Privacy Preservation in Patient Information Exchange Systems Based on Blockchain: System Design Study

حفظ حریم خصوصی در سیستم های تبادل اطلاعات بیمار بر اساس بلاک چین: مطالعه طراحی سیستم

سید احمد هاشمی

ژورنال کلاب

۱۴۰۲/۰۳/۲۲

مشخصات ژورنال

Name : Journal of Medical Internet Research

Indexing : ISI , PubMed , Scopus , DOAJ

Impact factor: 7.08 (2021)

Category : Health Informatics Q1

فهرست مطالب

فهرست مطالب

مقدمه و بیان مسئله

مقدمه و بیان مسئله

- پیشرفت روز افزون صنعت پزشکی
- افزایش تقاضا برای داده
- نیاز به تغذیه یکپارچه داده های پزشکی

مقدمه و بیان مسئله

اشتراک گذاری پرونده الکترونیک
سلامت با بیماران

یکپارچگی و امنیت داده ها

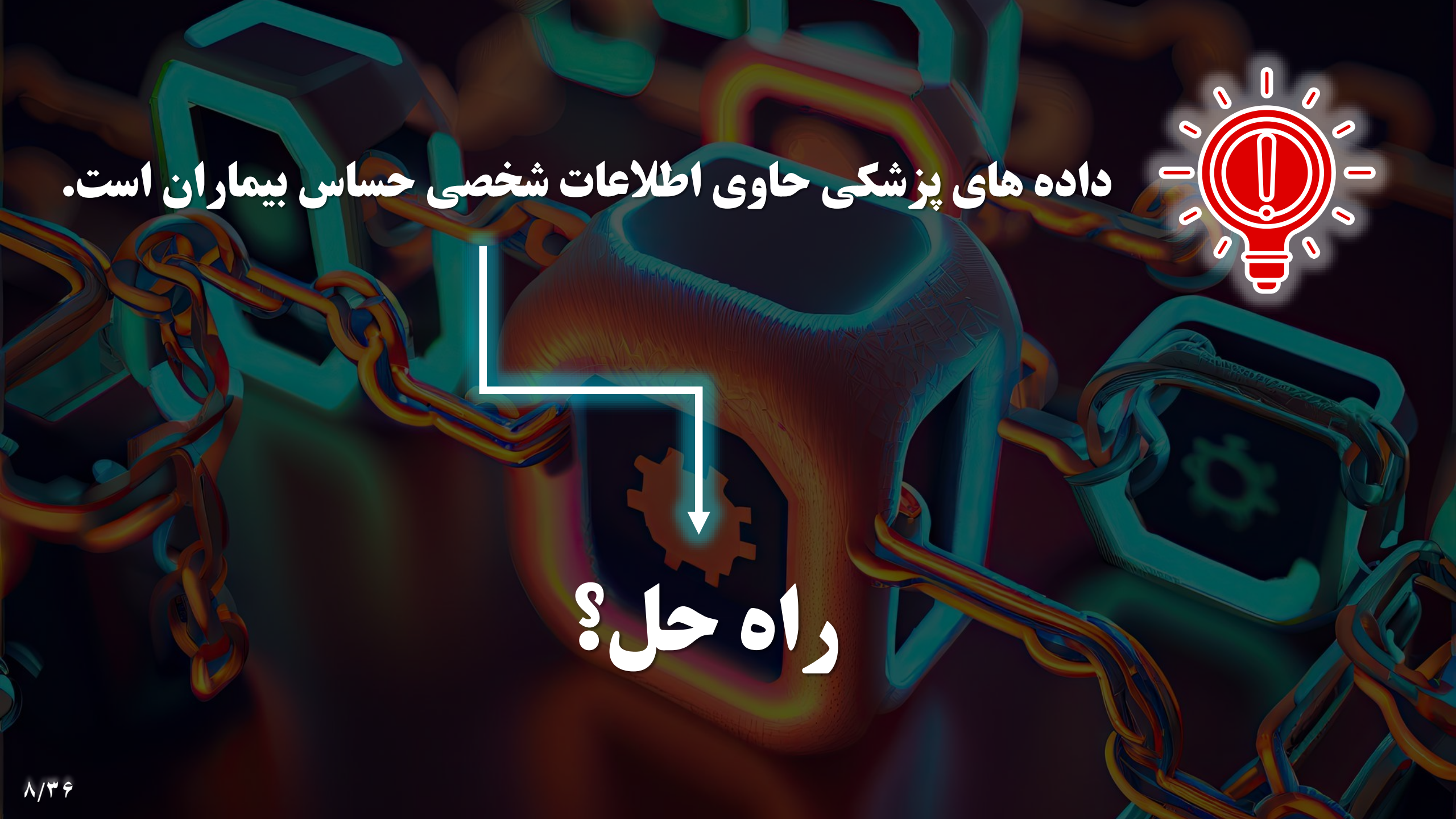
دسترسی شفاف به سوابق پزشکی

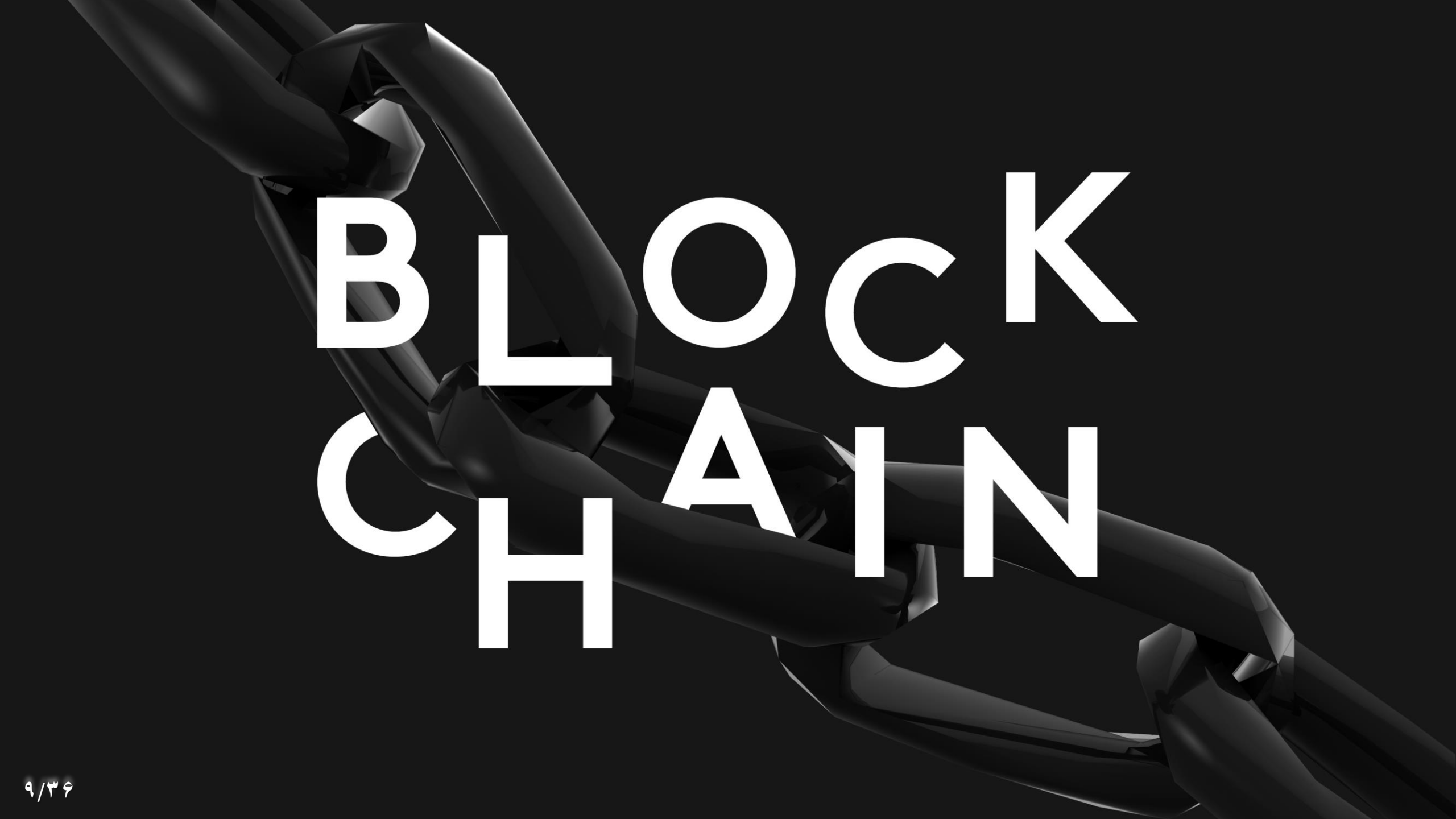
مقدمه و بیان مسئله

سوابق را می توان تغییر داد یا از دست داد

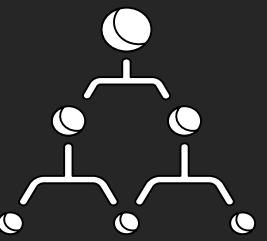
داده ها میتوانند توسط کادر درمان یا بیماران ساختگی یا دستکاری شده که قصد ارتکاب کلاهبرداری را دارد

سیستم فعلی بیمارستان ها مرکزی هست و بسیار آسیب پذیر است

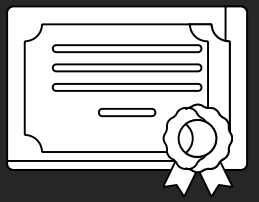

داده های پزشکی حاوی اطلاعات شخصی حساس بیماران است.
راه حل؟


BLOCK
CHAIN

بلاکچین (blockchain)چیست ؟

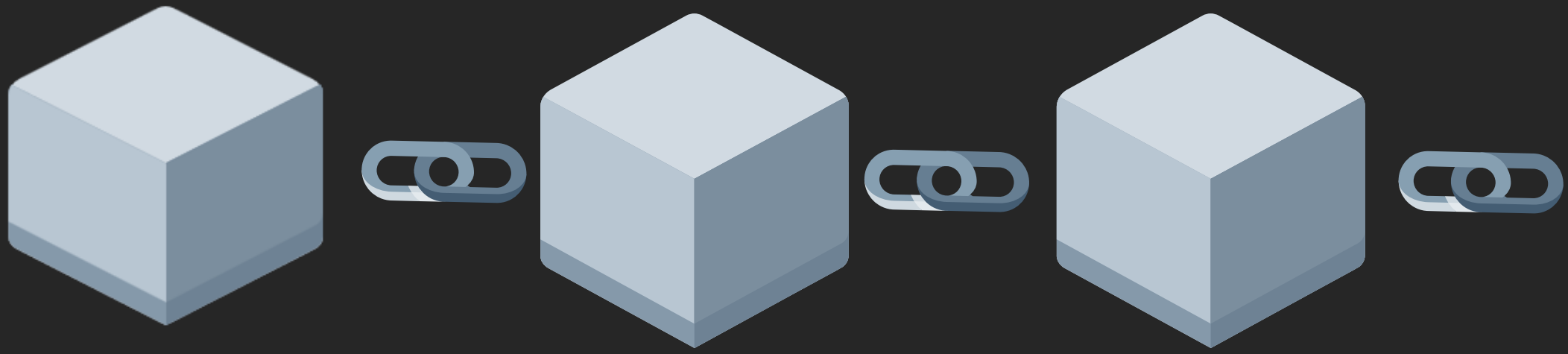


گره های(Node) بلاکچین چیست ؟

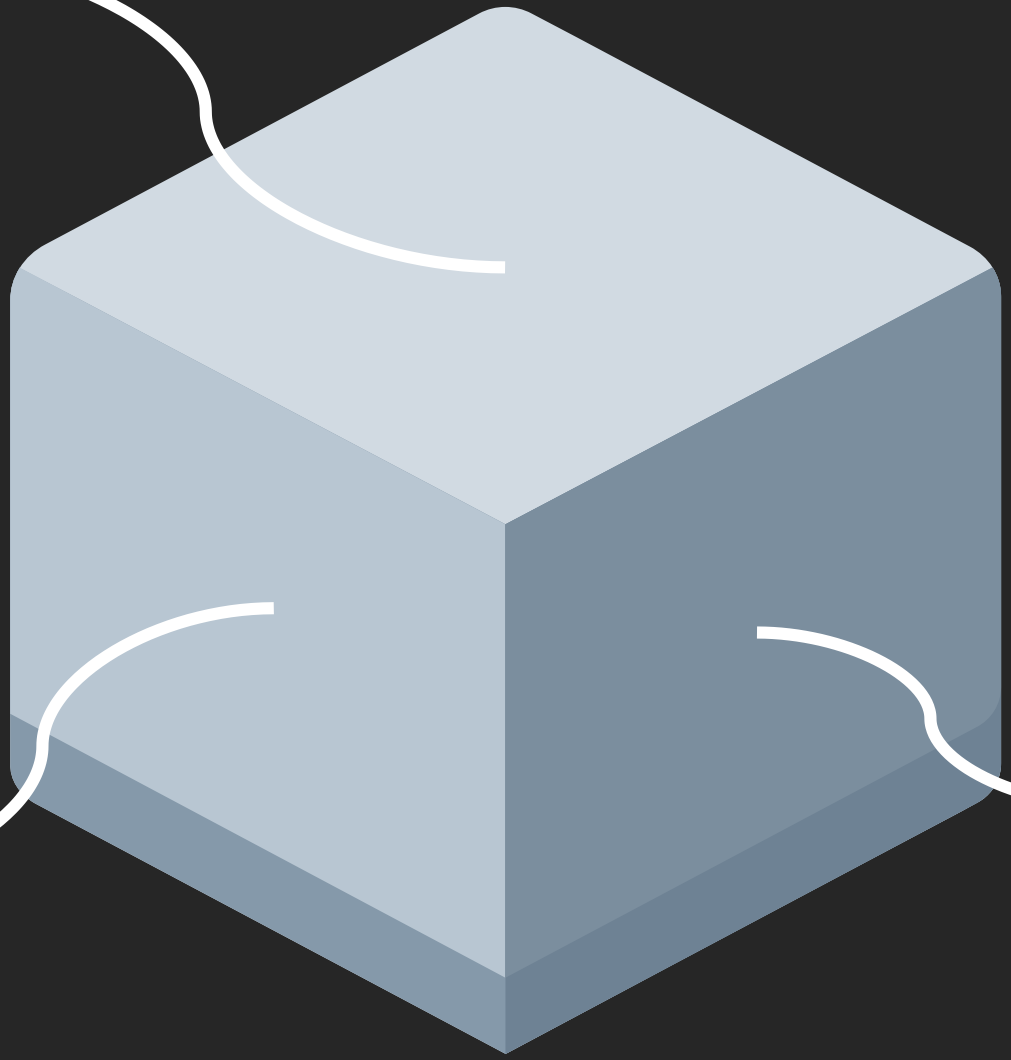


قرارداد هوشمند (Smart Contract)چیست ؟

بلاکچین چیست ؟



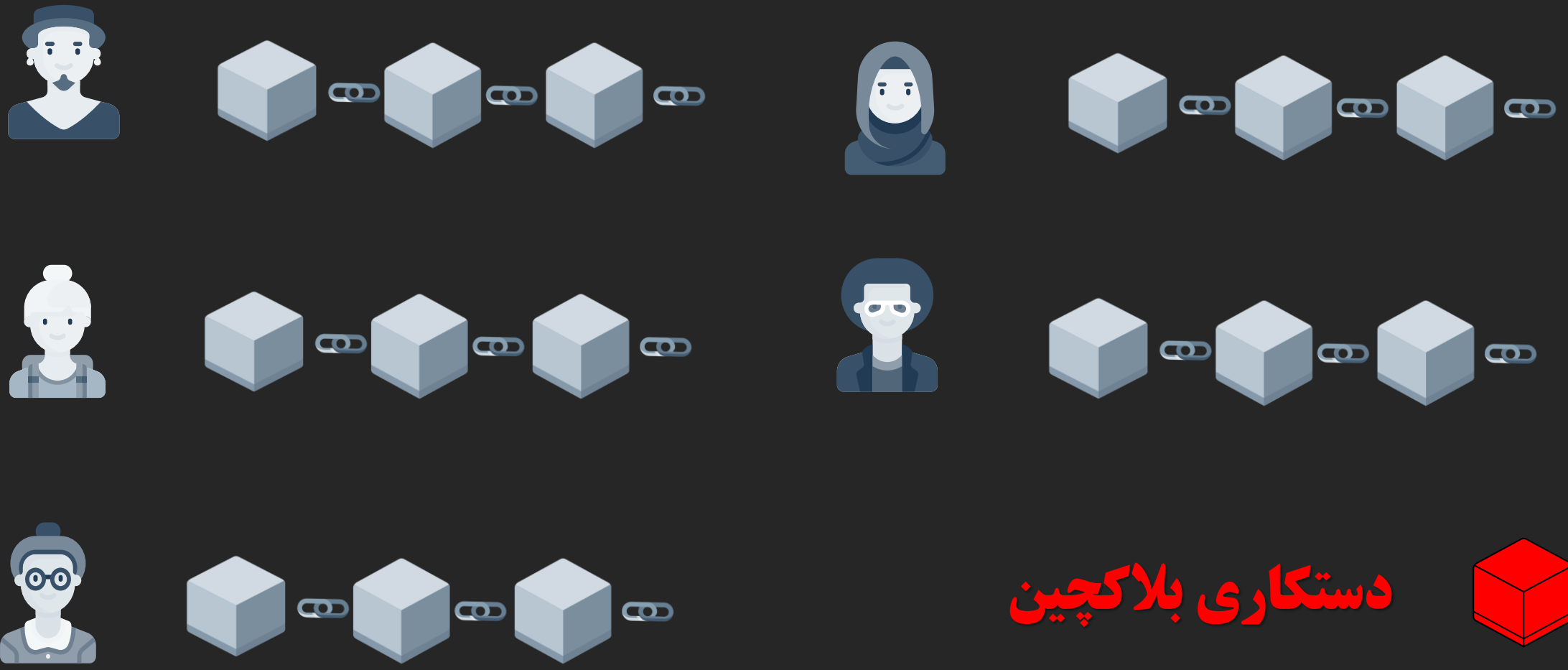
داده ها (Data)



کد هش (Hash)
این بلوک

کد هش (Hash)
بلوک قبلی

گره های(Node) بلاکچین چیست ؟



دستکاری بلاکچین

قرارداد هوشمند (Smart Contract)چیست ؟

یک برنامه کامپیوتری قابل اجرا در بلاکچین است که می‌تواند خودکار، قابل برنامه‌ریزی و قابل اجرا باشد.

مزایا

- شفافیت و کاهش نیاز به واسطه گری
- امنیت بالا
- ذخیره سازی داده ها
- اجرای خودکار
- قابلیت پیشبرد
- انعطاف پذیری

مقایسه سیستم مرکزی و غیر مرکزی در سیستم انتقال (EMR)

Table 1. Comparison of the decentralized (blockchain) and centralized (client–server) electronic medical record–sharing system.

Characteristics	Decentralized system	Centralized system
System-fault tolerance	Strong	Weak
Throughput	Low	High
Latency	High	Low
Data integrity	High	Medium
Trusted third party	No	Yes
Storage	Distributed ledger	Centralized database
Privacy preservation	Strong	Weak

اختصارات و اصطلاحات

پرونده الکترونیک پزشکی(electronic medical record)(EMR)

مرجع صدور گواهینامه (certificate authority) (CA)

سیستم تبادل اطلاعات بیمار (Patient Information Exchange) (PIE)

سیستم فایل توزیع شده (Interplanetary File System) (IPFS)

سیاست دسترسی (Access policy) (AP)

هدف مطالعه

طراحی یک سیستم تبادل اطلاعات غیر متمرکز بیمار
PIE(patient information exchange)

برپایه بلاکچین

با استفاده از تکنیک بازرمز نگاری
(Re-encryption)

قابلیت فروش داده های پزشکی

یکپارچگی EMR ها

اشتراک گذاری امن EMR ها

کاربر محور بودن و دسترسی بیمار

محافظت از حریم خصوصی

روش اجرا

تفاوت دو تکنیک رمزگزاری

کلید بازرمزنگاری(Re-Encryption key)

- به منظور دسترسی به بخشی از اطلاعات (EMR) ها
- امنیت بالاتری را تامین میکند

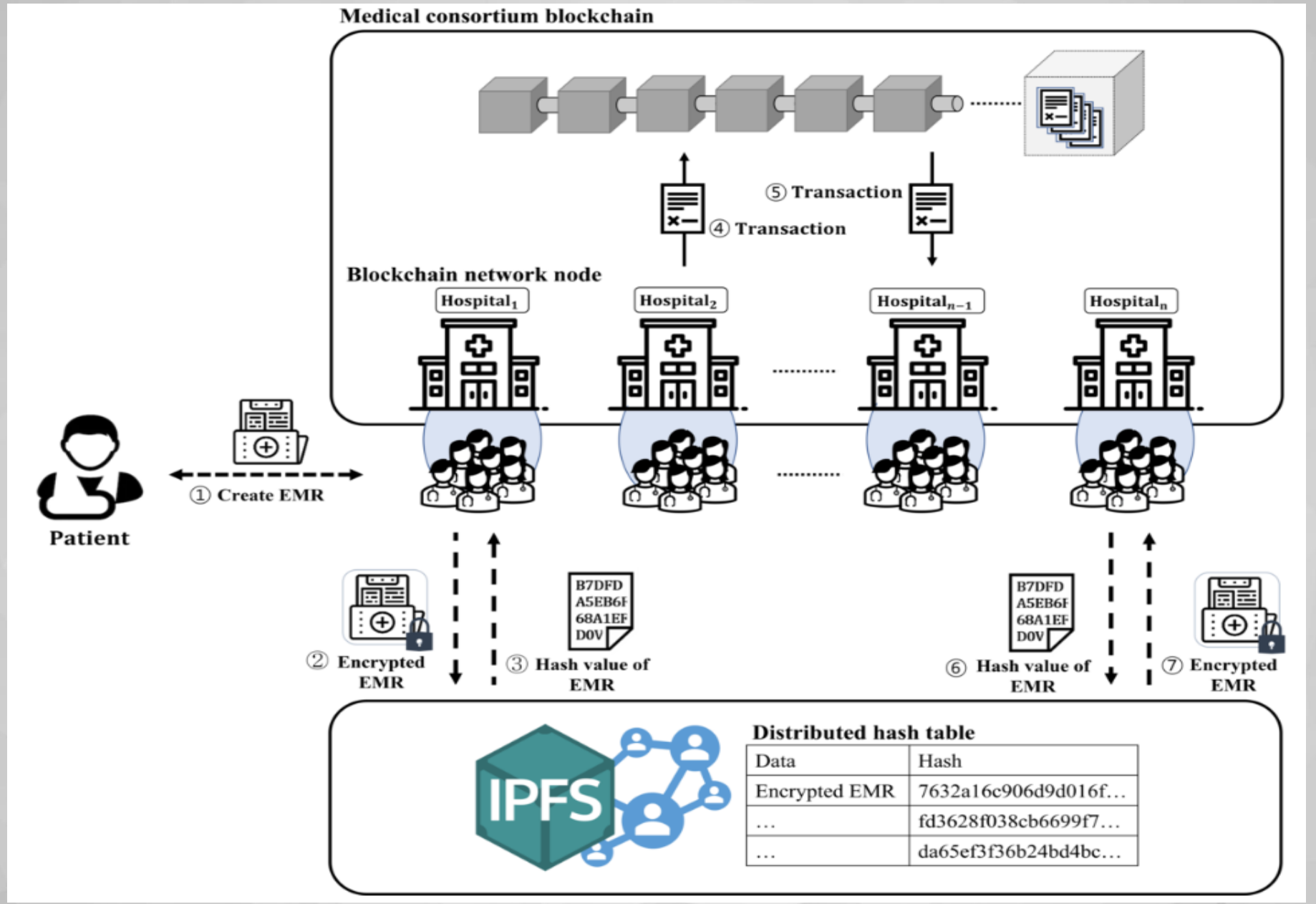
کلید رمزنگاری(Encryption key)

- به عنوان کلید اصلی و خصوصی استفاده میشود
- با استفاده از این کلید میتوان به همه ی اطلاعات موجود در بلاک دسترسی داشت

دسته بندی میزان امنیت لازم برای (EMR)

Table 5. Security levels required depending on the type of information contained in the electronic medical record.

Division and class	Security level
Medical record	
Medical information	Private
Admission record	Private
Prescription	Private
Medical imaging (x-ray, magnetic resonance imaging, and computed tomography)	Private
Clinical trial	
Medical device	Low
Medicine	Low
Clinical observation	Low
Omics (genomics)	Low
Lifelog	
Sensor data (weight, heart rate, and sleep pattern)	Moderate


Medical consortium blockchain
⑤ Transaction
④ Transaction
Blockchain network node
Hospital$_1$
Hospital$_2$
Hospital$_{n-1}$
Hospital$_n$
Patient
① Create EMR
② Encrypted EMR
③ Hash value of EMR
B7DFD
A5EB6F
68A1EF
D0V
⑥ Hash value of EMR
⑦ Encrypted EMR
IPFS
Distributed hash table
Data
Hash
Encrypted EMR
7632a16c906d9d016f…
…
fd3628f038cb6699f7…
…
da65ef3f36b24bd4bc…

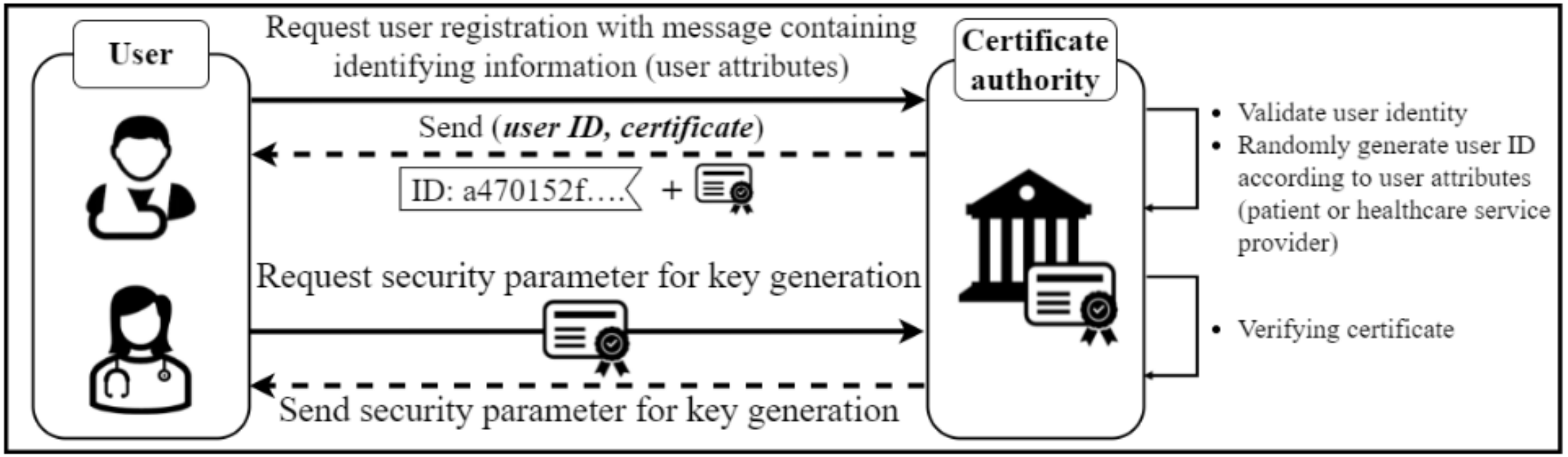
روش اجرا

این مطالعه شامل سه فاز بود:

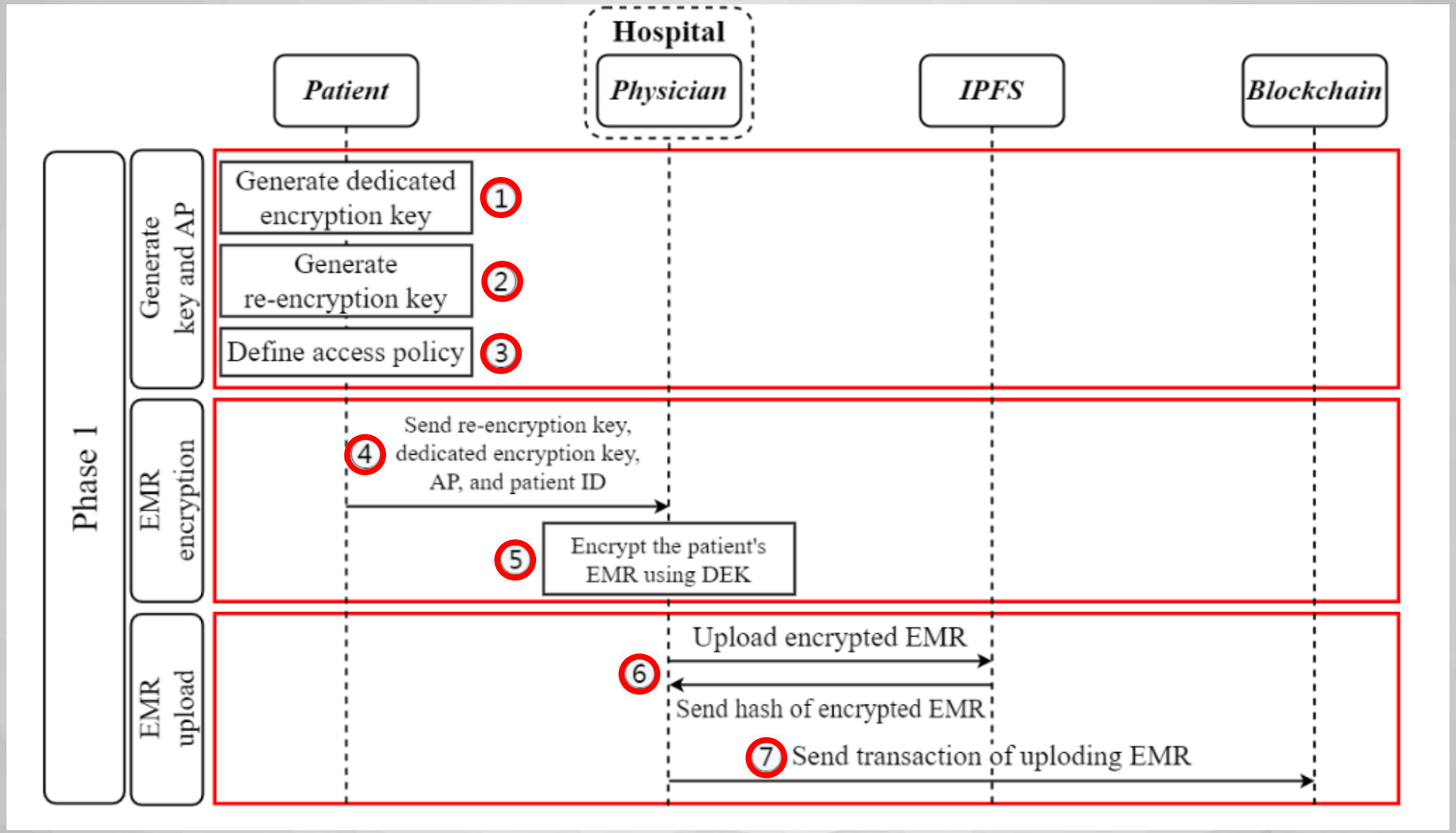
- فاز ابتدایی : ثبت نام کاربر
- فاز یک : آپلود EMR – تولید بلوک
- فاز دو : اشتراک گذاری EMR

فاز ابتدایی : ثبت نام کاربر

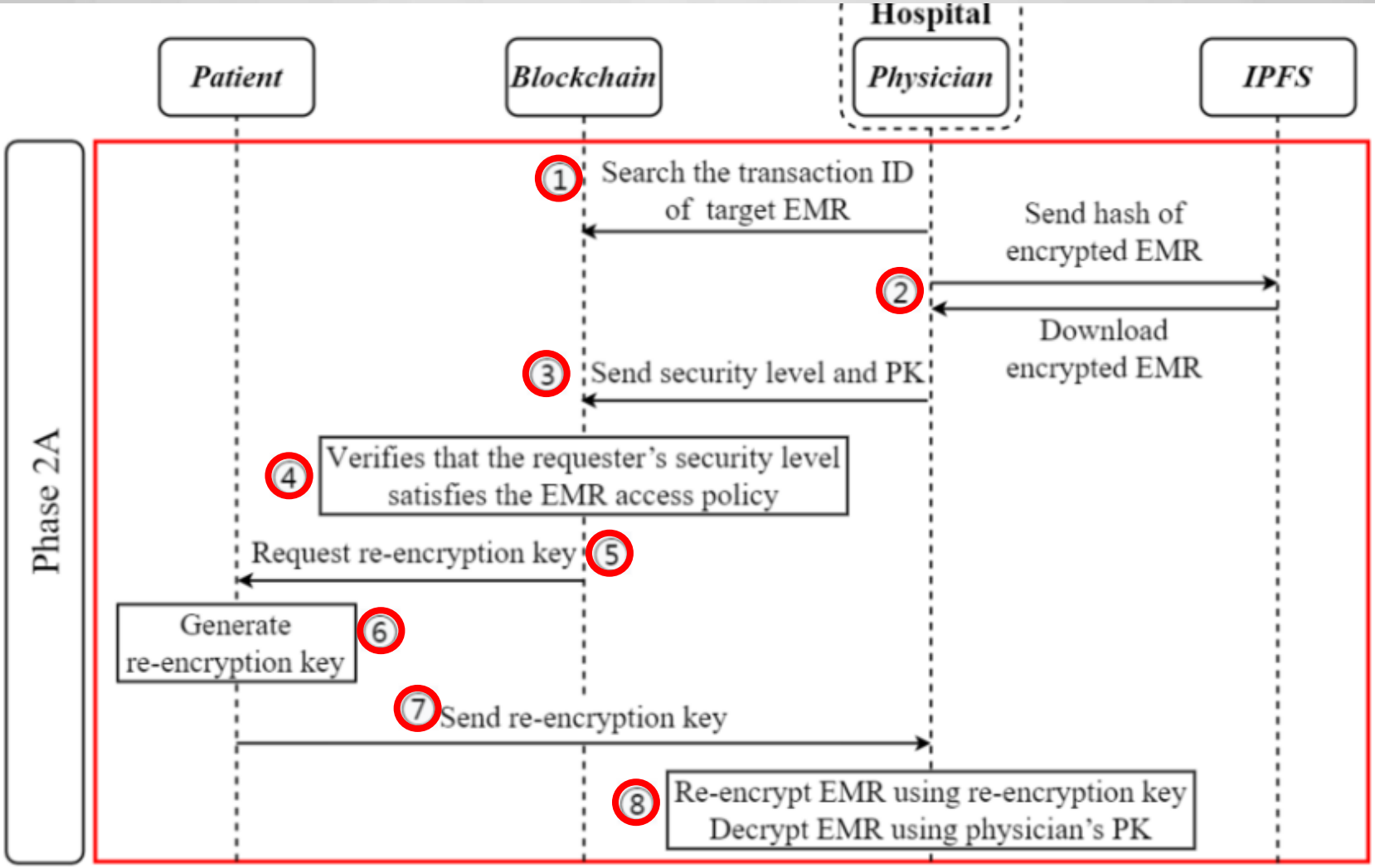
Figure 3. Initial phase: the user registration process to participate in the blockchain network.



فاز اول : آپلود EMR– تولید بلوک

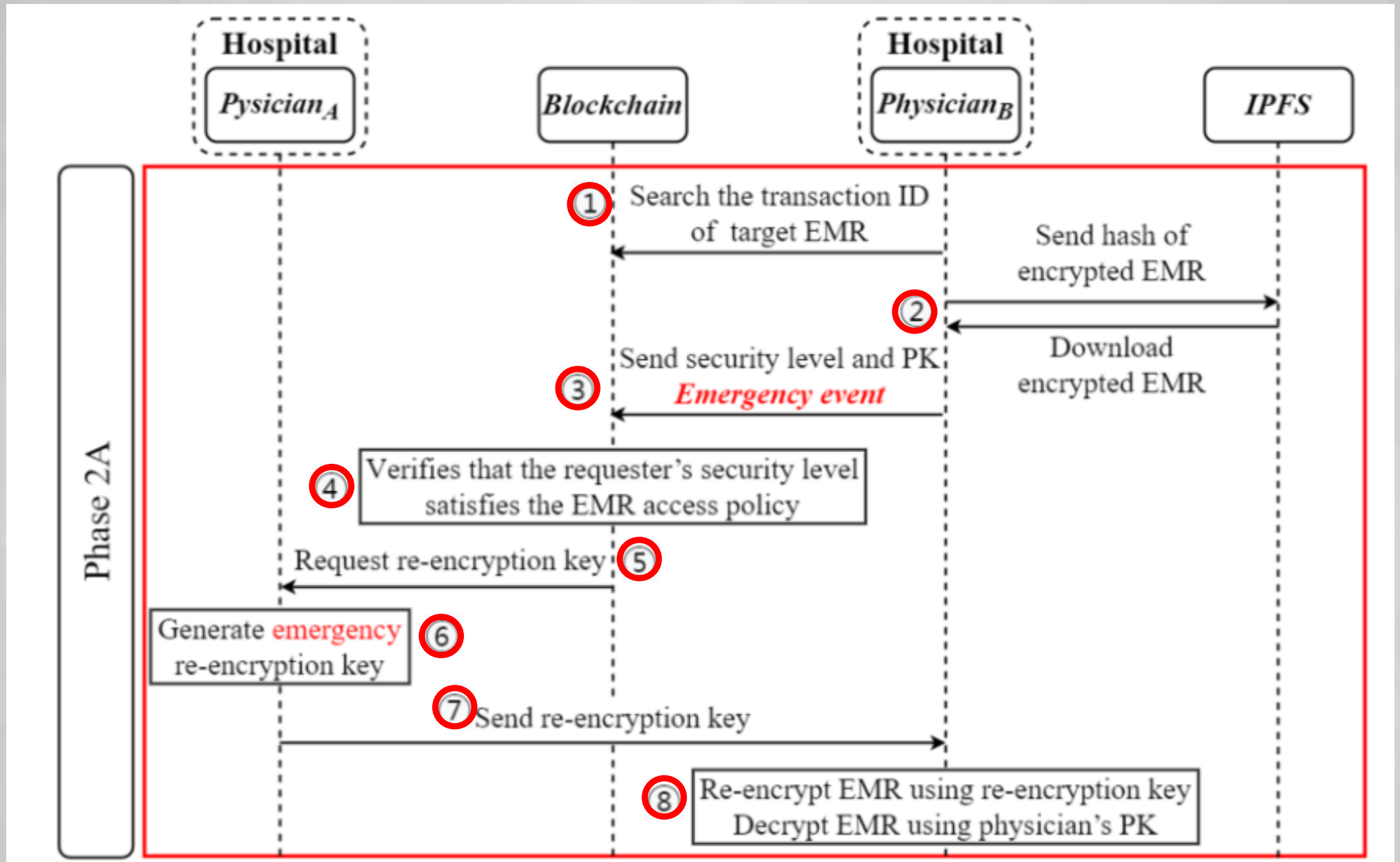


فاز دوم : اشتراک گذاری A – EMR



(A) EMR-sharing process in the general case where the patient controls the re-encryption key

فاز دوم : اشتراک گذاری B – EMR



(B) EMR-sharing process in emergencies where the patient has no control over the re-encryption key

نتایج

شبیه سازی:

۲ پزشک

یک بیمار

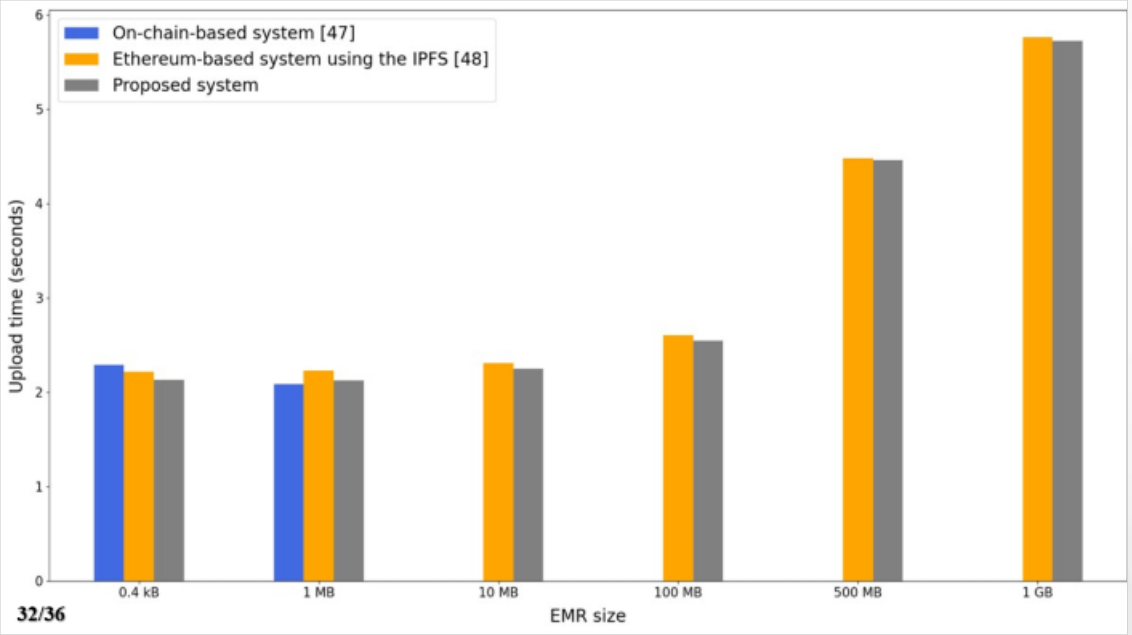
یک کنسرسیوم پزشکی

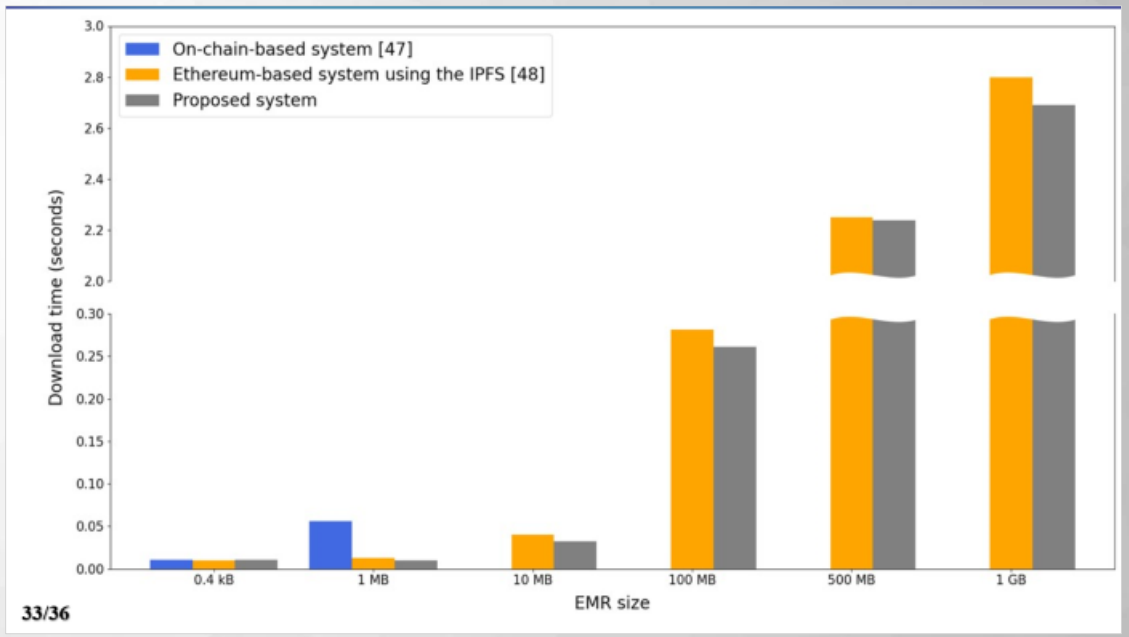
یک شبکه عمومی IPFS

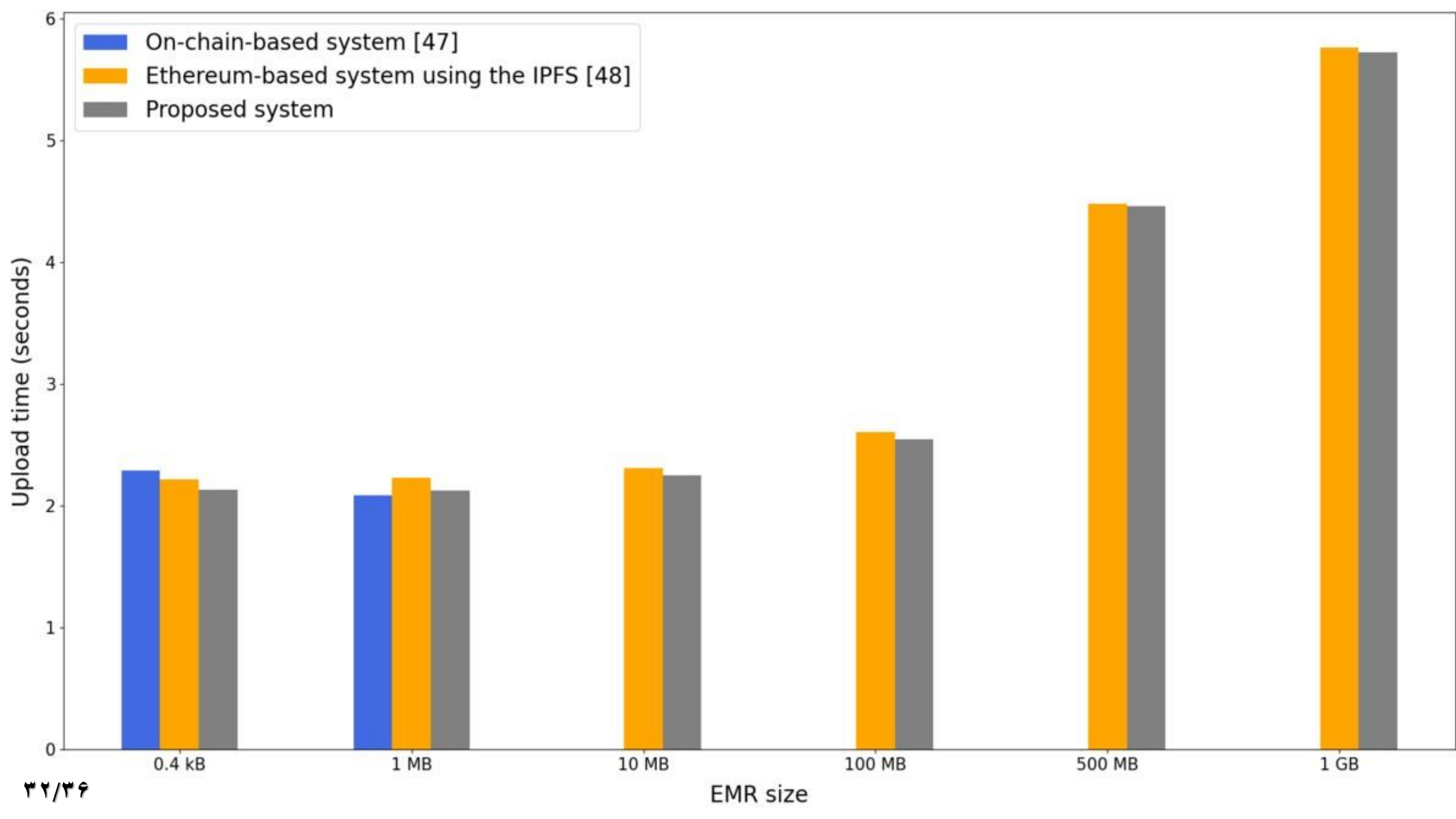
نتایج

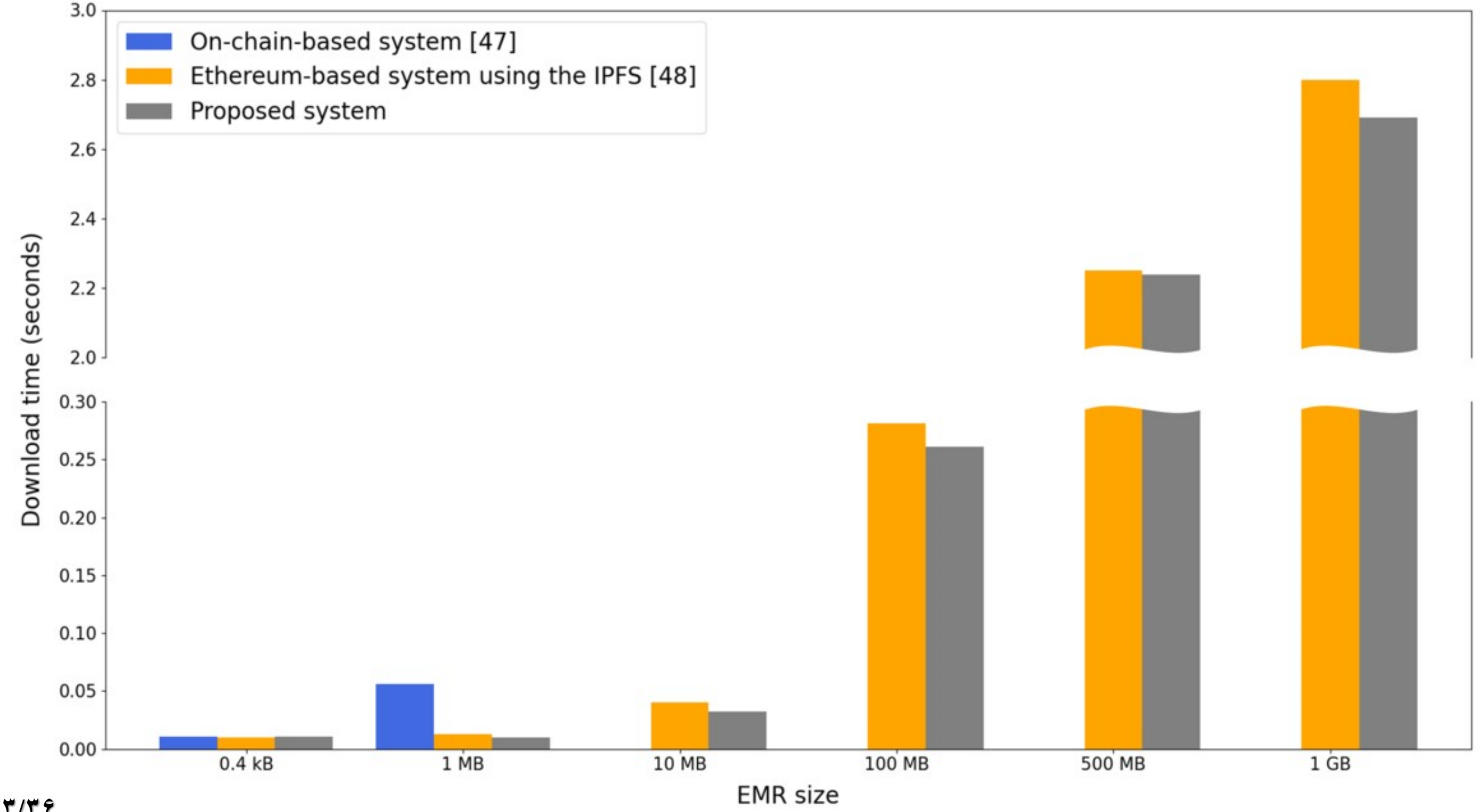
مقایسه با سه سیستم مبتنی بر بلاکچین

سرعت آپلود و دانلود:






On-chain-based system [47]
Ethereum-based system using the IPFS [48]
Proposed system
Upload time (seconds)
0
1
2
3
4
5
6
0.4 kB
1 MB
10 MB
100 MB
500 MB
1 GB
EMR size


On-chain-based system [47]
Ethereum-based system using the IPFS [48]
Proposed system
Download time (seconds)
3.0
2.8
2.6
2.4
2.2
2.0
0.30
0.25
0.20
0.15
0.10
0.05
0.00
0.4 kB
1 MB
10 MB
100 MB
500 MB
1 GB
EMR size

نقاط قوت و ضعف

۱ حفظ حریم خصوصی قوی

۲ سرعت کمتر نسبت به سیستم غیر متمرکز

۳ یکپارچگی داده

۴ خطر و تعداد تغییرات اسناد

۵ امنیت شبکه

پیشنهاد مطالعات آینده و دیدگاه من

استفاده از سازوکاری مانند لایه دوم شبکه اتریوم

ممنون از توجه شما