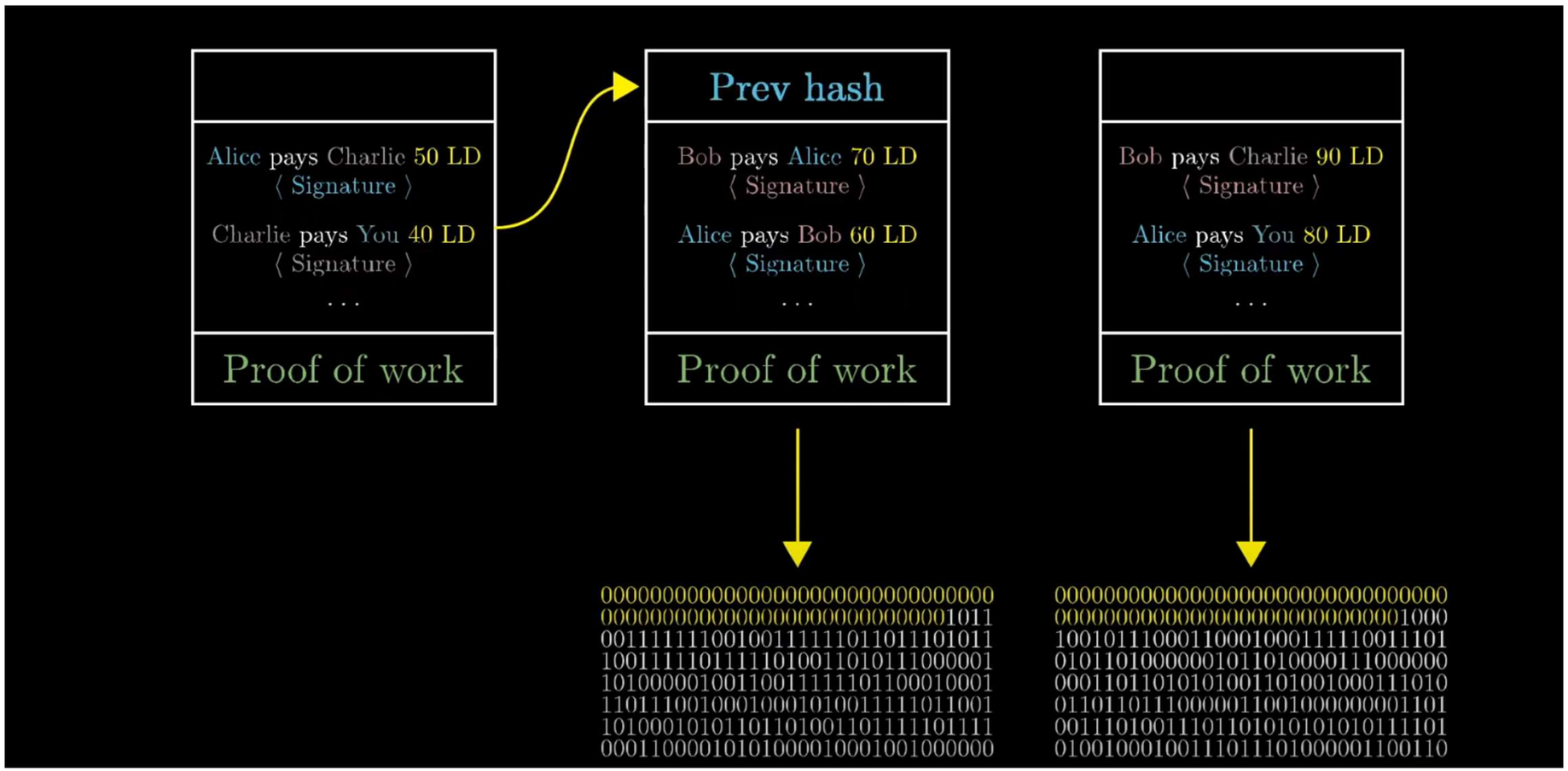
هر بلاک شامل لیست تراکنشها و عدد مخصوص Proof of Work میباشد





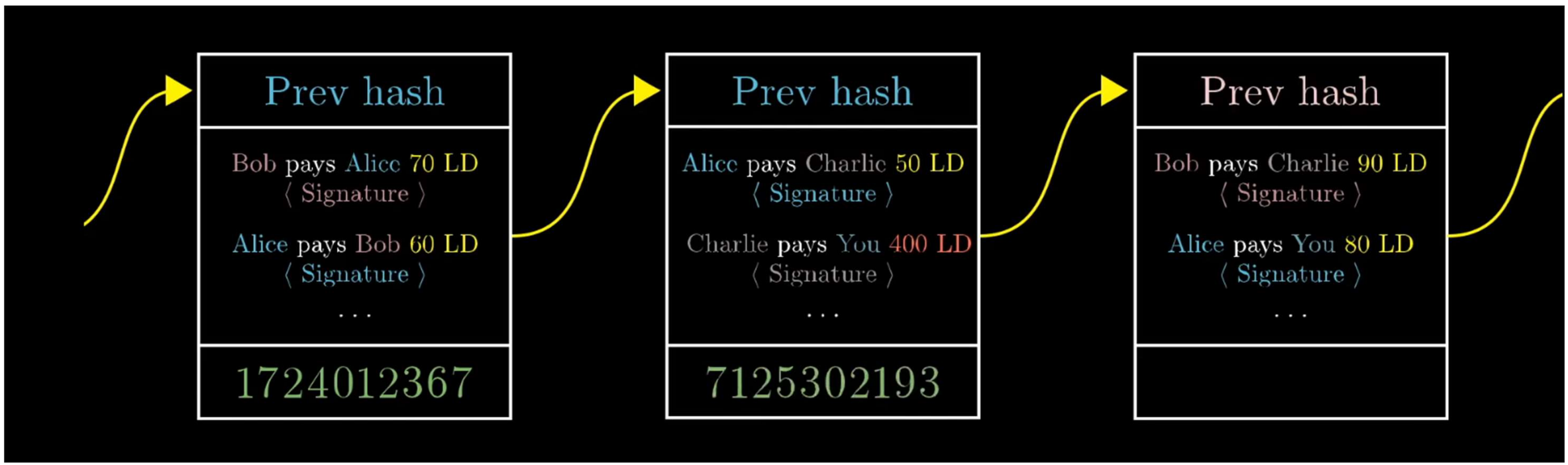
همانگونه که یک تراکنش تنها زمانی که امضای دیجیتال داشته باشد معتبر است
یک بلاک هم تنها زمانی اعتبار دارد که دارای هش مربوط به Proof of Work باشد

همچنین برای نظم بیشتر و مشخص بودن ترتیب تراکنشها
ابتدای هر بلاک هش مربوط به Proof of Work بلاک پیشین قرار میگیرد

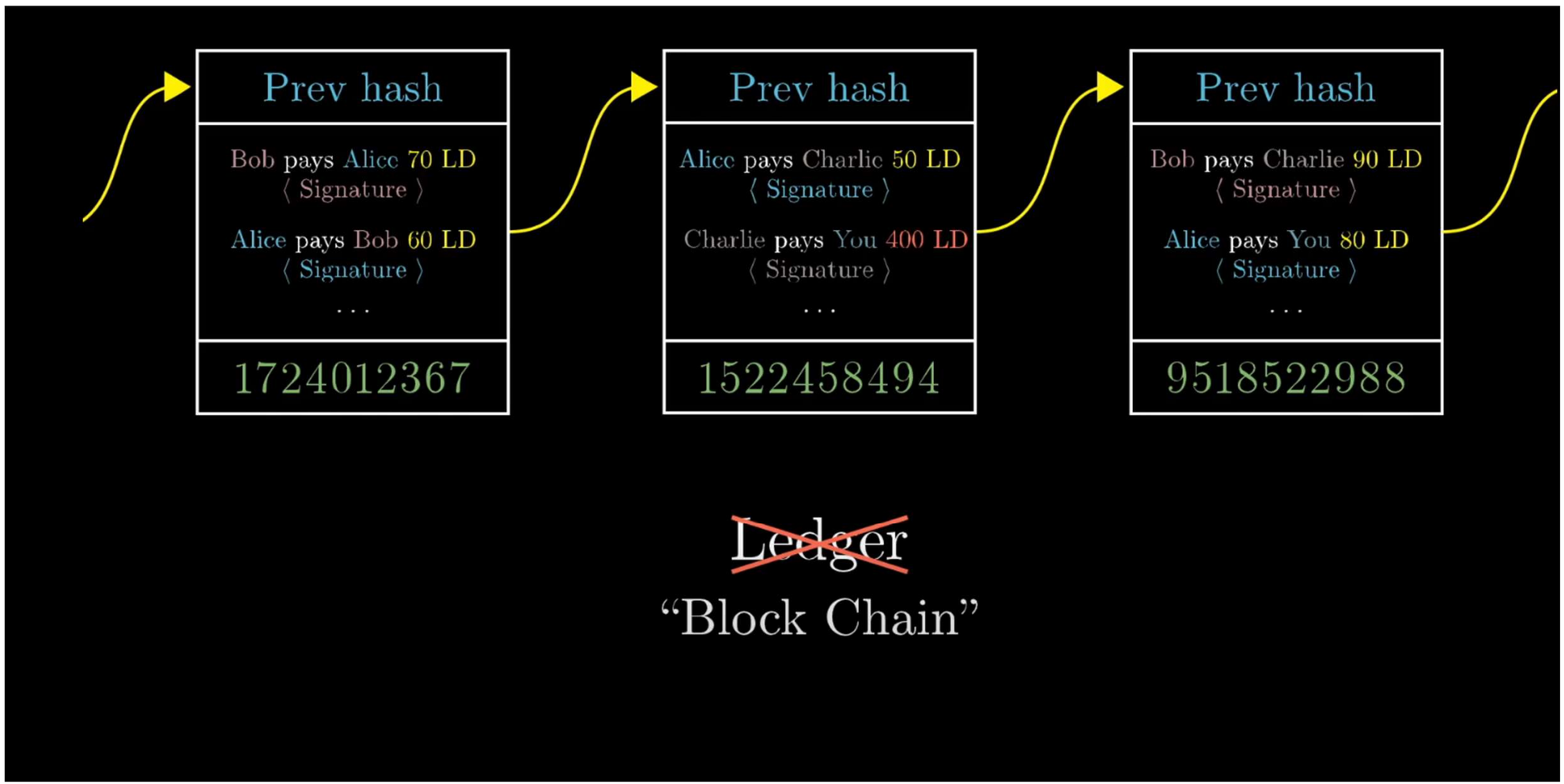


در این صورت اگر شخصی به عقب بازگشته تا اطلاعات موجود در یک بلاک و یا ترتیب دو بلاک را تغییر دهد این امر باعث تغییر هش آن بلاک شده که نتیجه آن تغییر هش بلاک بعدی و بعدی و... خواهد بود

این امر نیازمند انجام کار محاسباتی بسیار سنگین و یافتن هش تمامی بلاکهای بعد از آن بلاک میباشد



به دلیل لینک شدن بلاکها به این شکل، بجای دفتر کل به آن بلاکچین گفته میشود

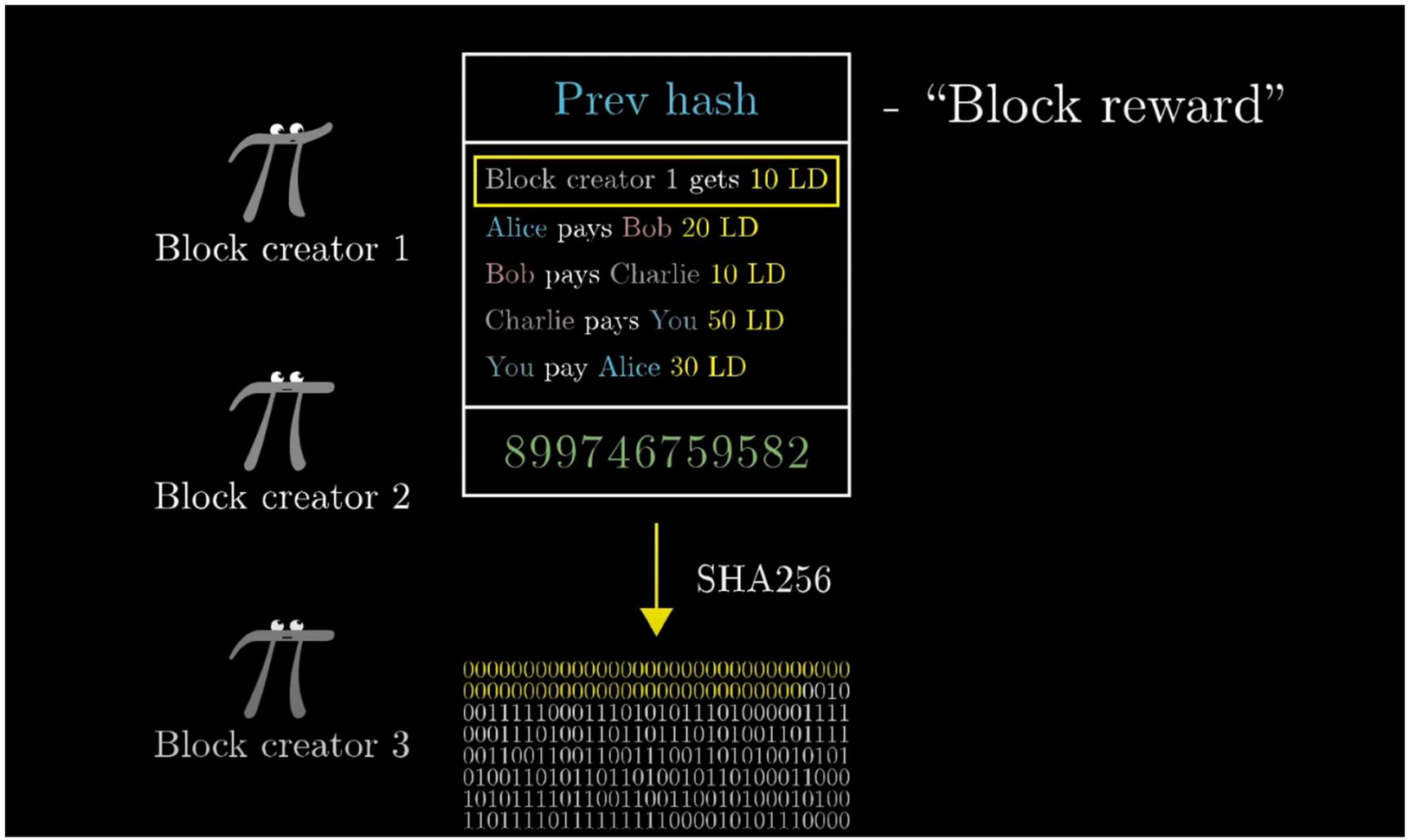


بنابراین افرادی وجود دارن که تولید کننده بلاکها هستند

مدام در حال گوش دادن بوده و لیست تراکنشها را مرتب کرده و سپس هش مربوط به آن بلاک را پیدا میکنند

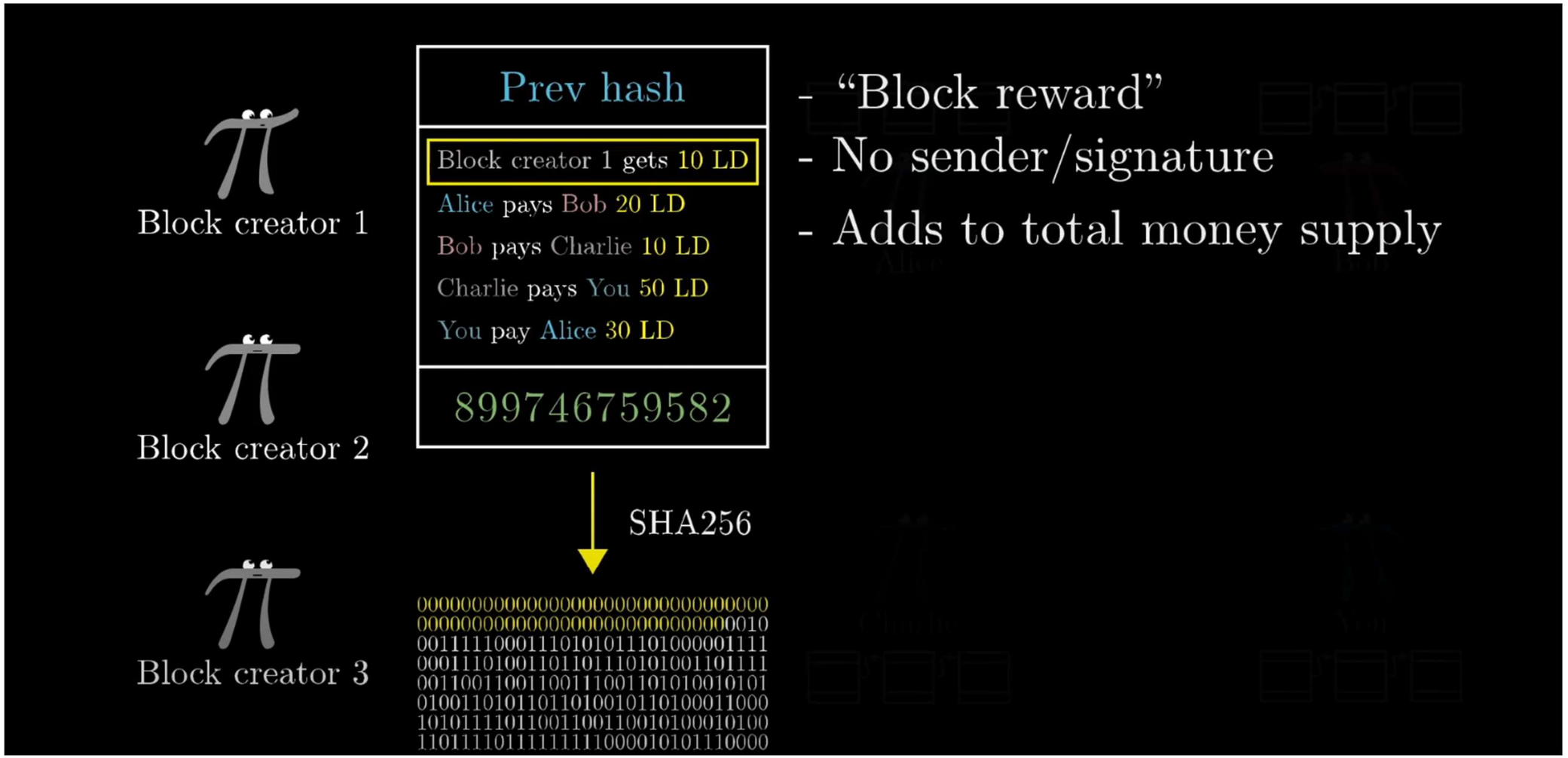
پس از یافتن هش مربوطه تولید کننده بلاک که زودتر از بقیه توانسه عدد صحیح را حدس بزند
آن را به تمامی شبکه اعلام میکند تا چک شده و صحت آن بررسی شود

برای پاداش تولید کننده بلاک و بخاطر کار محاسباتی زیادی که انجام داده است به او اجازه داده میشود تا در ابتدای بلاک یک تراکنش ویژه برای خودش ثبت کند که به عنوان پاداش مبلغ مشخصی را دریافت کند

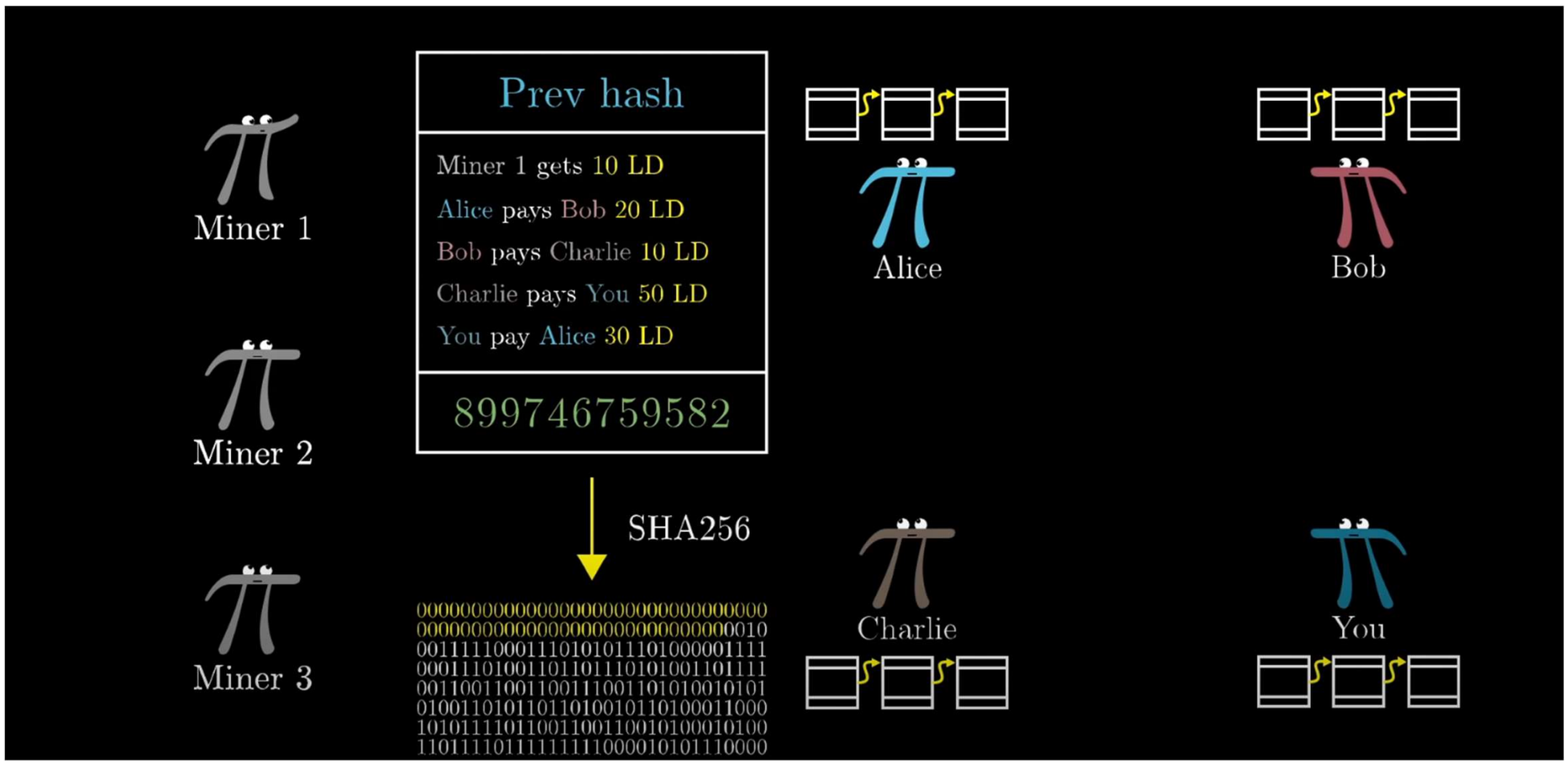


این مبلغ از جانب کسی ارسال نمیشود بنابراین نیاز به امضا ندارد

همچنین با تولید هر بلاک به میزان منابع پول موجود اضافه میشود (تولید میشود)



از آنجا که تولید بلاک نیازمند کار زیادی بوده و همچنین تولید منابع مالی میکند به این کار ماینینگ یا استخراج گفته میشود



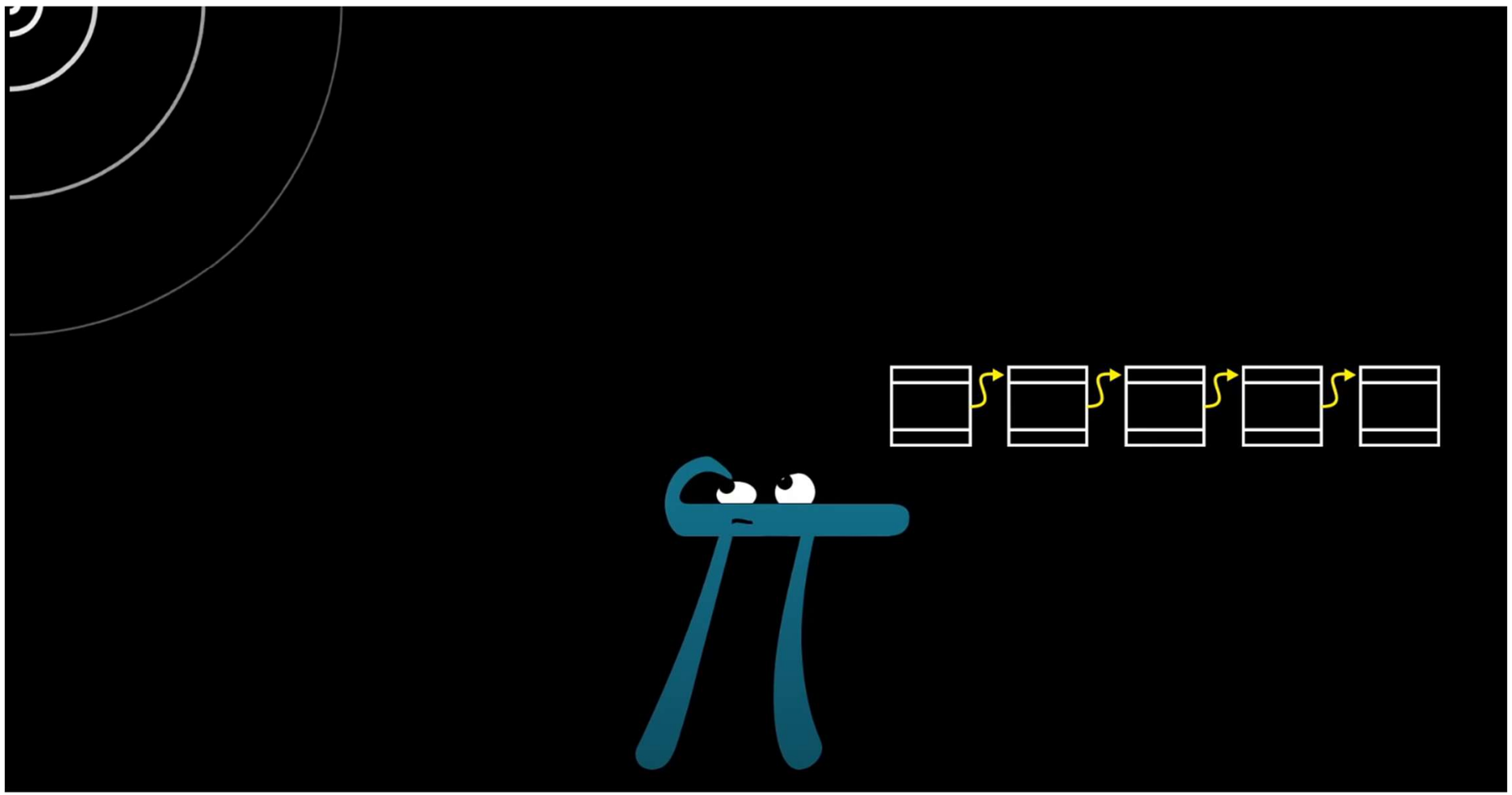
بنابراین کار ماینرها :

دریافت و مرتب کردن تراکنشها

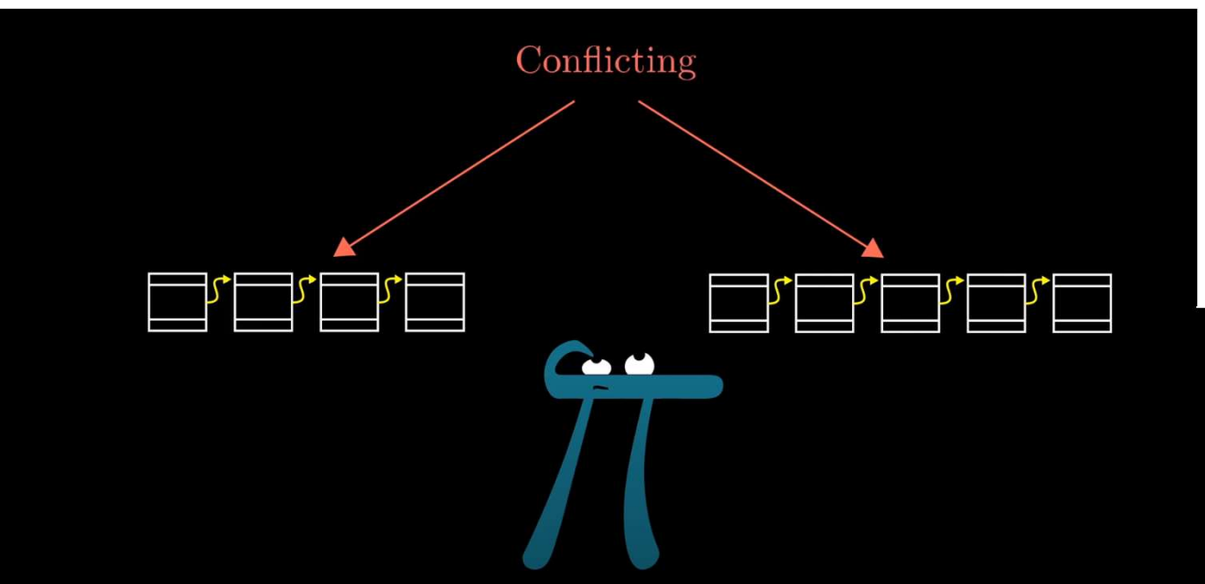
حدس زدن هش بلاک

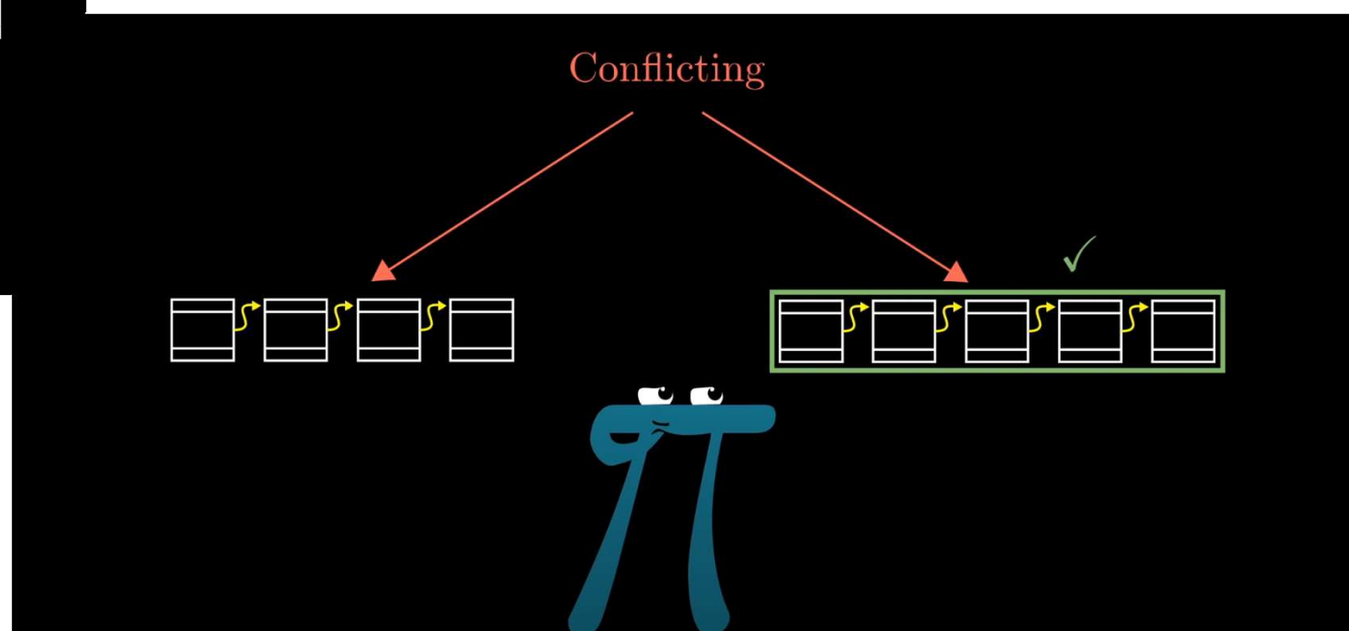
اعلام هش و بلاک در شبکه جهت دریافت تاییدیه و پاداش

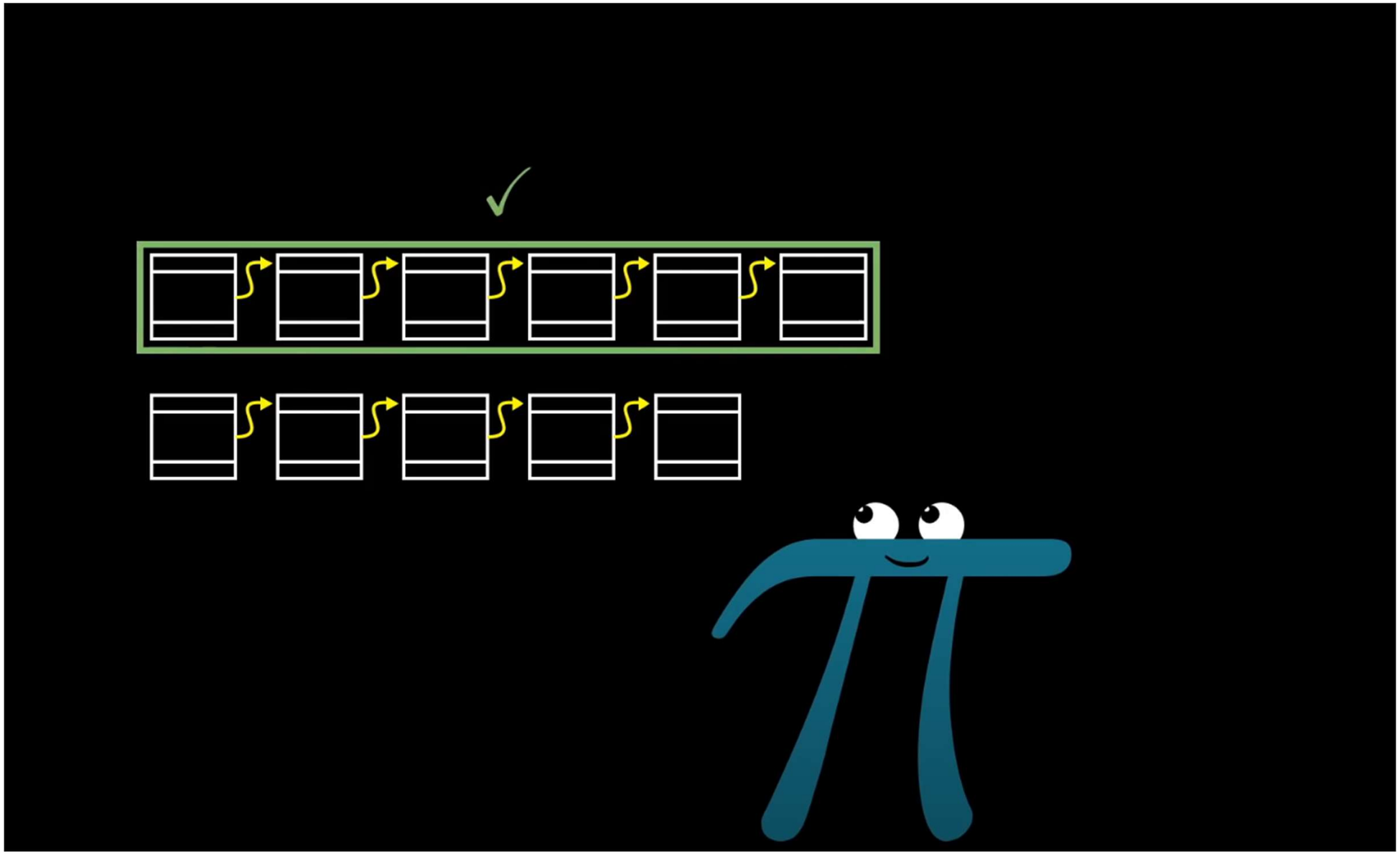
این در حالی است که کار بقیه کسانی که فقط از شبکه جهت انجام تراکنش استفاده میکنند تنها اعلام تراکنش و سپس دریافت و ثبت بلاک در صورت درست بودن هش است



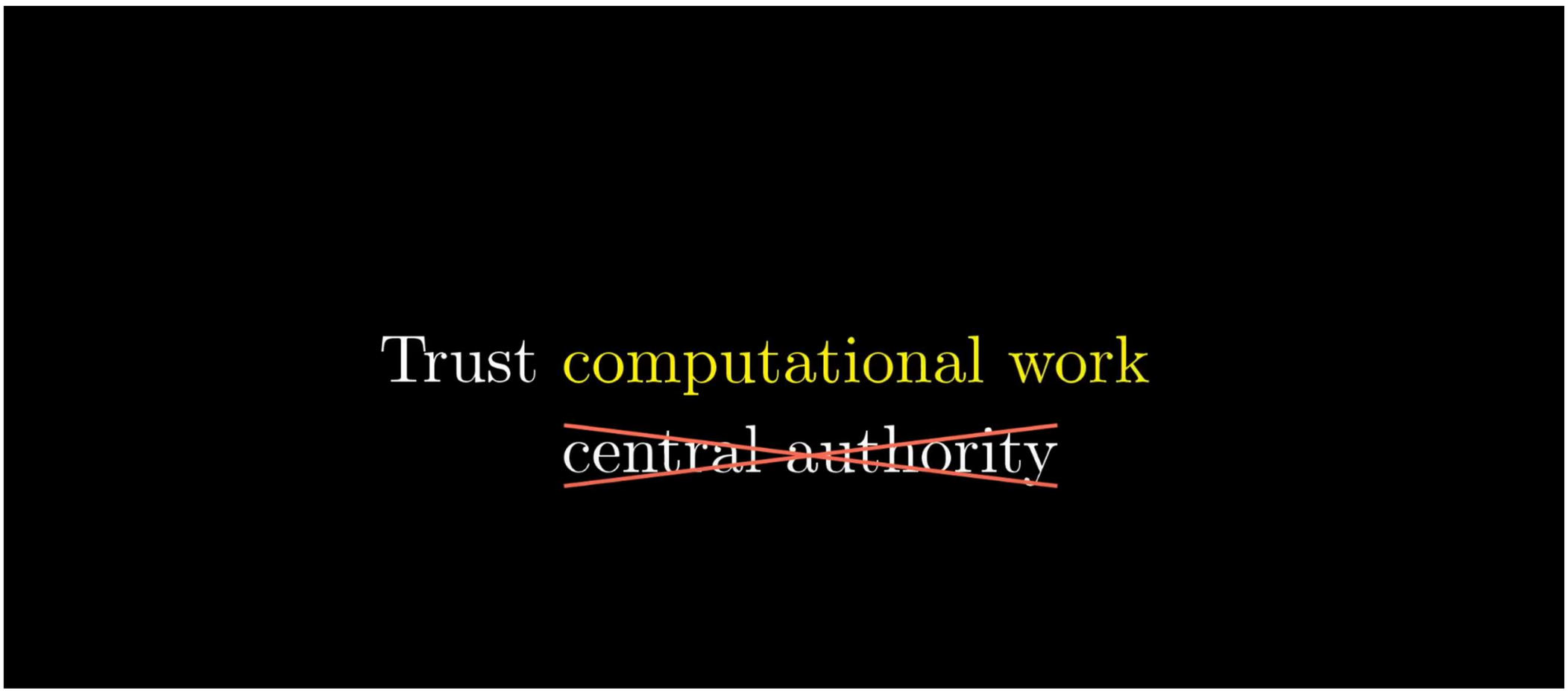
نکته کلیدی دیگر این است که در صورتی که دو بلاکچین مختلف دریافت شد
آن بلاکچینی که تعداد بلاک بیشتری دارد و یا به عبارت دیگر کار محاسباتی بیشتری انجام داده است
مورد قبول است



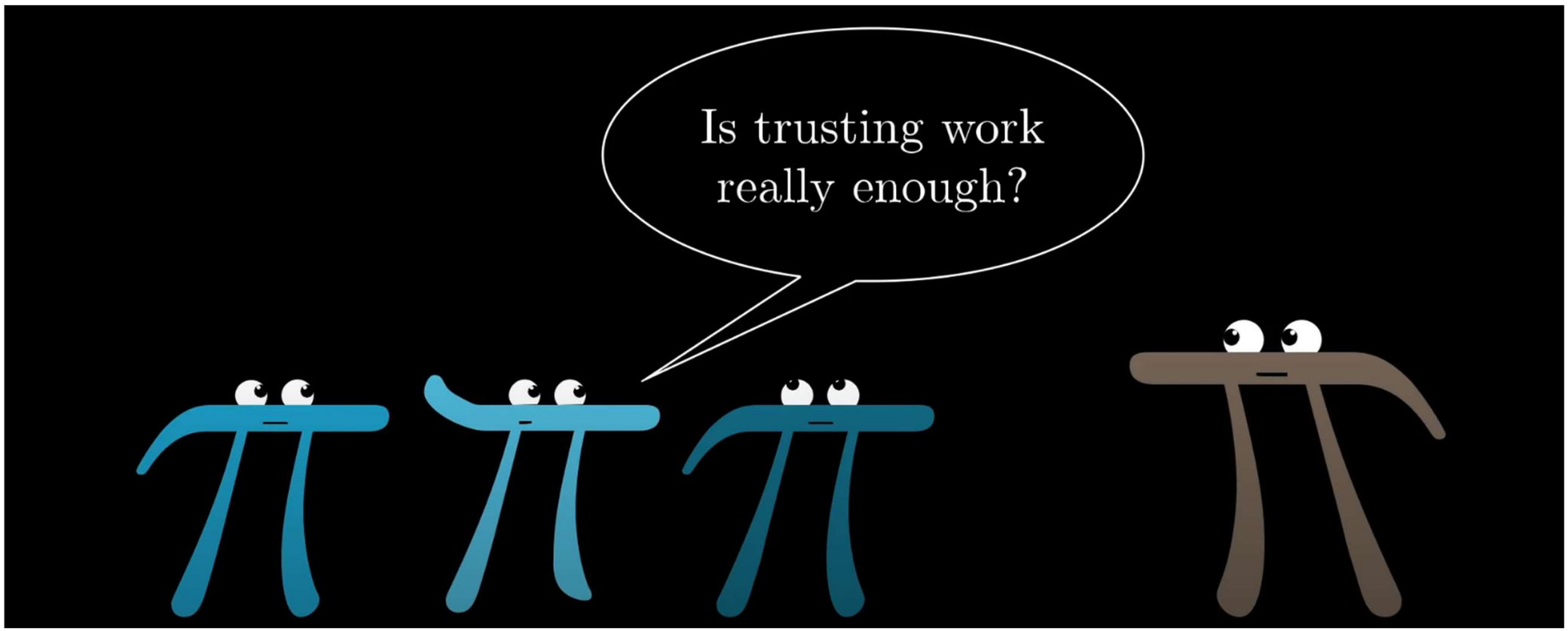




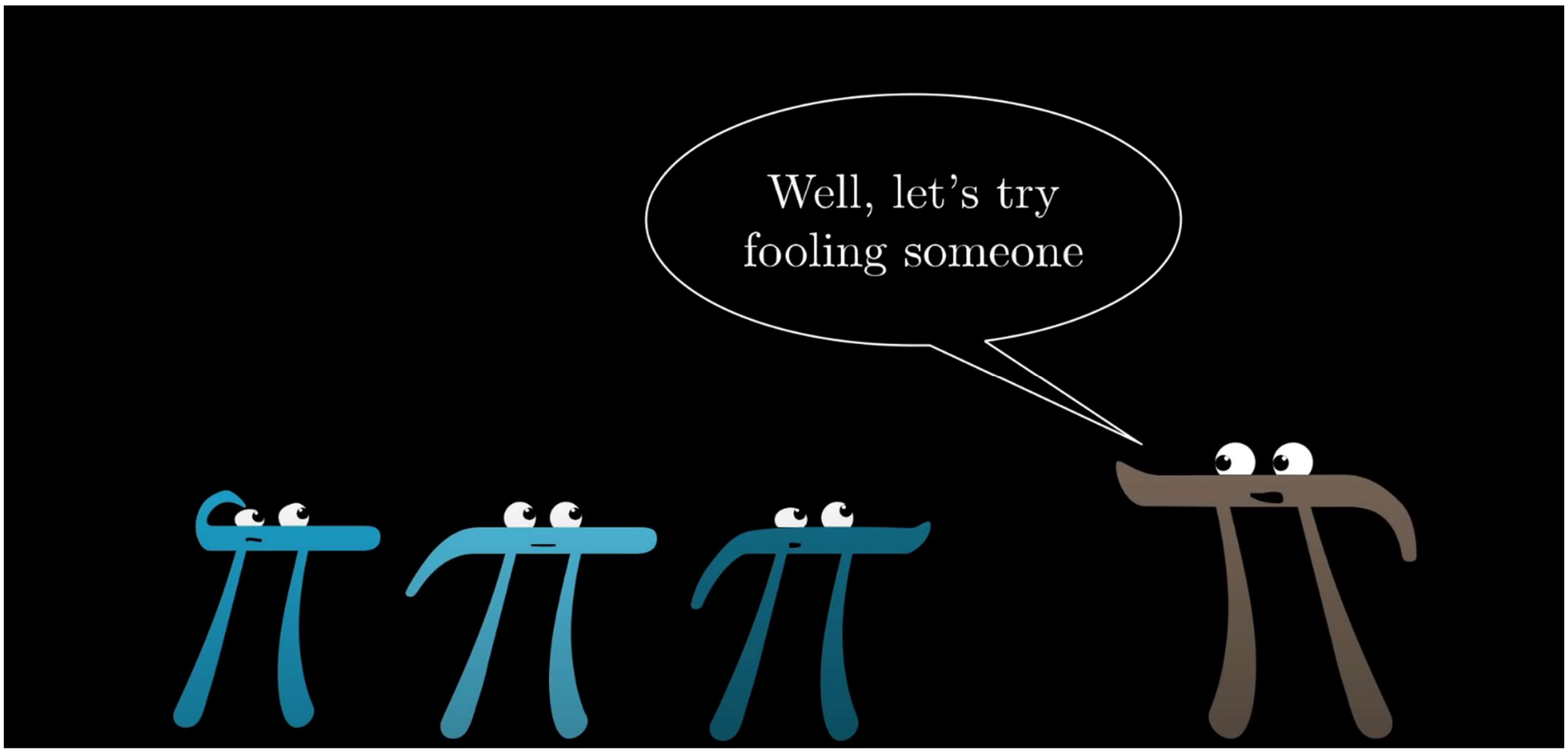
بنابراین بجای اعتماد به یک سیستم متمرکز که به ما بگوید کدام بلاکچین معتبر و مورد قبول است
وقتی همه به توافق برسیم که بلاکچینی که بیشترین کار محاسباتی را انجام داده مورد قبول است
به یک اجماع غیر متمرکز دست میابیم



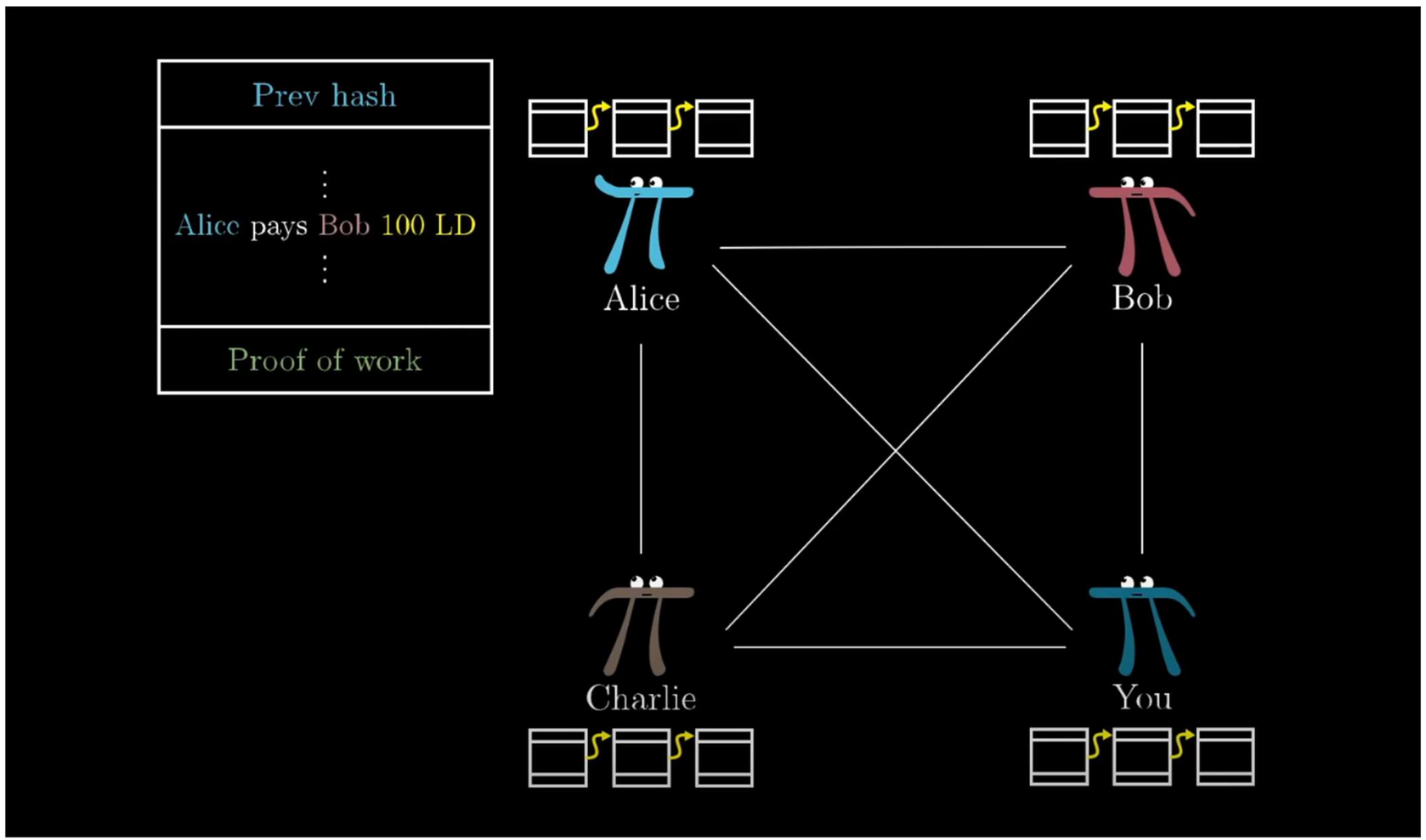
آیا اعتماد به بیشترین کار محاسباتی کافی است؟

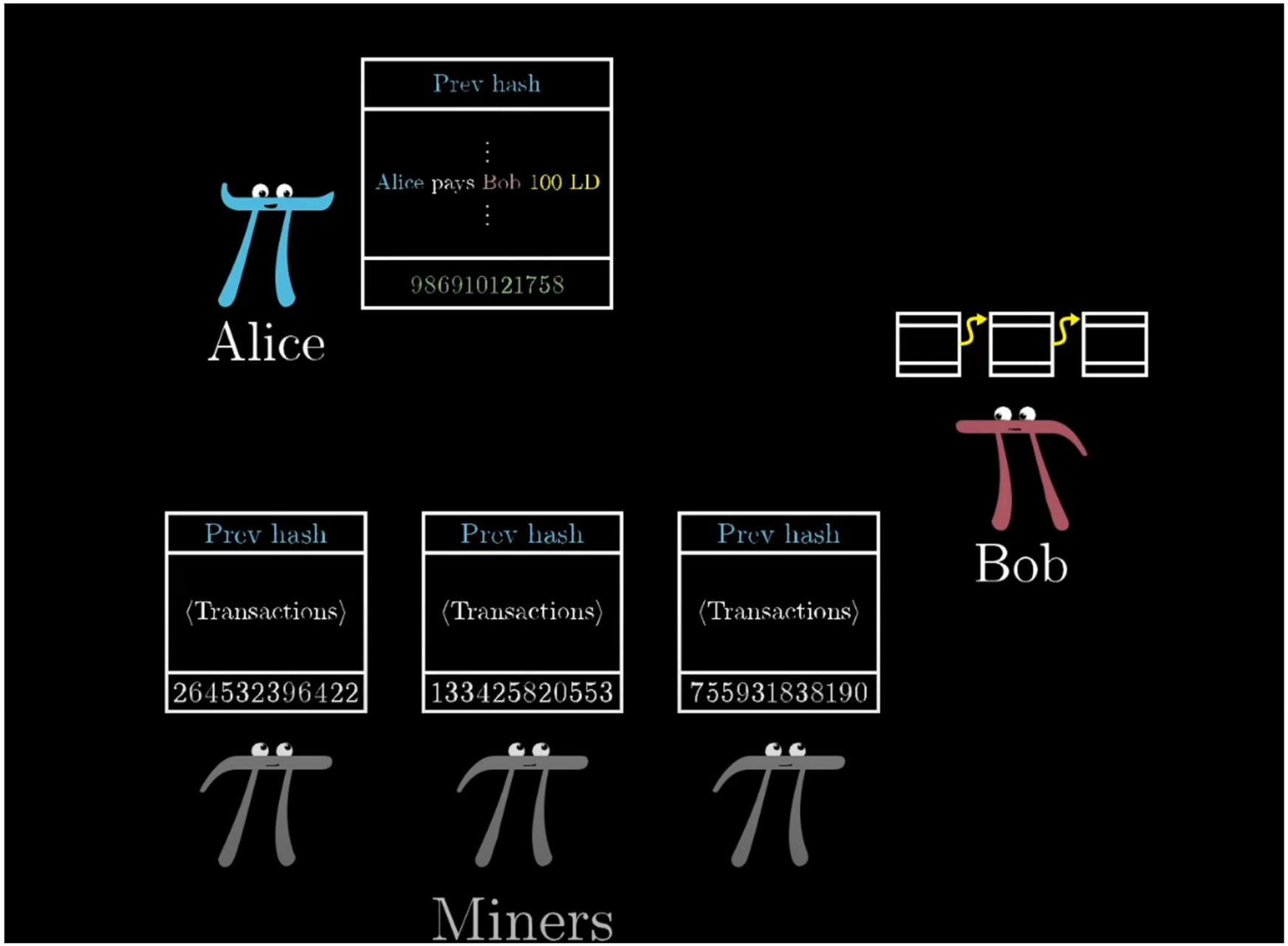


آیا میشود چنین سیستم غیر متمرکزی را گول زد؟



فرض کنید Alice یک بلاک برای Bob بفرستد که در آن قید شده که 100 دلار به او پرداخت کرده
و این بلاک را برای بقیه شبکه ارسال نکند
بنابراین بقیه هنوز تصور میکنند که او هنوز آن 100 دلار را دارد





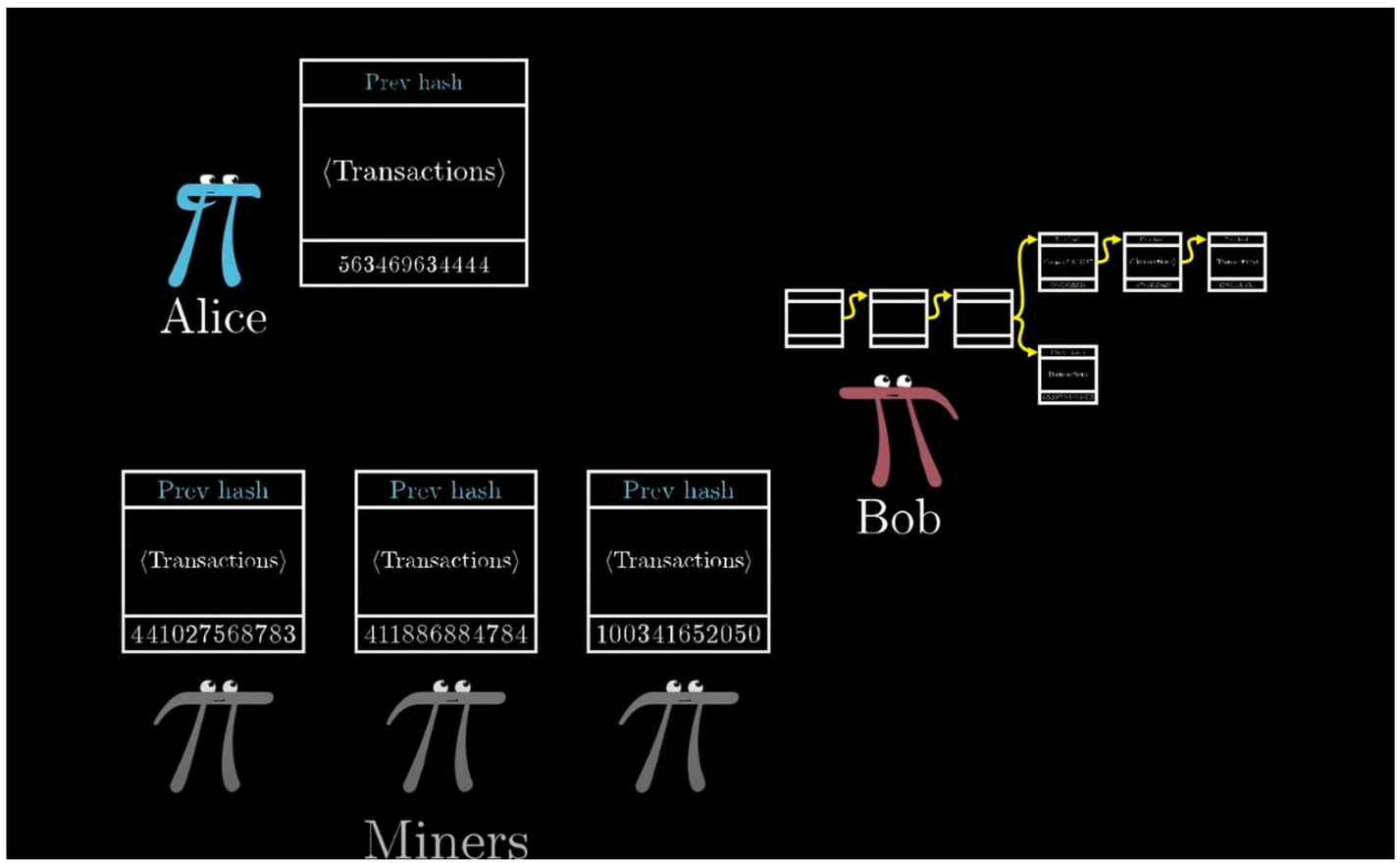
بنابراین Alice مجبور است که قبل از بقیه هش بلاک را حدس زده و آن را ثبت کند

این اتفاق دور از دسترس نیست و احتمال انجامش وجود دارد

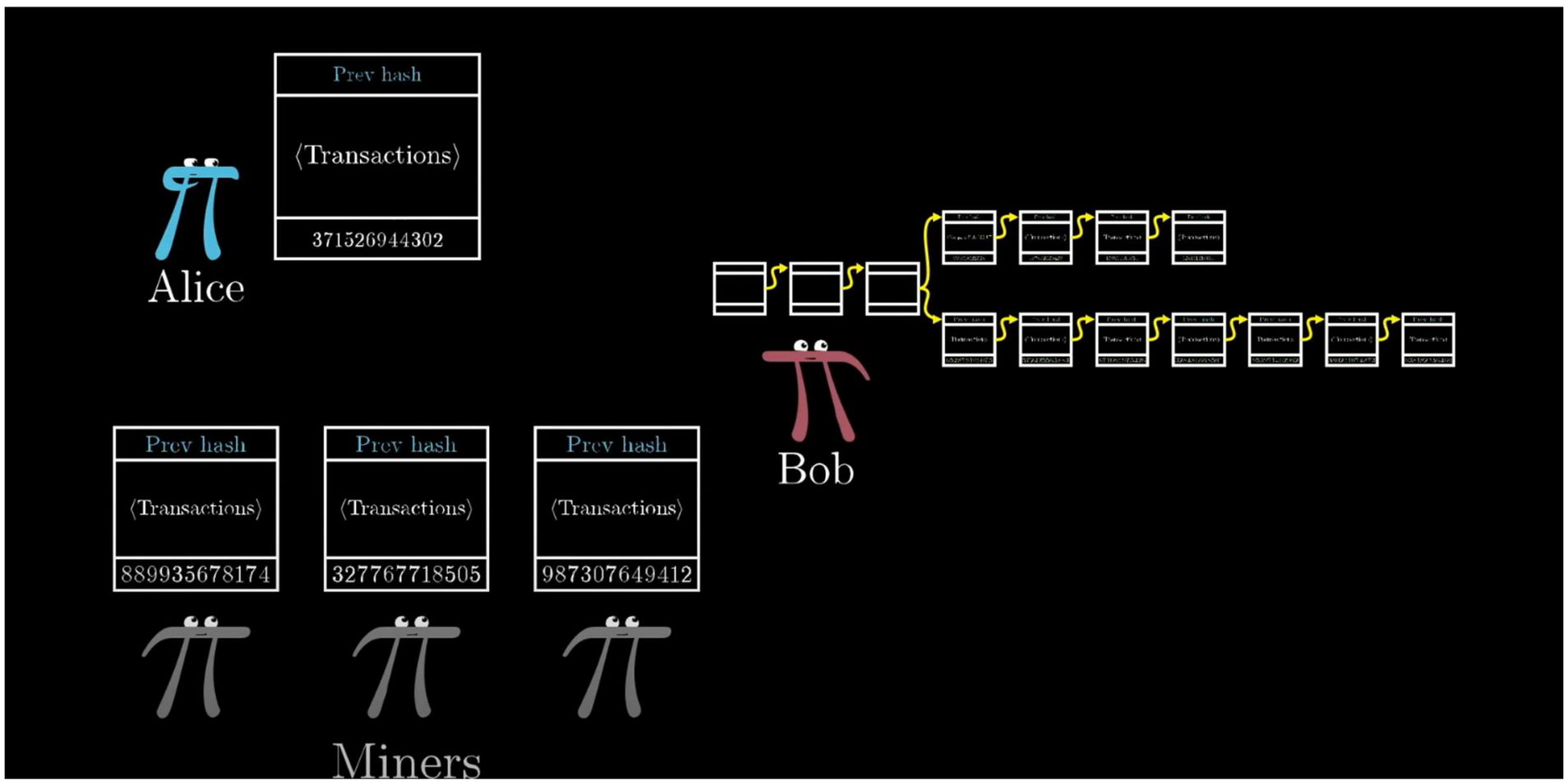
ولی Bob همچنان بلاکهای بقیه را هم میشنود

لذا برای اینکه Alice بتواند Bob را گول بزند باید همچنان به تولید بلاکهای جدید ادامه دهد تا طولانیترین بلاکچین را داشته و بتواند او را متقاعد کند که این تراکنش درست است

طبق قوانین Bob به بلاکچینی اعتماد میکند که بیشترین کار محاسباتی را انجام داده یعنی طولانیترین بلاکچین است

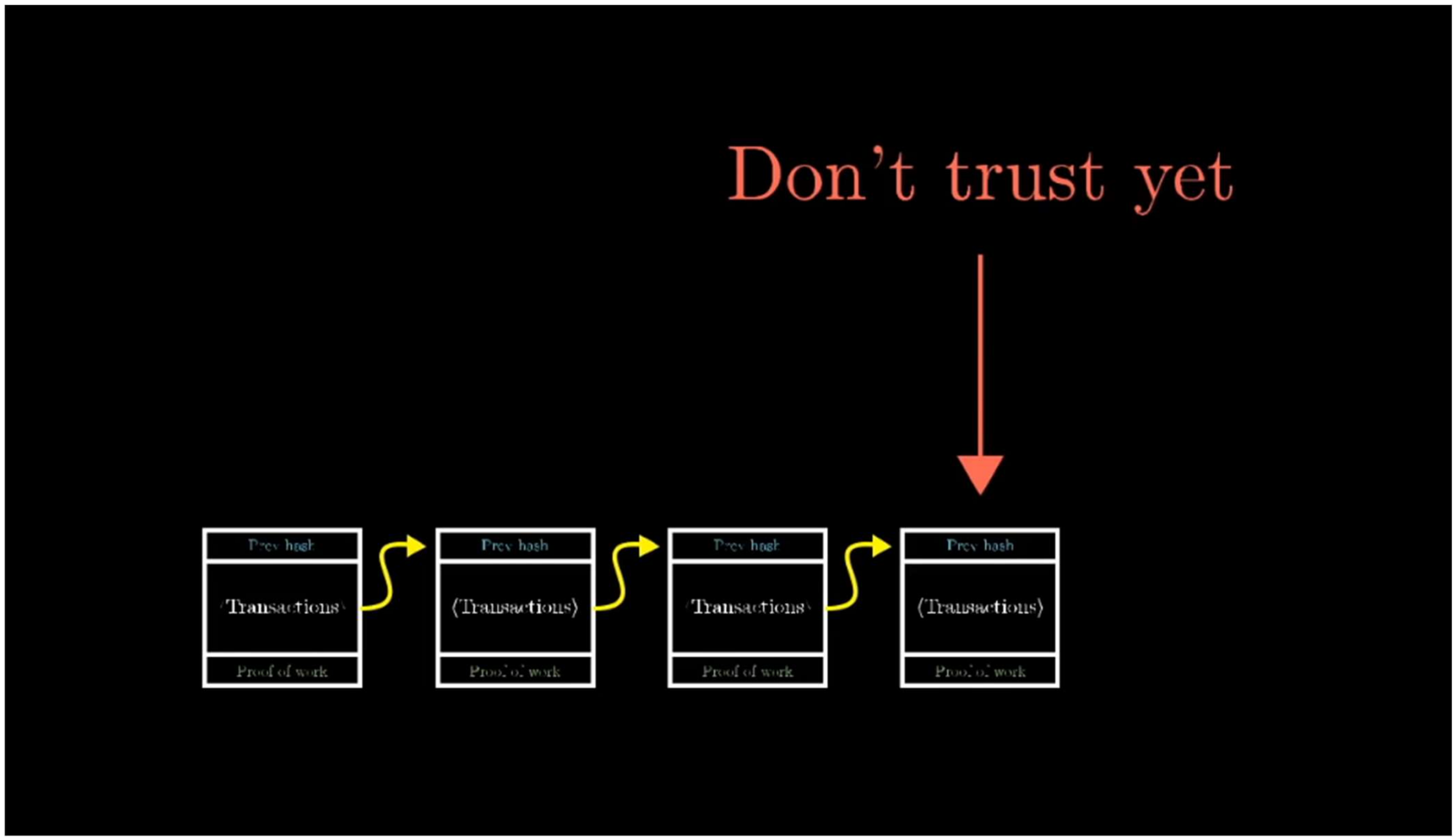


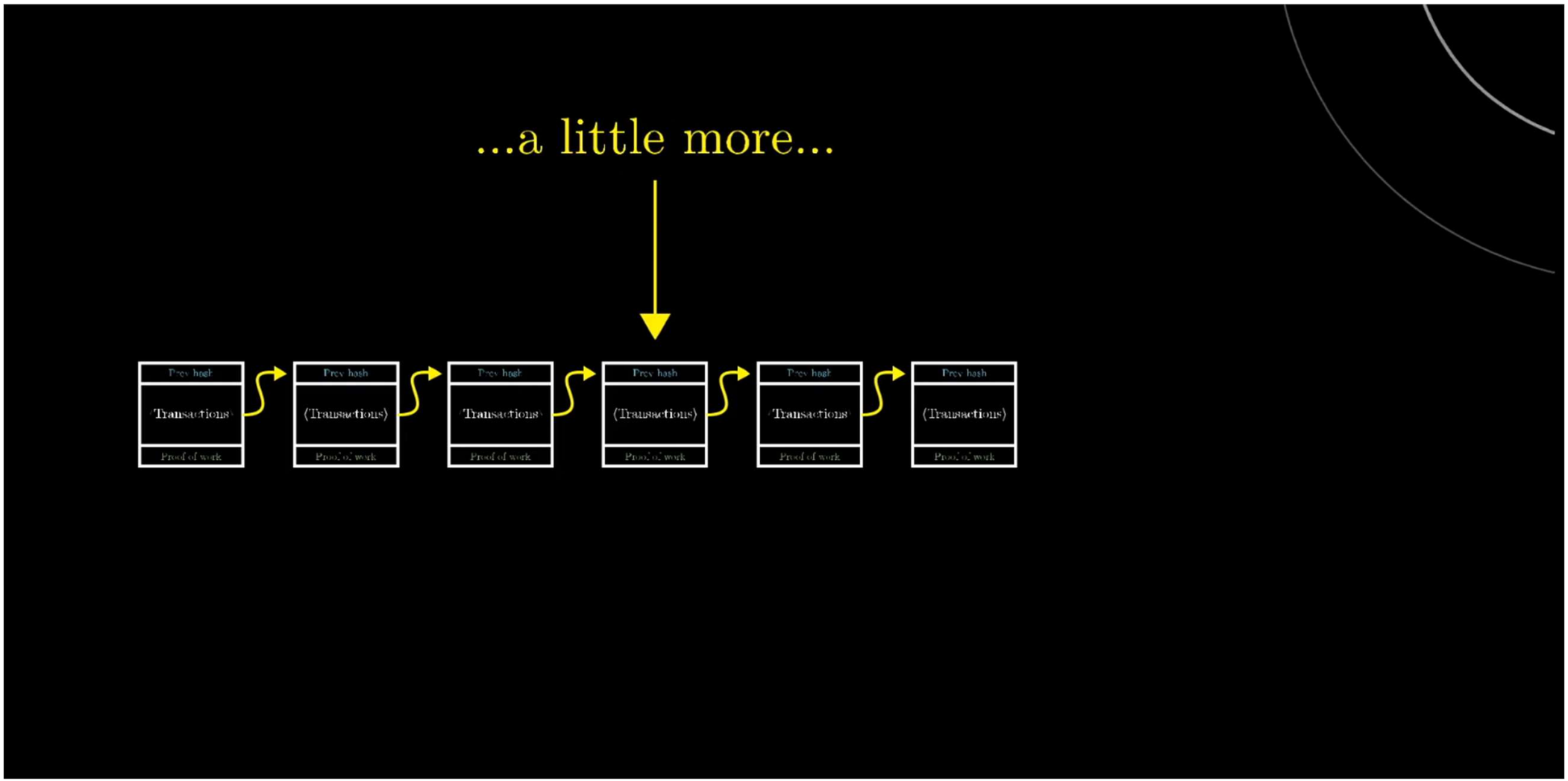
تنها در صورتی که Alice بیشتر از 50% قدرت محاسباتی شبکه را داشته باشد
میتواند به این روند ادامه داده و موفق شود
در غیر اینصورت نهایتا بلاکچین ارسال شده توسط بقیه ماینرها طولانیتر شده
و بلاکچین Alice رد میشود

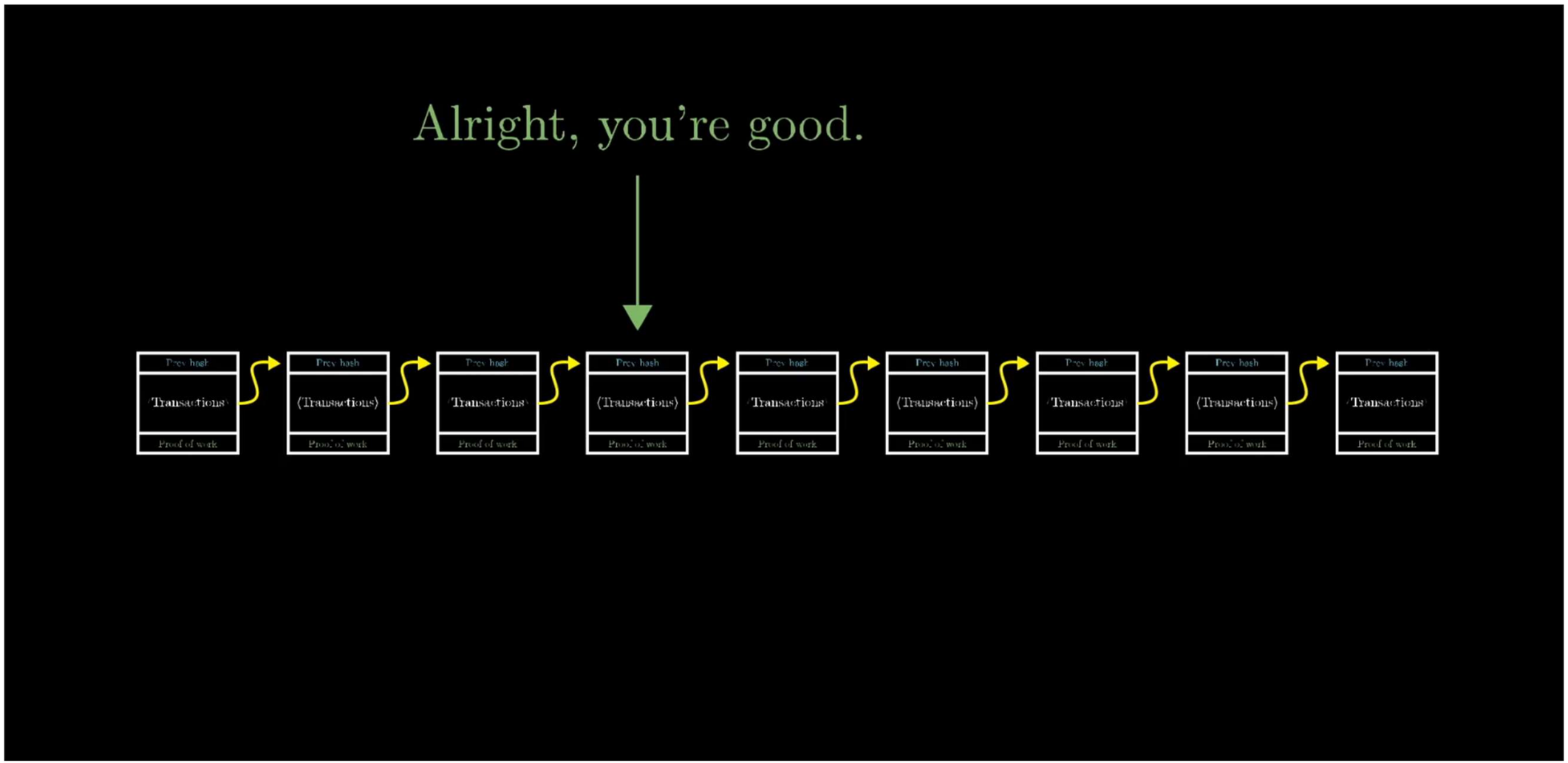


در نتیجه به محض دریافت یک بلاک، بلافاصله به آن اعتماد نکرده و نپذیرید

اجازه دهید چند بلاک در ادامه ثبت شود تا از صحت آن اطمینان داشته باشید

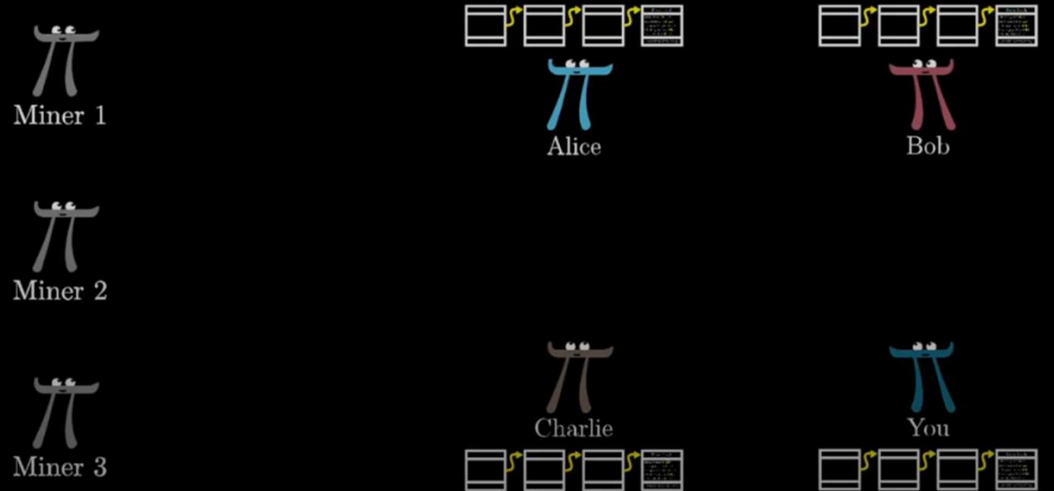






Main ideas

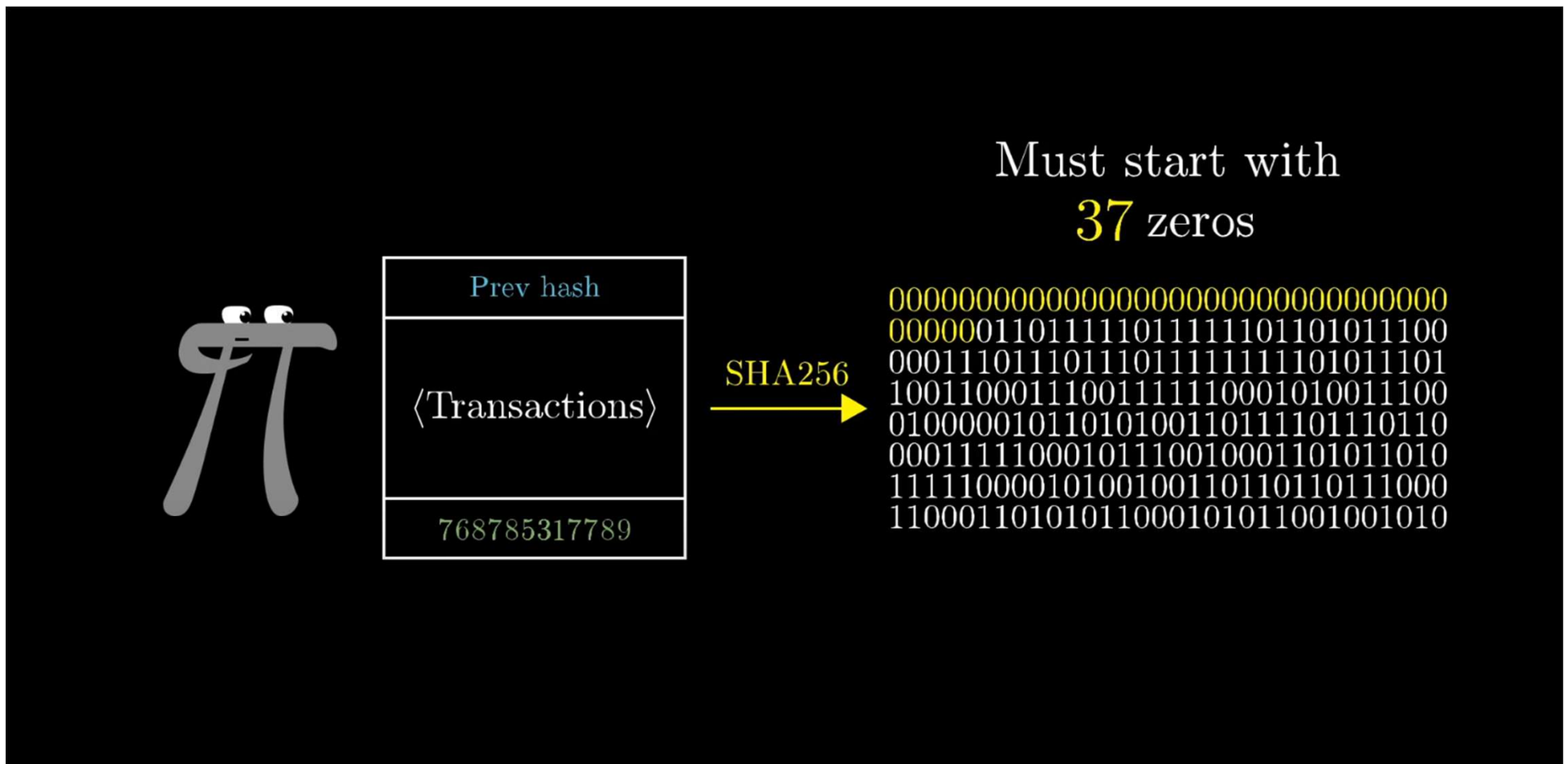
- Digital signatures
- The ledger is the currency
- Decentralize
- Proof of work
- Block chain



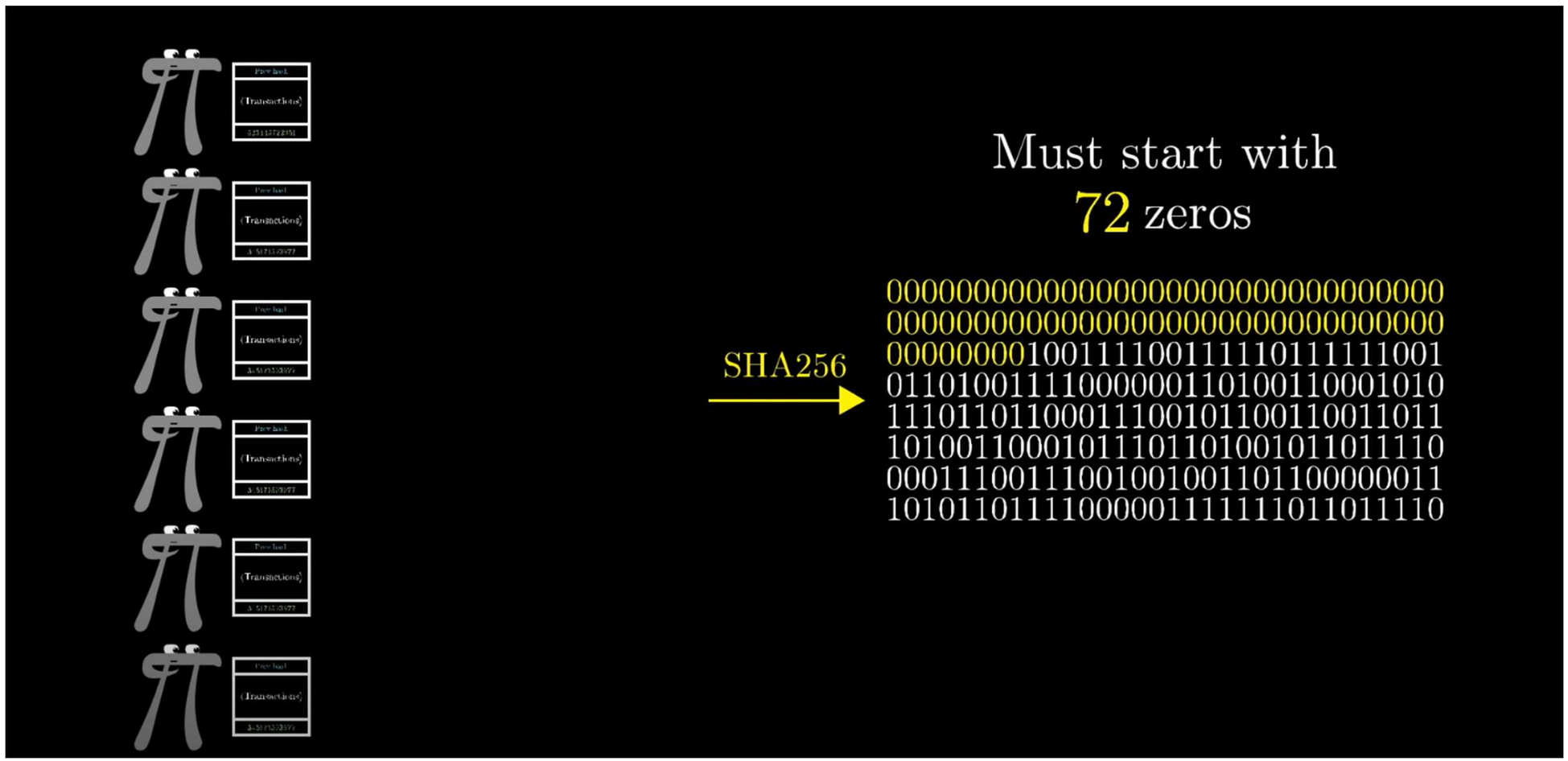
ساختاری که ایجاد و مورد بررسی قرار گرفت رویه کارکرد بیتکوین و بسیاری از رمزارزهای دیگر است

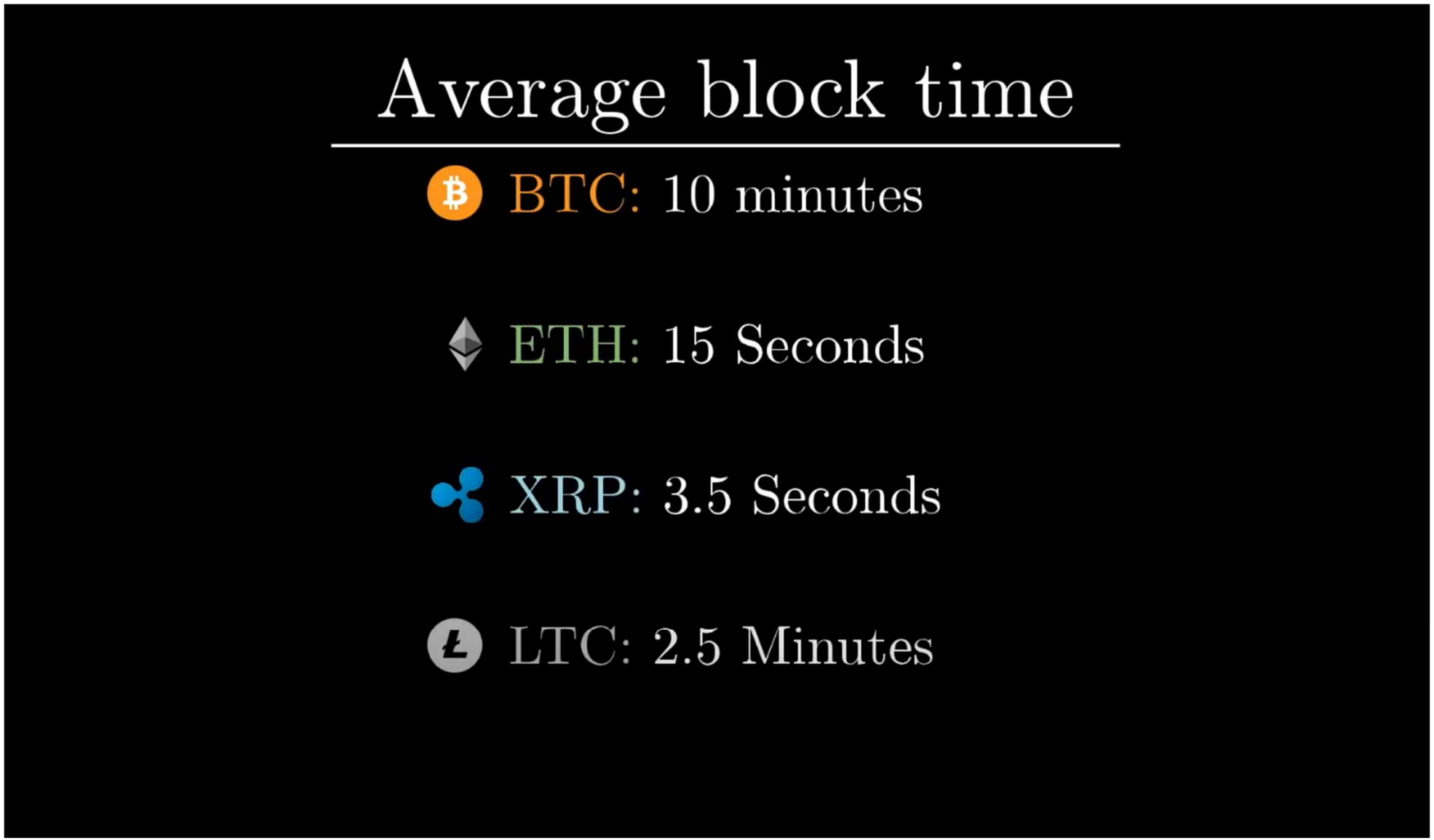
تنها در مورد هش بلاک و تعداد صفرهای ابتدای آن لازم به ذکر است

طبق پروتوکل بیتکوین تعداد صفرها مدام در حال تغییر است
به گونه ای که همیشه زمان تقریبی جهت حدس زدن هش بلاک
حدود 10 دقیقه باشد

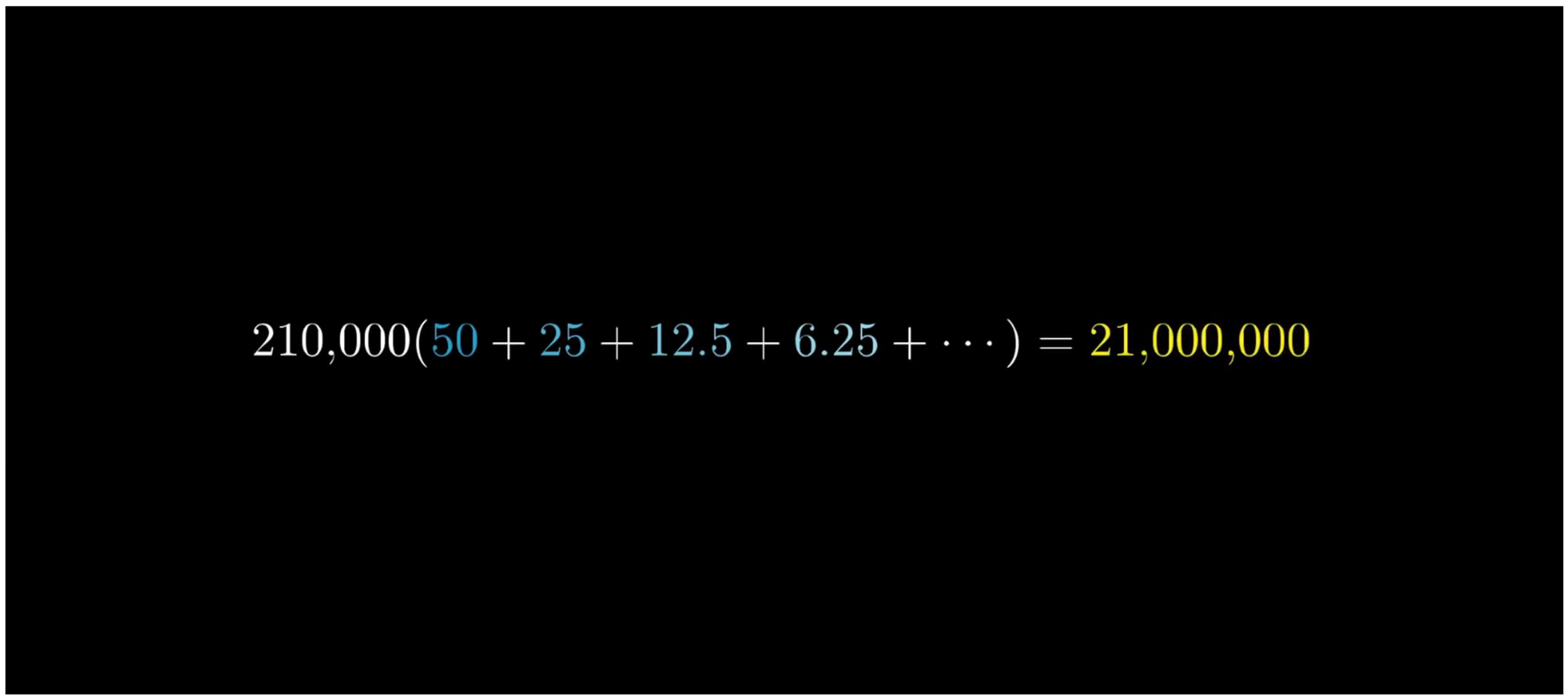


در نتیجه با افزایش قدرت محاسباتی ماینرها و هش ریت شبکه، تعداد صفرهای ابتدای هش افزایش یافته
و حل این پازل برای دریافت پاداش آن و تولید بیتکوین سختتر میشود

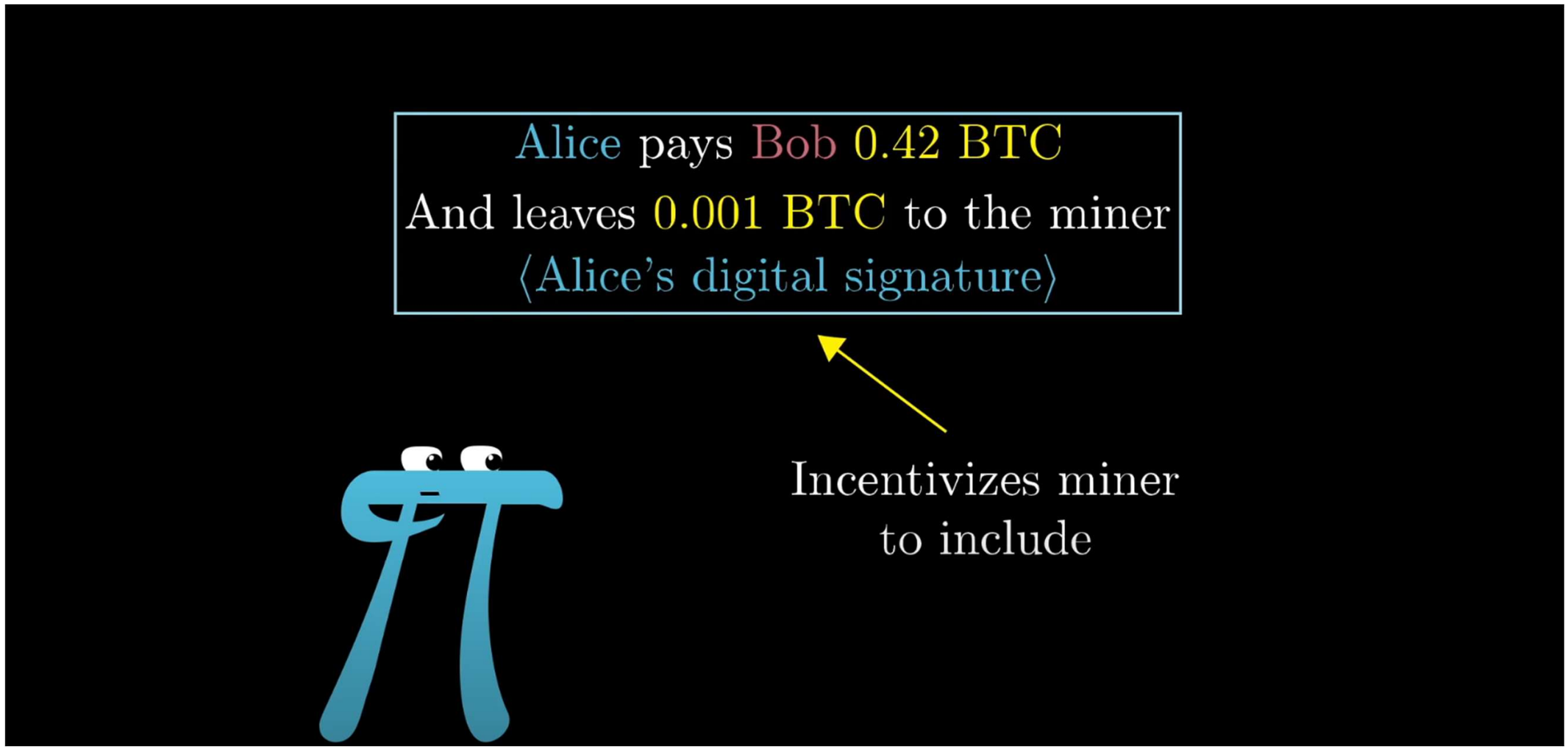




همانگونه که گفته شد پاداش تولید و ثبت بلاک بروی شبکه بیتکوین از 50 بیتکوین
به ازای هر بلاک شروع شده و هر 4 سال یا به عبارت دیگر هر 210000 بلاک این پاداش نصف میشود
که با محاسبه آن خواهیم دید که میزان نهایی بیتکون استخراج شده ماکسیموم 21 ملیون بیتکوین است که
این میزان جزیی از الگوریتم بیتکوین است و قابل تغییر نمیباشد.



علاوه بر پاداش تولید بلاک، ماینرها بابت ثبت تراکنشها نیز پاداشی به عنوان هزینه تراکنش دریافت میکنند



هزینه تراکنش برای ایجاد انگیزه برای ماینرها جهت ثبت تراکنش میباشد

زیرا هر بلاک تعداد محدودی تراکنش را میتواند شامل شود