



# ***Blockchain***

---

Blockchain based Data Distribution and Traceability Framework in the  
Electric Information Management System

Atousa Toghyani & Sara Kochakinejad



# *Contents*

- 01** *Introduction*
- 02** *Related Work*
- 03** *Methodology*

**Implementation  
and Results** **04**

**Conclusions** **05**





# 01

---

## *Introduction*



---

سیستم های اطلاعاتی نقشی اساسی در جامعه مدرن دارند. سیستم های اطلاعاتی به طور کلی به سخت افزار ، برنامه های دیجیتال ، ذخیره سازی ، سیستم های ارتباطی ، خدمات اینترنتی و تقریباً هر جنبه دیگری از زیرساخت های فناوری یک کسب و کار ، سازمان ، دولت ، مدرسه یا گروه دیگر اشاره دارند که مفهوم داده های بزرگ را تشکیل می دهند. فناوری Blockchain به طور فزاینده ای در سیستم اطلاعات مدیریت به ویژه در جنبه امنیت داده ها نقش مهمی دارد.

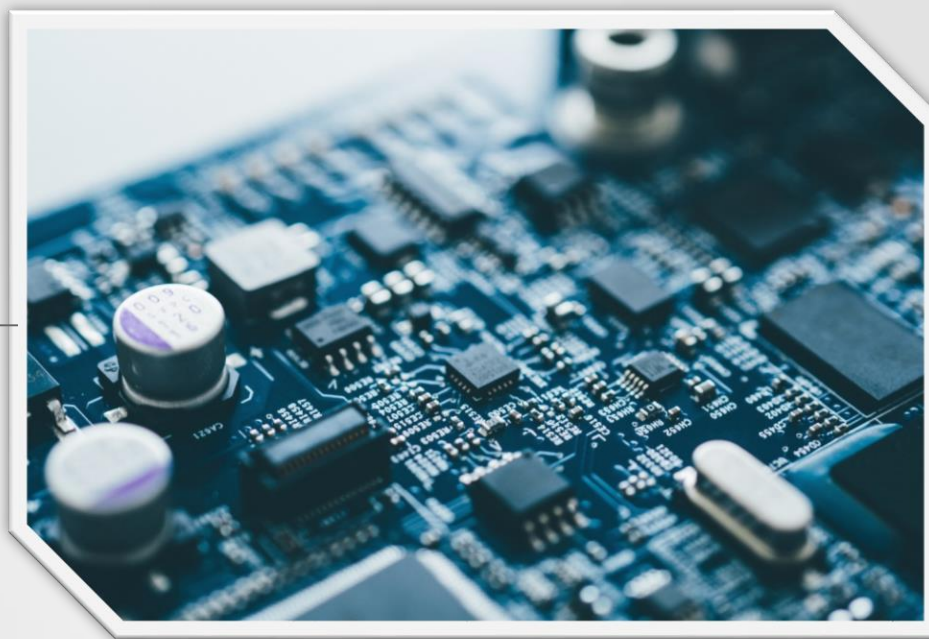
---



# *Electric Information Management System*

سیستم مدیریت اطلاعات الکتریکی نقش مهمی در امنیت تأمین انرژی ملی دارد. داده های حساس زیادی در سیستم وجود دارد و کنترل و ردیابی دسترسی این مجموعه داده ها ضروری است.

همراه با توسعه زیرساخت های فناوری اطلاعات ، به اشتراک گذاری اطلاعات بیشتر و راحت تر می شود ، با این وجود مشکل امنیت داده ها را نیز به همراه دارد.





# بلاک چین چیست؟

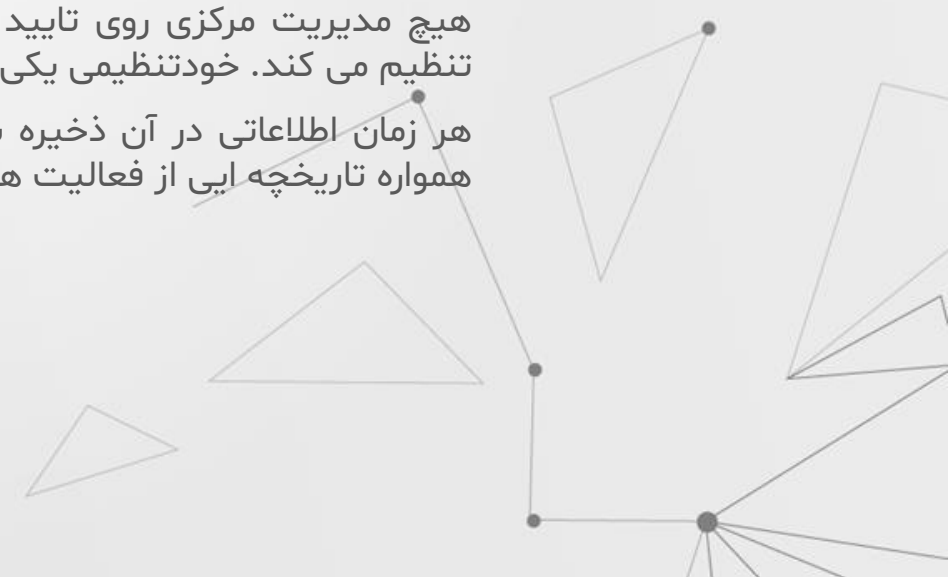
بلاک چین یک نوع سیستم ثبت اطلاعات و گزارش است. تفاوت آن با سیستم‌های دیگر این است که اطلاعات ذخیره‌شده روی این نوع سیستم، میان همه اعضای یک شبکه به اشتراک گذاشته می‌شود. با استفاده از رمزنگاری و توزیع داده‌ها، امکان هک، حذف و دستکاری اطلاعات ثبت‌شده، تقریباً از بین می‌رود.

بلاک چین زیرساختی توزیع شده است که اجازه می‌دهد اطلاعات را با بالاترین استاندارد امنیتی ممکن از یک مکان به مکان دیگر انتقال دهید.

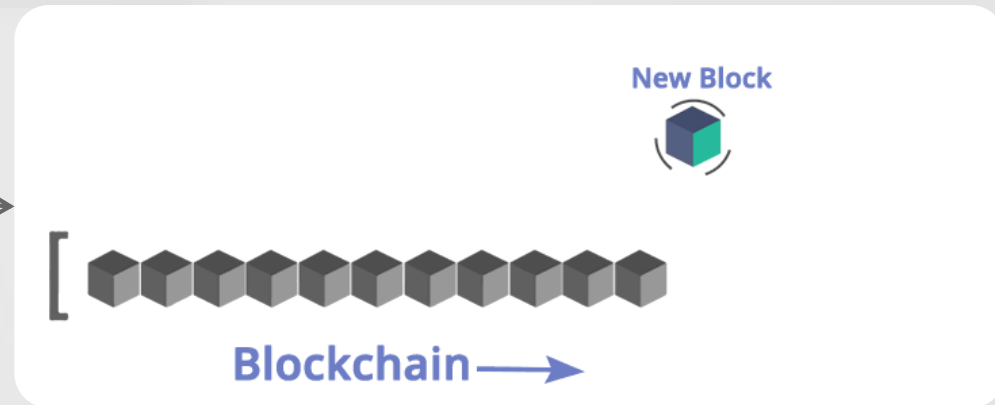
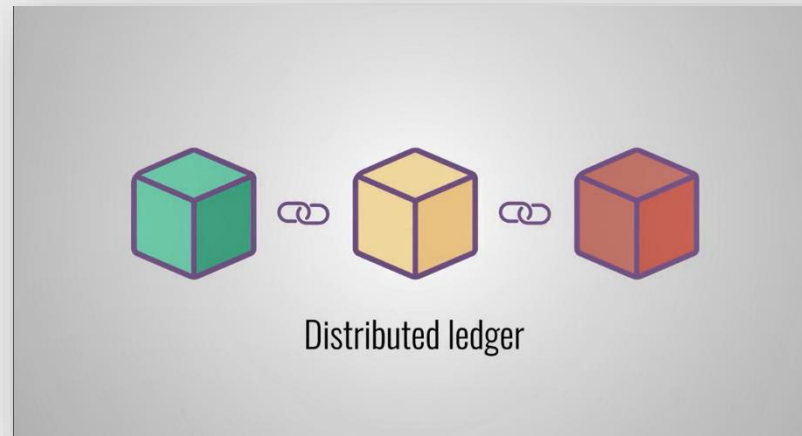
یک فناوری متن باز است که در تملک هیچ انسانی قرار نداشته و می‌تواند یک بانک اطلاعاتی، پروتکل یا نرم افزار باشد.

هیچ مدیریت مرکزی روی تایید اعتبار تراکنش‌ها وجود نداشته و این خودفناوری است که همه چیز را تنظیم می‌کند. خودتنظیمی یکی از مهمترین نوآوری‌های به کارگرفته شده در بلاک چین است.

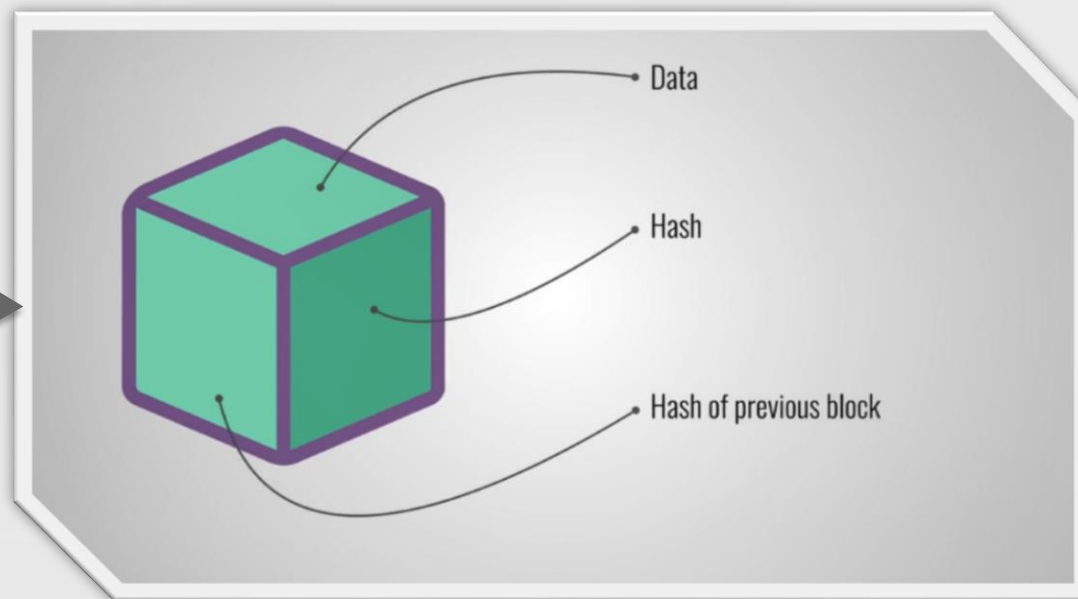
هر زمان اطلاعاتی در آن ذخیره سازی می‌شود، امکان رونویسی یا تغییر اطلاعات وجود ندارد. در نتیجه همواره تاریخچه‌ای از فعالیت‌ها ثبت می‌شود.



# بلاک چین چیست؟

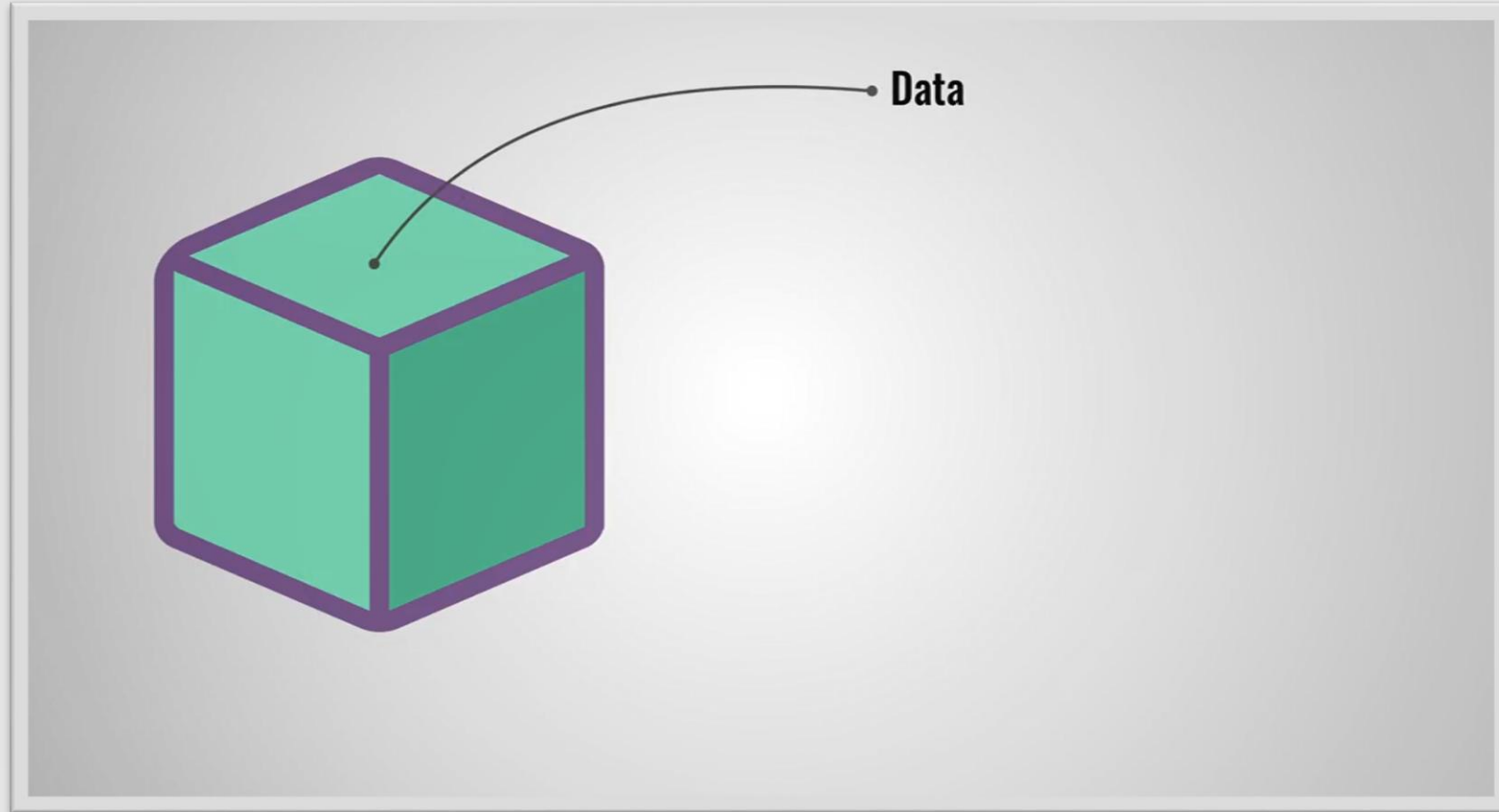


# بلاک چیست؟

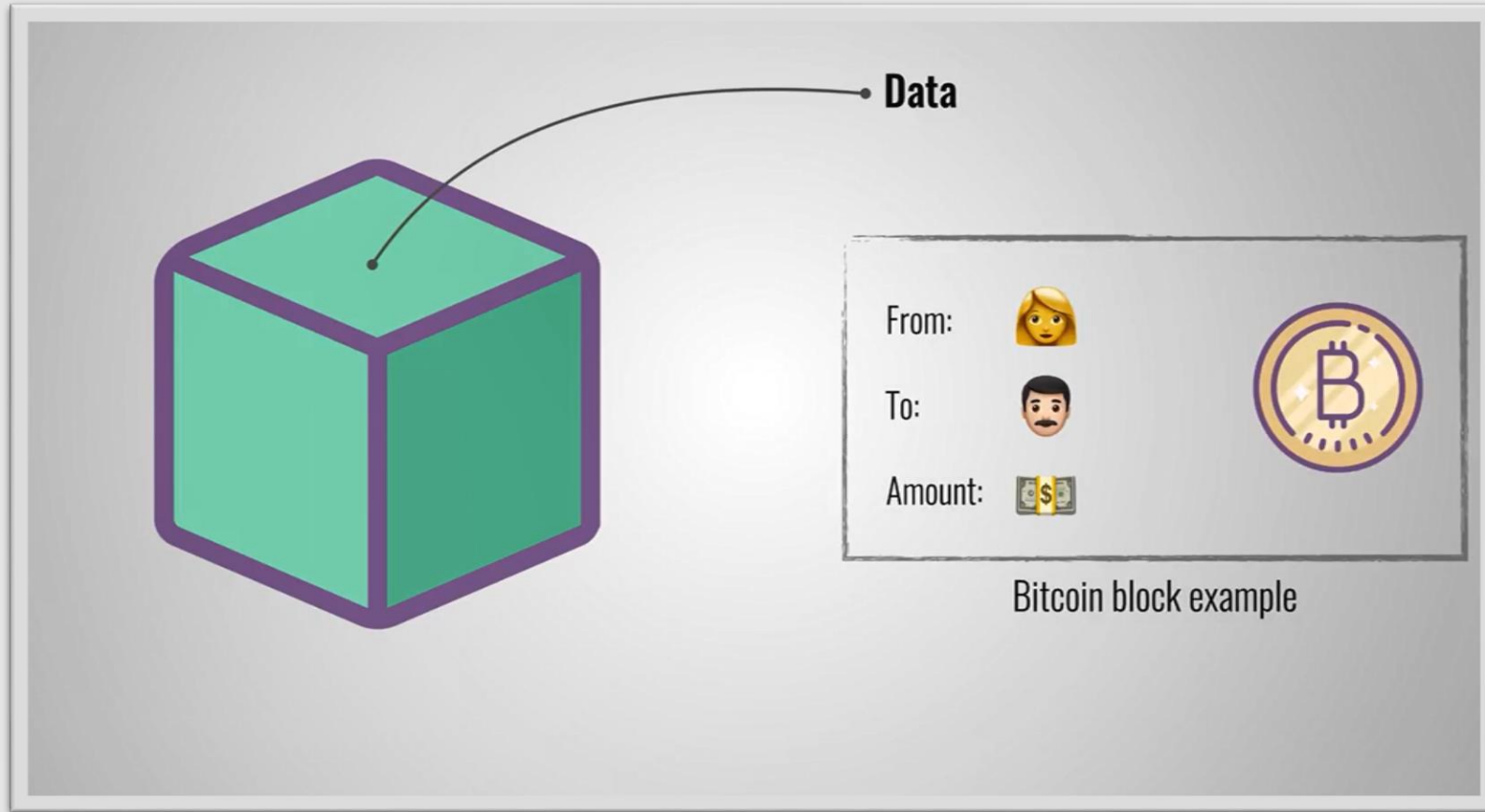




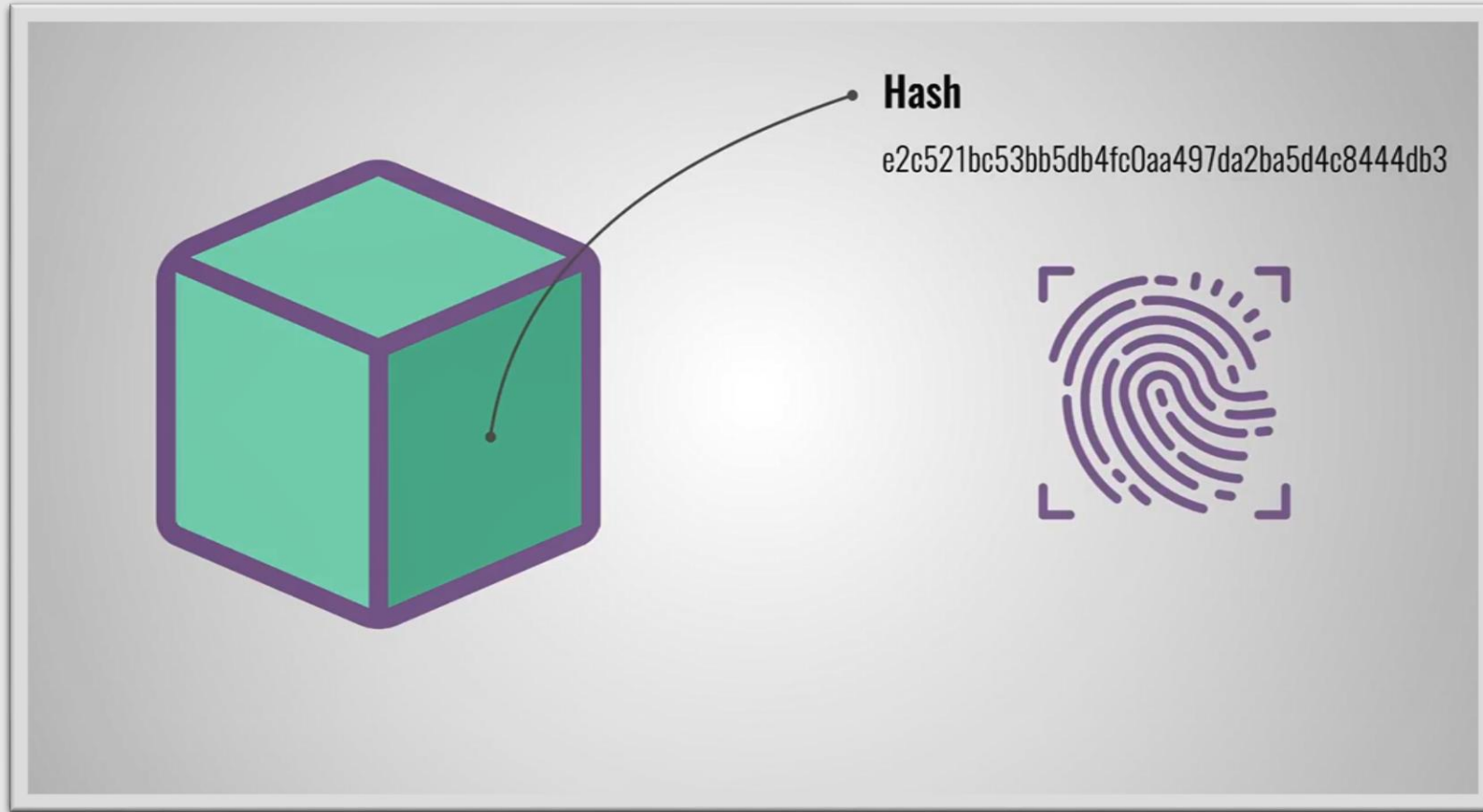
# بلاک چیست؟



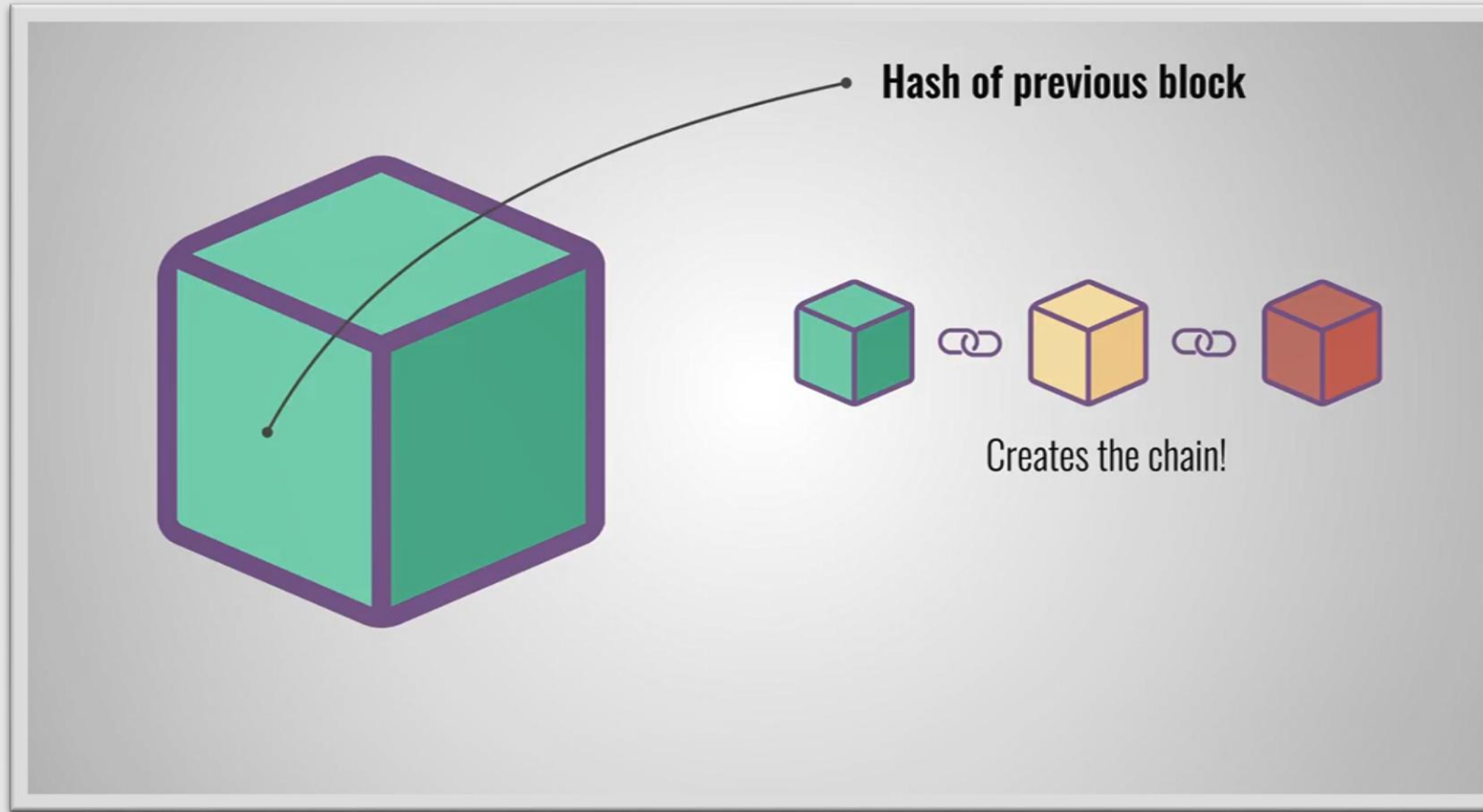
# بلاک چیست؟



# بلاک چیست؟



# بلاک چیست؟





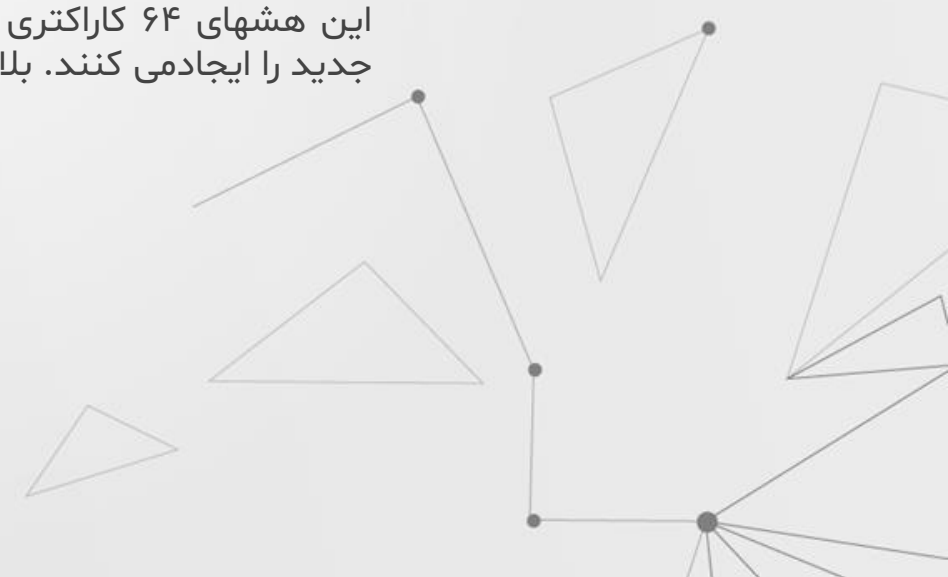
# بلاک چین چگونه کار می کند؟

---

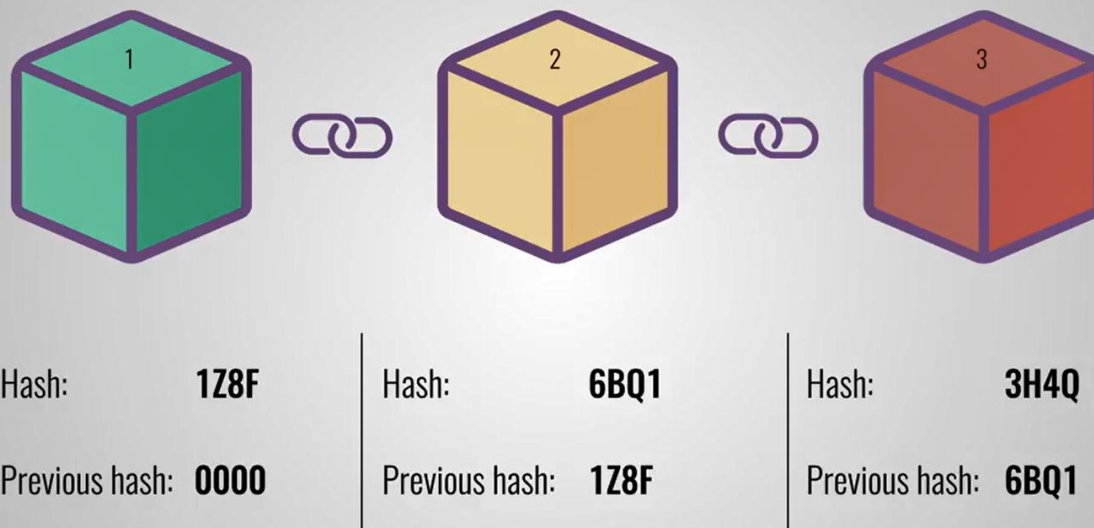
از طریق به کارگیری مکانیزم رمزگذاری، تراکنش ها به شکل مادام العمر و عمومی ضبط می شوند. هر یک از تراکنش ها مهر زمانی داشته، ترتیب خطی دارند و رشته کاراکترهای یکبار مصرف داده ای یا هش ها را ایجاد می کنند.

در شرایط خاص بلاک های دیجیتالی ساخته شده تنها زمانی که دو طرف موافقت خود را اعلام کنند تنها می توانند به روزرسانی شوند، در نتیجه امکان حذف یا ویرایش اطلاعات مجاور یکدیگر تقریباً غیرممکن است. همین موضوع باعث شده تا امکان دستکاری اطلاعات یا درج اطلاعات غیر معتبر در این فناوری غیرممکن باشد.

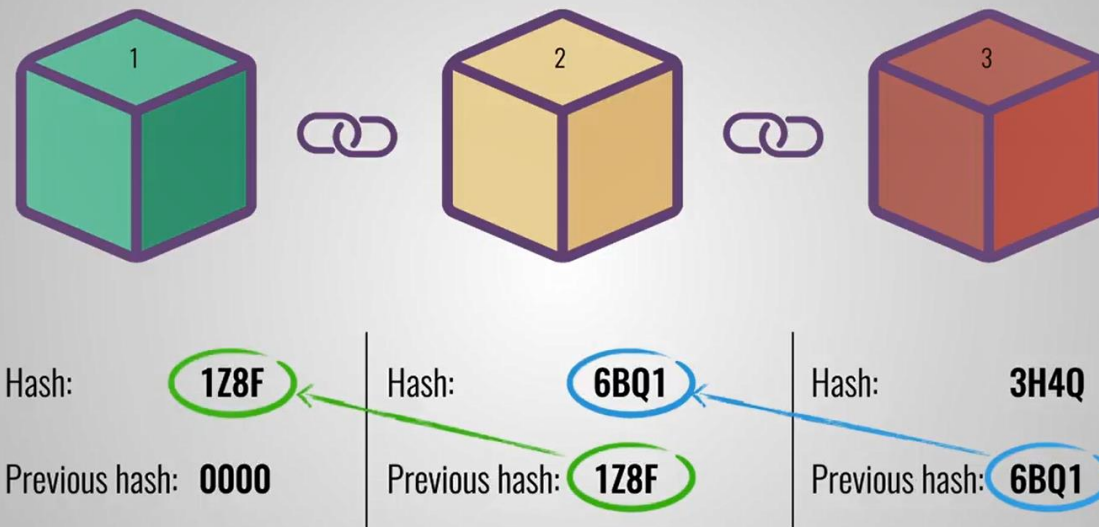
این هشهای ۶۴ کاراکتری تولید شده باکدهای هش قبلی ترکیب شده و به این شکل یک بلاک جدید را ایجاد می کنند. بلاکی که با بلاک قبل تراز خود مرتبط است.



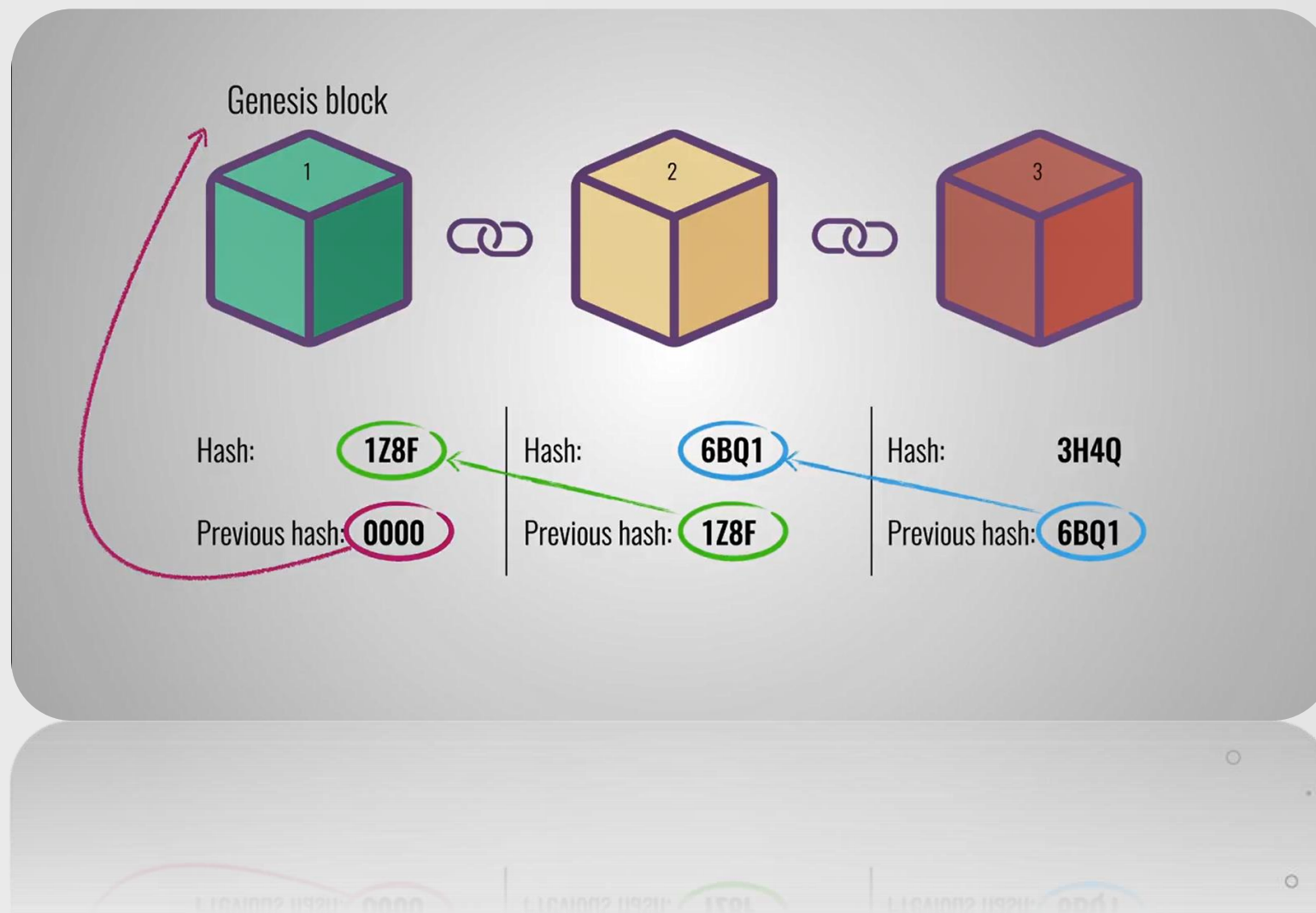
# بلاک چین چگونه کار می کند؟



# بلاک چین چگونه کار می کند؟

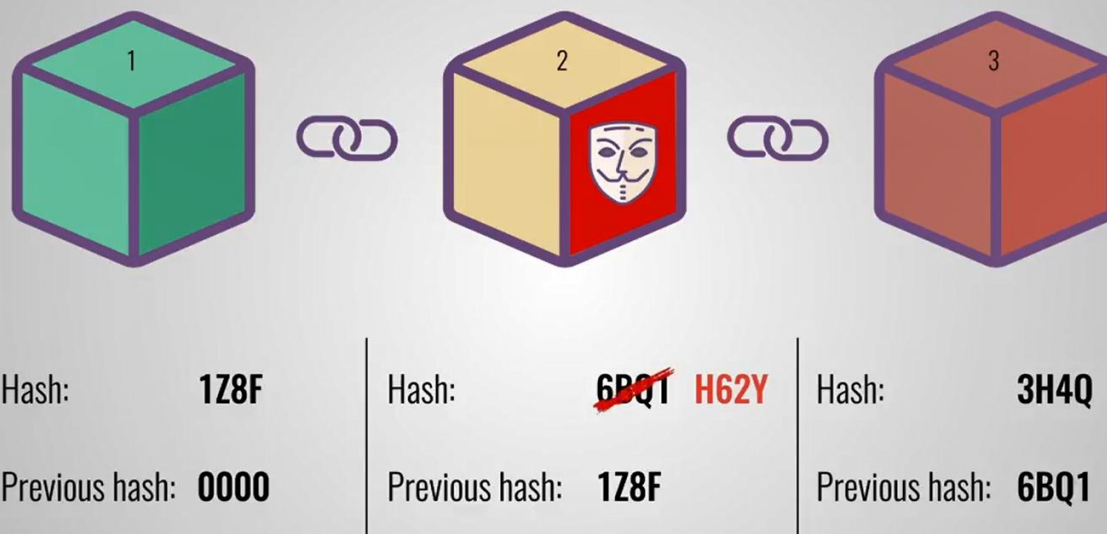


# بلاک چین چگونه کار می کند؟





# بلاک چین چگونه کار می کند؟



# بلاک چین چگونه کار می کند؟



Hash: **1Z8F**

Previous hash: **0000**

Hash:

~~6BQ1~~ **H62Y**

Previous hash: **1Z8F**

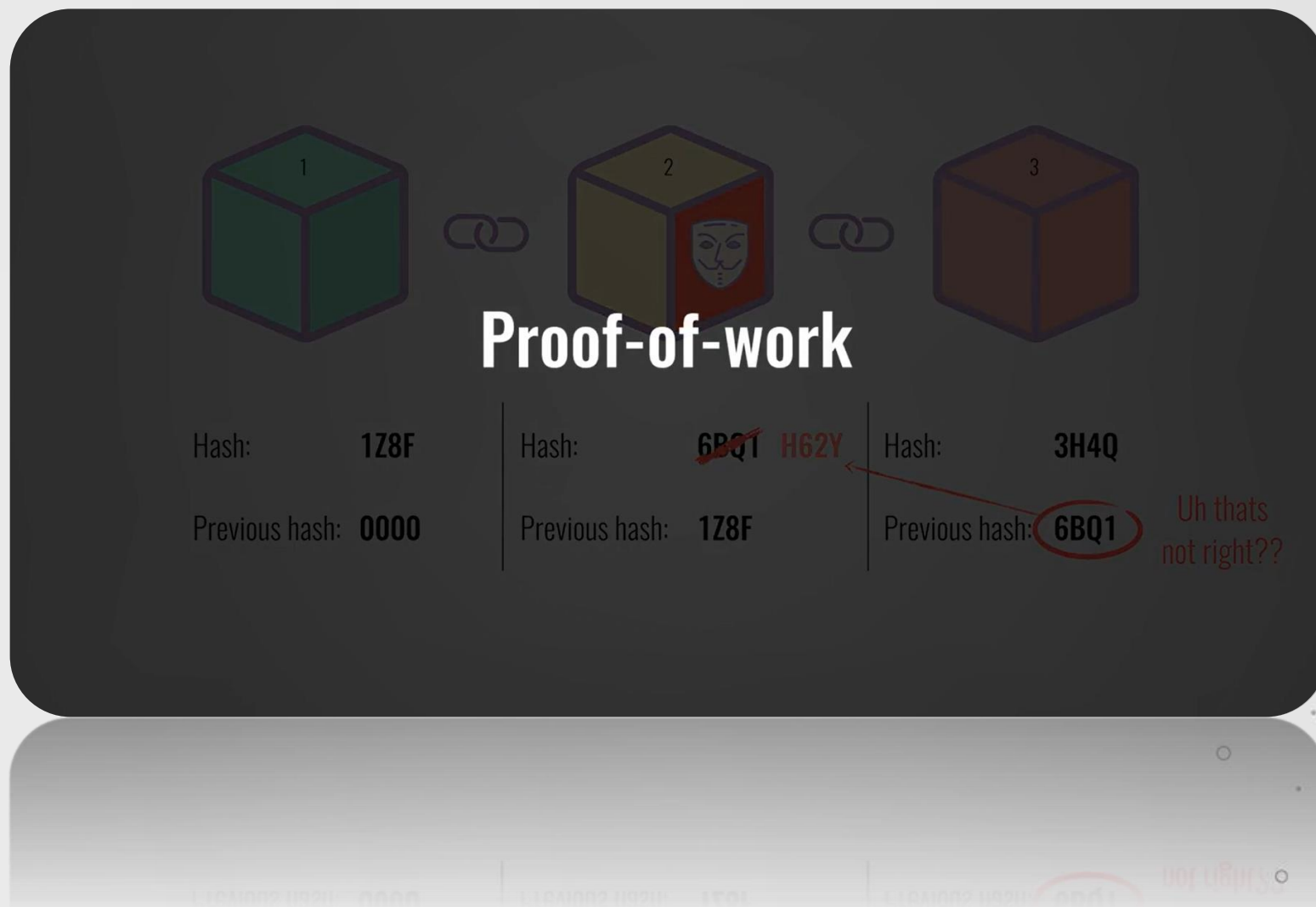
Hash:

**3H4Q**

Previous hash: **6BQ1**

Uh thats  
not right??

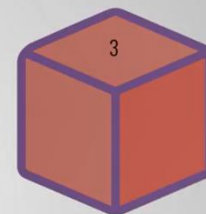
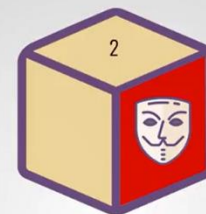
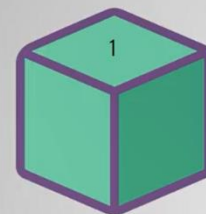
# بلاک چین چگونه کار می کند؟



# بلاک چین چگونه کار می کند؟



Slow and steady...

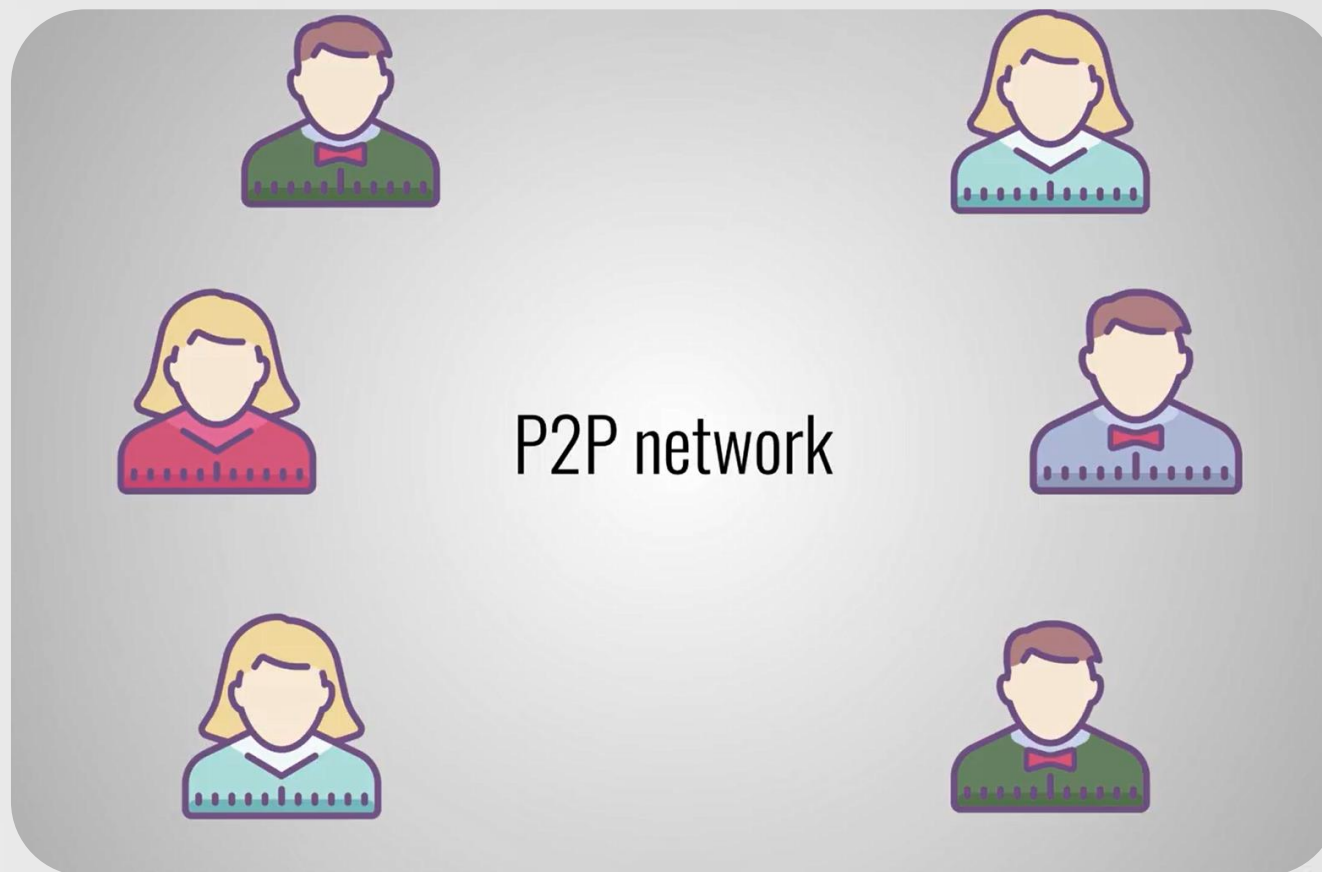


10 minutes

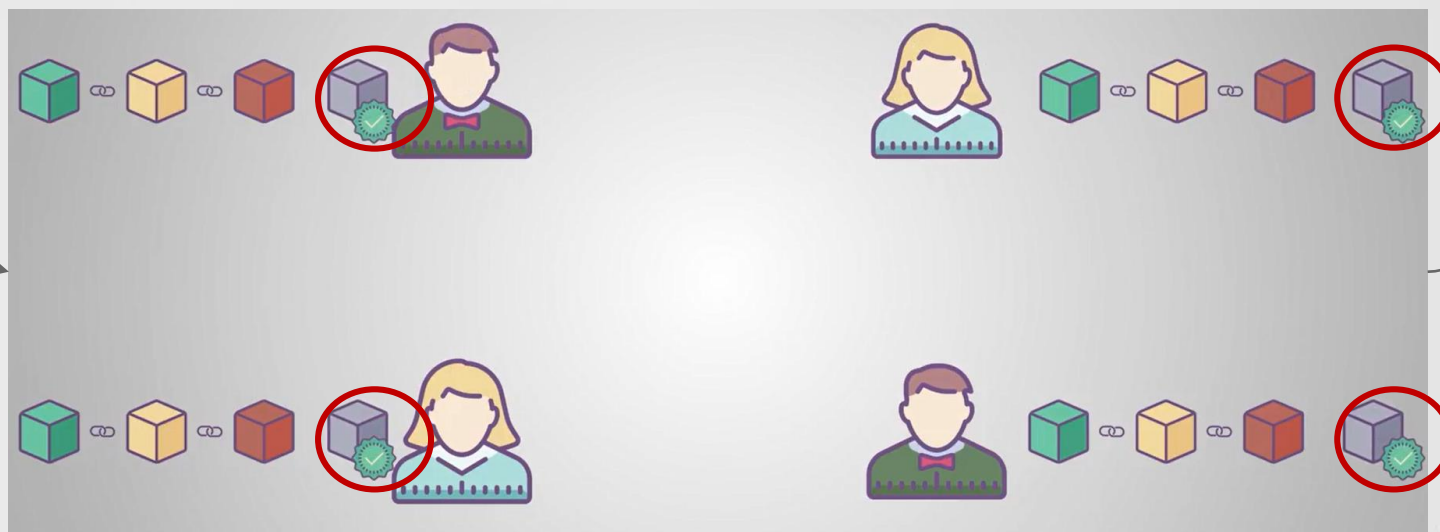
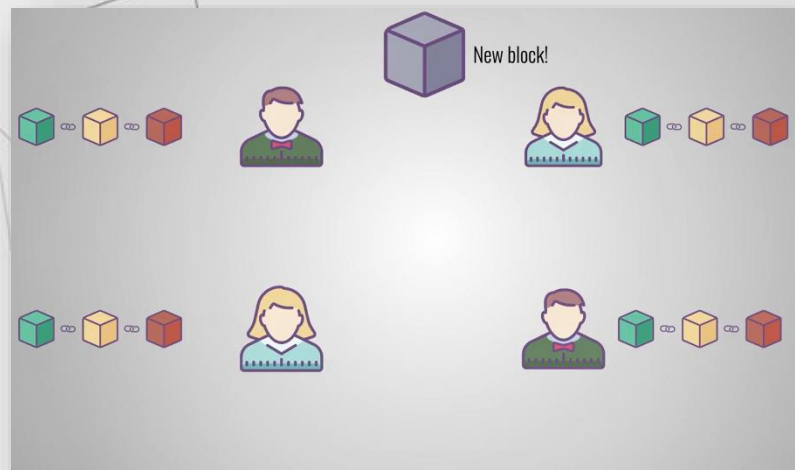


10 minutes

# بلاک چین چگونه کار می کند؟



# بلاک چین چگونه کار می کند؟



# کاربرد های بلاک چین:



Bank



Energy



Health



IOT



## دو نوع شبکه بلاک چین وجود دارد:

Permissionless or  
public blockchains

اینها شبکه های منبع باز هستند که هرکسی می تواند به آنها دسترسی پیدا کند و از آنها استفاده کند (مانند کاربران بیت کوین که با استفاده از بیت کوین برای پرداخت با یکدیگر معامله می کنند).

Permissioned  
blockchains

این شبکه ها شبکه های اختصاصی هستند که افراد یا نهادهای خاص برای انجام معاملات از آنها استفاده می کنند (مانند گروهی از بانک ها که تراکنش های مالی را پردازش می کنند).



# برخی اصطلاحات بلاک چین:

Distributed ledger technology (DLT)

Proof of work

Proof of stake

Mining

Virtual currency

Virtual currency exchange

Cryptocurrency

Token





02

---

*Related Work*

# Related Work

## Data distribution and traceability analysis

---

همراه با توسعه اینترنت اشیا و 5G ، تعداد فزاینده مجموعه داده های حساس به ویژه برای سیستم اطلاعات مدیریت الکتریکی جمع آوری می شود ، که در آن امنیت انتقال داده ها و به اشتراک گذاری وظیفه اساسی برای عملکرد پایدار کلی سیستم است.

## Blockchain technology

---

بلاکچین در بسیاری از برنامه ها برای بهبود امنیت داده ها مانند IoT اعمال می شود.

از بلاک چین برای مدیریت داده های ابری استفاده می شود.

از بلاکچین و smart contract برای برنامه های حامل داده در محیط اینترنت اشیا استفاده می کنند.

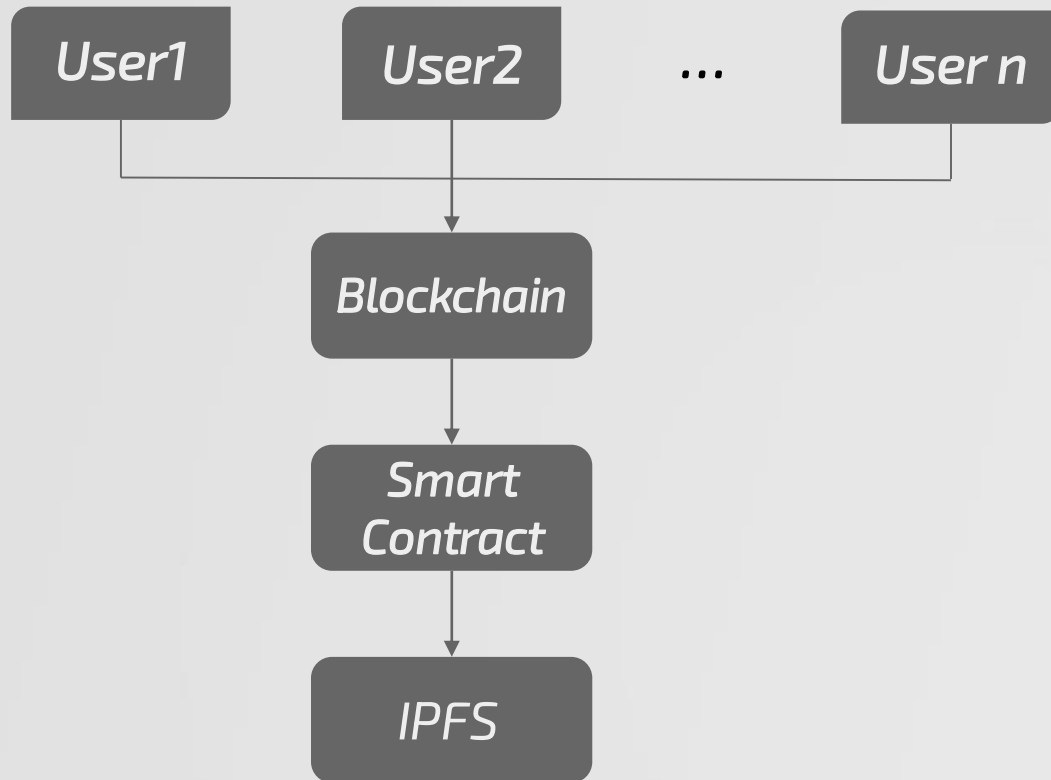
پایگاه داده توسط بلاک چین برای تهیه یکپارچگی و قابلیت اطمینان داده ها بهبود پیدا کرد.



03

*Methodology*

## 3.1. Overall framework



ابتدا داده ها در IPFS ذخیره می شوند که می توانند دسترسی به داده های مورد نیاز را از طریق کد هش تأمین کنند.

همه داده ها رمزگذاری شده اند تا بتوانیم دسترسی آنها را فقط با استفاده از کلید کنترل کنیم ، که می تواند کارایی توزیع داده ها را تسریع کند.

برای انتقال کلید دسترسی داده ها از سیستم بلاکچین استفاده می شود.

علاوه بر این ، داده ها فقط از طریق یک سیستم قرارداد هوشمند متصل به بلاکچین قابل خواندن هستند.

بر اساس اطلاعات موجود در بلاکچین ، می توانیم تجزیه و تحلیل قابلیت دستیابی برای همه داده های سیستم را اجرا کنیم.

## 3.2. Data distribution based on Blockchain

هر کاربر در سیستم پیشنهادی می تواند داده ها را از طریق دیگران ارسال یا دریافت کند. با این حال ، داده ها مستقیماً بین کاربران (به عنوان مثال A و B) منتقل نمی شوند بلکه از طریق سه مرحله زیر انتقال می یابند.

01

داده های حساس ابتدا توسط کاربر A رمزگذاری و در IPFS ذخیره می شوند. همه می توانند داده های رمزگذاری شده را با توجه به کد هش داده ها بارگیری کنند ، اما فقط یکی از کلیدهای موجود قادر به خواندن داده ها است.

02

اگر A بخواهد داده ها را برای B ارسال کند ، او رکوردی در زنجیره بلوک می نویسد که نشان می دهد A داده D را به B ارسال کرده است. این رکورد همچنین حاوی کلید داده D است که توسط کلید عمومی B رمزگذاری شده است ، به طوری که فقط B می تواند کلید را دریافت کند و داده های D را از A بخواند.

03

یک پروتکل Consensus برای اطمینان از عدم انکار رکوردهای انتقال داده انتخاب می شود. در این چارچوب ، پروتکل (PBFT) برای بهبود عملکرد سیستم انتخاب شده است. در مقایسه با PoW or PoS Consensus Protocols که به طور گسترده استفاده می شوند ، PBFT می تواند بدون tokens / coins که در سناریوی مدیریت اطلاعات الکترونیکی ضروری نیست ، اجرا شود.

# کلید ها در بلاک چین؟

## EVERY USER IN THE BITCOIN NETWORK HAS TWO KEYS

Phil



PUBLIC KEY



address that  
everyone in the  
network knows of

PRIVATE KEY

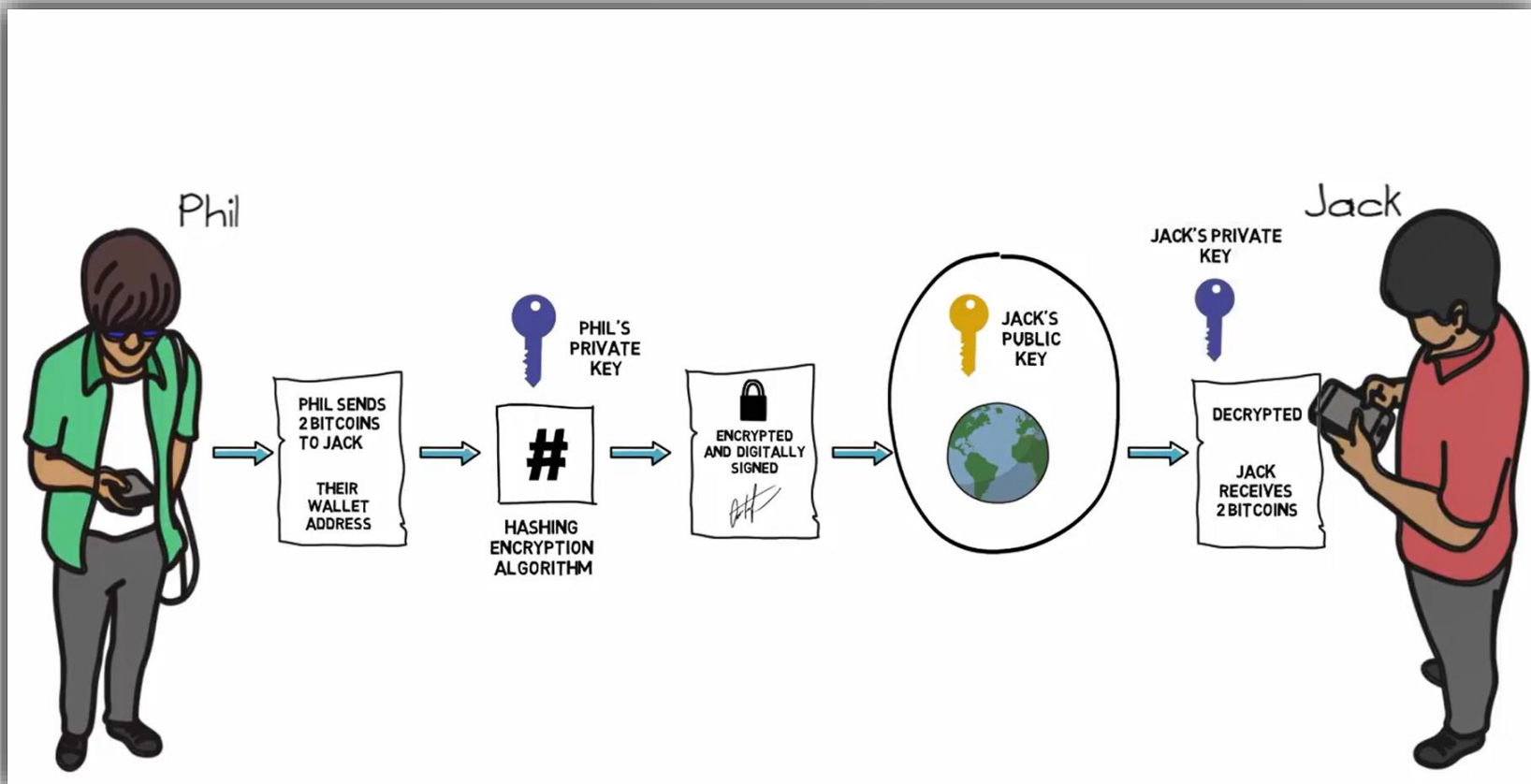


unique address that  
only the user has  
knowledge of

Jack



# کلید ها در بلاک چین؟





## 3.3. Data access with Smart contract

در این مقاله ، ما یک قرارداد هوشمند برای کنترل قابلیت دسترسی به داده های حساس در سیستم مدیریت اطلاعات الکتریکی ایجاد کرده ایم. قرارداد هوشمند پیشنهادی عمدتاً با داده های خوانده شده سروکار دارد ، که عملیاتی نسبتاً ساده است و به راحتی قابل تأیید است. ابتدا همه کاربران در سیستم یک قرارداد هوشمند امضا می کنند که می تواند با خواندن اطلاعات کاربر رکورد تولید کند. این قرارداد هوشمند در بلاکچین ثبت شده و برای هر کاربر در سیستم ارسال می شود. برای کاربر جدید ، او همچنین قرارداد را امضا می کند و قرارداد را به روز می کند.

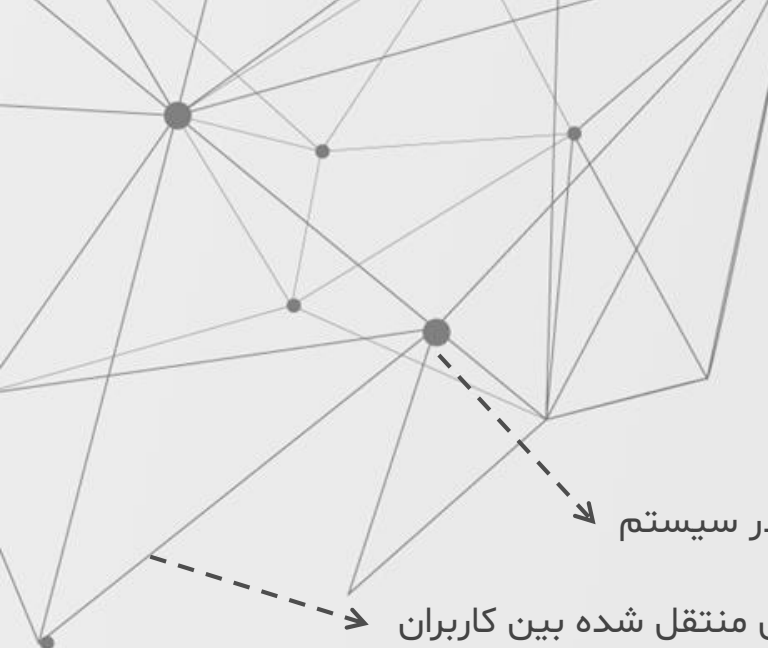


قرارداد هوشمند پروتکلی است که بدون اشخاص ثالث به روشی قابل پیگیری و برگشت ناپذیر قابل انجام است. گرچه قرارداد هوشمند در حدود سال ۱۹۹۷ پیشنهاد شده است ، اما اخیراً براساس فناوری های بلاکچین اجرا شده است که الزامات ایجاد یک کاربرد عملی را پیاده سازی می کند. قرارداد هوشمند به عنوان ویژگی blockchain2.0 نیز شناخته می شود.

وقتی کاربر B داده ها و کلید را از کاربر A دریافت می کند ، B قرارداد هوشمند را برای خواندن داده ها اجرا می کند. قرارداد هوشمند خدمات رمزگذاری و رمزگشایی در سیستم را تأمین می کند ، به عبارت دیگر ما فقط می توانیم داده ها را از طریق قرارداد هوشمند بخوانیم حتی اگر کلید را بدانیم. قرارداد هوشمند تولید شده رمزگشایی داده ها و نوشتن رکورد در زنجیره بلوک نشان می دهد چه زمانی و چه کسی داده ها را می خواند.

مالک یا فرستنده داده همچنین می تواند با به روزرسانی قرارداد هوشمند ، دسترسی به یک مجموعه داده را خاتمه دهد.

## 3.4. Graph based traceability analysis



نماینگر کاربران در سیستم

نماینگر داده های منتقل شده بین کاربران

حاوی ویژگی های مربوط به داده ها ، زمان و اطلاعات دسترسی از گیرنده ها است.

در پایگاه داده گراف:

بلاک چین شامل تمام اطلاعات مربوط به توزیع اطلاعات حساس و دسترسی به سوابق است. با این حال ، اطلاعات در بلوک های مختلف گنجانده شده است که تجزیه و تحلیل و querying دشوار است. در چارچوب پیشنهادی ، ما اطلاعات ردیابی را از بلاکچین استخراج کرده و برای تجزیه و تحلیل بیشتر در پایگاه داده گراف ذخیره می کنیم.

بر اساس نمودار ردیابی -- ما می توانیم به راحتی منابع و اهداف داده را شناسایی کرده و جریان داده را نشان دهیم ، که برای تجزیه و تحلیل و کنترل گسترش داده ها در سیستم مفید است.

سپس ، فاصله بین گره ها و لبه ها بر اساس ویژگی های آنها تعریف می شود. برای کاربردهای مختلف ، ویژگی های گره ها و لبه ها متفاوت است و باید فاصله ها را بر این اساس تنظیم کرد. بعد ، فاصله کلی بین دو نمودار را می توان با الگوریتم های تشابه نمودار مانند Distance'Nested Earth Mover s محاسبه کرد. سرانجام ، نمودارهای قابلیت ردیابی را می توان طبقه بندی کرد و نقاط پرت به عنوان نمودارهای غیر عادی تشخیص داده می شوند.

02

کاربرد دیگر برای تجزیه و تحلیل قابلیت ردیابی مبتنی بر نمودار ، تشخیص غیر عادی است. از آنجا که تجارت در سیستم مدیریت اطلاعات الکتریکی معمولاً به صورت دوره ای یا مشابهت با سابقه است ، ما تشخیص غیر طبیعی را براساس محاسبه تشابه نمودار پیاده سازی می کنیم. ابتدا ، برای هر مجموعه داده ، یک نمودار قابل ردیابی از پایگاه داده نمودار ایجاد می شود.

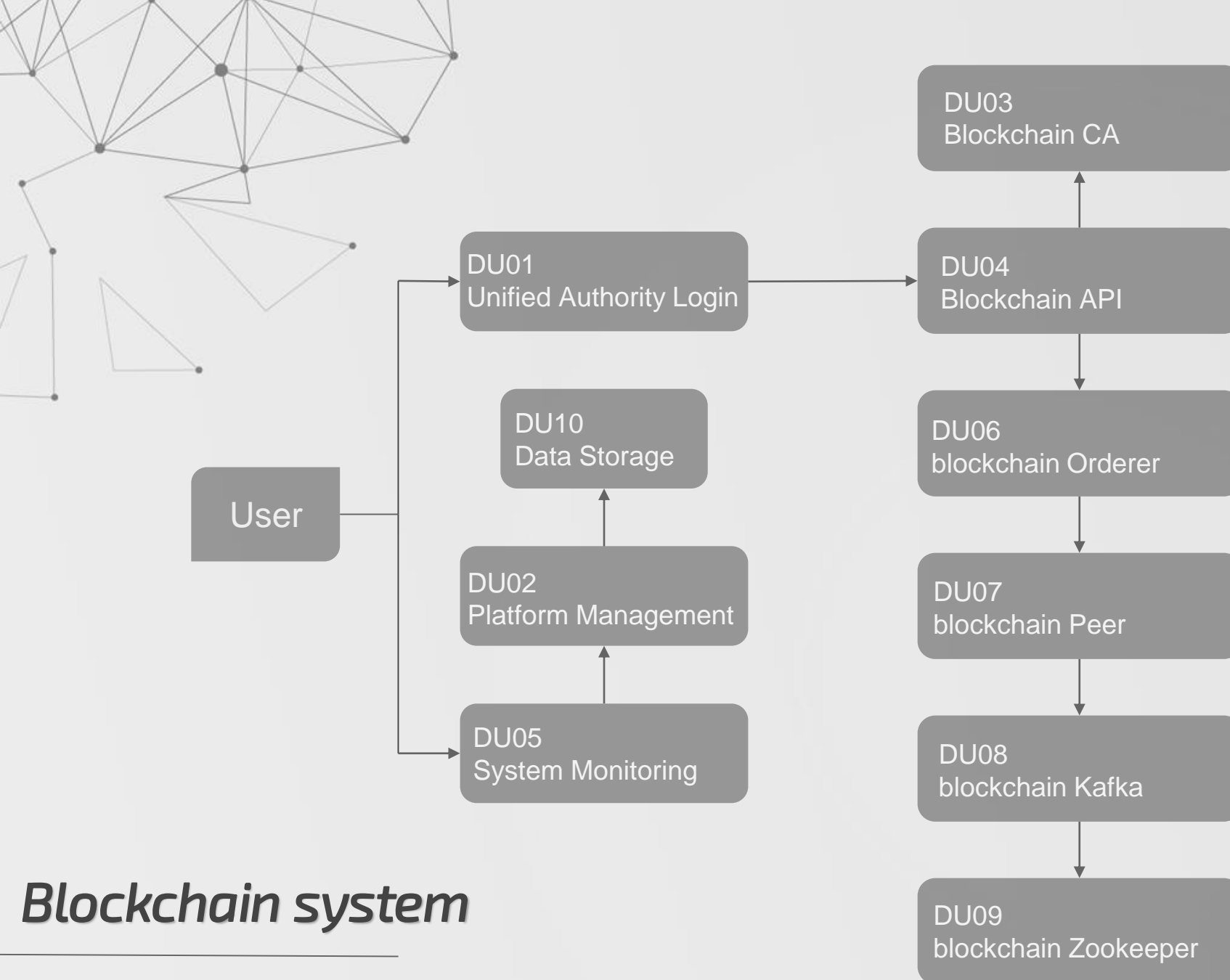
01

# 04

---

## *Implementation and Results*





برای اجرای سیستم پیشنهادی توزیع و ردیابی داده ها ، ما ده واحد استقرار (DU) در اینترنت شرکت مستقر در چهار مکان فیزیک ایجاد می کنیم.

این DU ها روی ماشین های مجازی با ۸ هسته ۲.۶GHz ، حافظه ۱۶G ، ۵۰۰G دیسک و ۲ اتصال شبکه ۱۰۰۰M در حال اجرا هستند. واحد ذخیره سازی داده های DU10 حاوی فضای دیسک ۱۶T اضافی است. تمام DU ها با CentOS 7.0 پیکربندی شده اند ، MySQL به عنوان پایگاه داده و WEBLOGIC 10g به عنوان سرور برنامه استفاده می شود.

چارچوب پیشنهادی براساس Ethereum اجرا می شود که رابطی را برای ادغام بلاچین و قرارداد هوشمند در سیستم فراهم می کند.

## Blockchain system

Fig. 2. System implementation framework



# *System GUI*

---

یک سیستم مبتنی بر وب برای پیکربندی و مدیریت چارچوب توزیع داده مبتنی بر بلاکچین پیاده سازی شده است. ما می توانیم داده ها را بارگذاری کرده و داده ها را در سیستم بارگیری کنیم.

# 05

---

## *Conclusions*





## Conclusions

---

در این مقاله ، ما یک سیستم مبتنی بر بلاکچین برای توزیع داده ها و تجزیه و تحلیل ردیابی در سیستم اطلاعات مدیریت برق پیاده سازی کردیم. چارچوب پیشنهادی از مزایای بلاکچین و قرارداد هوشمند برای اطمینان از امنیت اشتراک داده در سیستم استفاده می کند. سیستم آزمایشی اجرا شده کارایی چارچوب پیشنهادی را تأیید می کند.

---



# *References*

- [1] Blockchain based Data Distribution and Traceability Framework in the Electric Information Management System, Mengchen Cai\*, Ming Li, Wanwan Cao, ITQM 2019
- [2] [https://youtu.be/SSo\\_ElwHSd4](https://youtu.be/SSo_ElwHSd4)
- [3] <https://youtu.be/yubzJw0uiE4>
- [4] Mahnameh Shabakeh 204





***Any Questions?***

***Thanks For Your Attention***

