

BlockChain in IoT

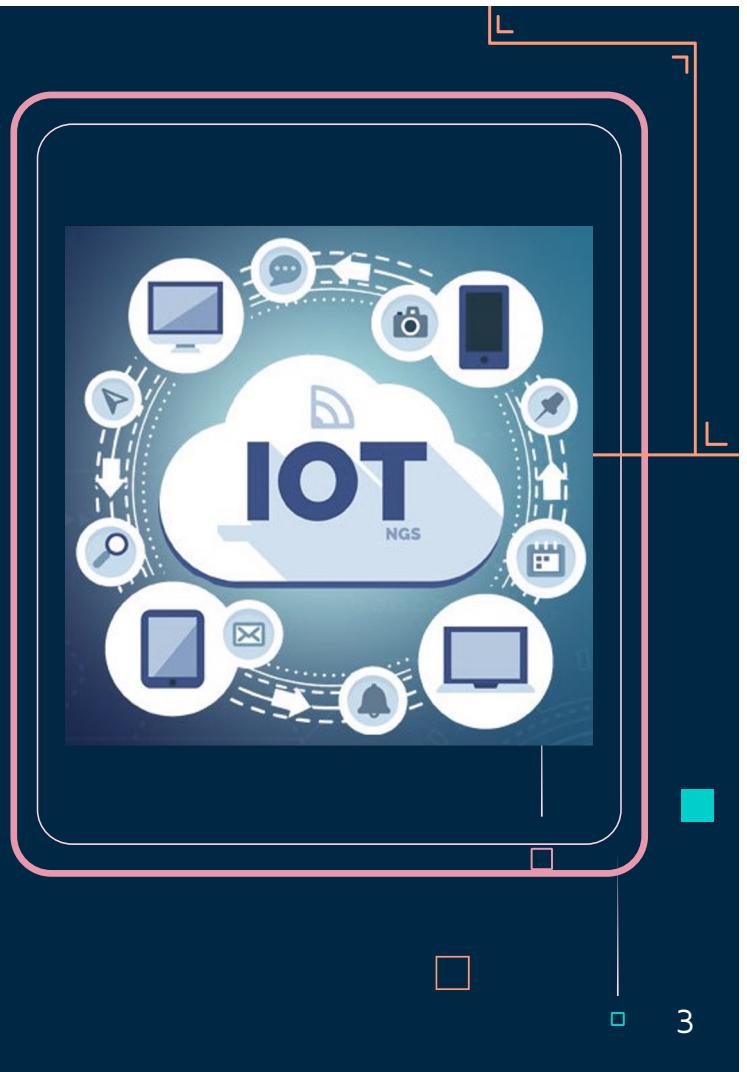
Rasoul Bousaeedi
Ali Ahangarpour
Hanie Solaty Nia
Sobhan Karimi
Mahdi Alipour

Internet of things

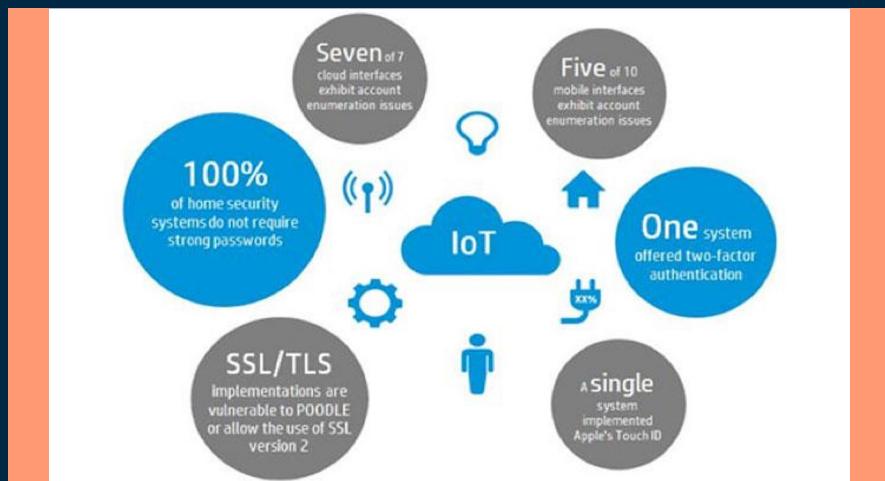
01

اینترنت اشیا

- شبکه‌ای جهانی از سیستم‌ها و دستگاه‌های متصل به یکدیگر
- ارزش اصلی: ارتقا سطح زندگی افراد و کمک به صاحبان کسب‌وکارها
- دلایل حرکت به سمت اینترنت اشیا
 - نیاز به نوآوری و تغییر
- در نظر گرفتن چالش‌ها و فرصت‌ها جهت بهینه‌سازی cost-benefit



چالش‌های اینترنت اشیا



شكل ۱. مثال‌هایی از امنیت نامناسب دستگاه‌های اینترنت اشیا

- حجم عظیمی از داده‌های ناهمگون

- مراجعه اجباری شرکت‌ها به مراکز داده

- نیاز مراکز داده به بهبد زمان پاسخگویی و پردازش

- چالش‌های اصلی اینترنت اشیا

- مدیریت داده

- داده‌کاوی

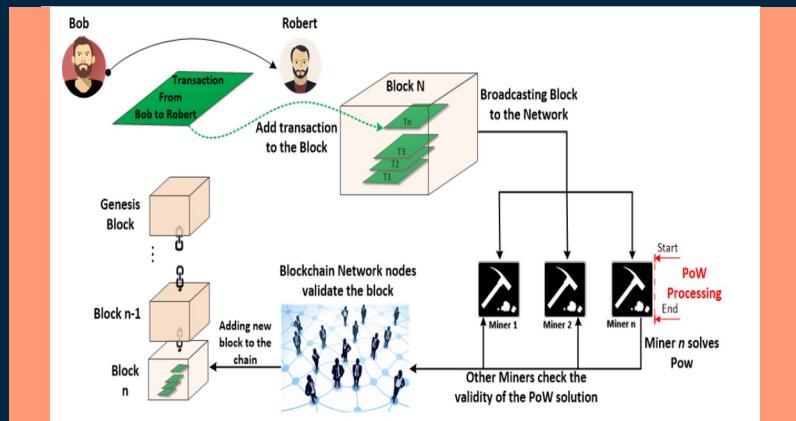
- امنیت و حریم خصوصی

- هرج و مرج

Blockchain

02

بلاک چین



شکل ۲. اعتبارسنجی بلاک‌های تراکنش و روند اضافه‌شدن بلاک

- زنجیره‌ای از بلاک‌ها به مانند یک لینک لیست
- سه قسمت اصلی هر بلاک :

data	○
current block hash	○
previous block hash	○

- چالش جدی بلاک‌چین: نفوذهای گسترده برای چندین بلاک متوالی
- راهکار: الگوریتم‌های اجماعی مانند PoS، PoW

بلاک چین (ادامه)

Proof of Work

- تایید شدن هر کدام از بلاک‌های ورودی به شبکه توسط تمام ماینرها
- هدف اصلی mining: اجازه دادن به نودهای سیستم برای دستیابی به یک اجماع امن و مقاوم
- پرداخت کارمزد تراکنش و مقدار مشخصی از کوین‌های تازه ایجاد شده به ماینرها در هنگام تایید شدن یک بلاک
- سازگاری سیستم به طور خودکار با تمام قدرت mining شبکه و ثابت نگهداشتن آن تا مدتی معین
- تنظیم میزان دشواری، PoW پس از مقدار مشخصی از بلاک‌ها براساس عملکرد شبکه
- هدف این دو مورد تایید تمام تراکنش‌ها توسط همه نودهای شبکه برای جلوگیری از چالش Double Spending

چالش‌های حوزه بلاکچین

- مقياس‌پذیری: سنجن شدن بلاکچین با افزایش روزانه حجم تراکنش‌ها
 - فضا برای ذخیره همه تراکنش‌ها، محدودیت اصلی ظرفیت بلاک، زمان مورد نیاز برای تولید بلاک جدید
- نشت حریم خصوصی: تراکنش با آدرس‌ها و نه هویت واقعی → اعتقاد عموم بر این بودن بلاکچین
 - تضمین نشدن حریم خصوصی تراکنش‌ها در بلاکچین
- استخراج خودخواهانه: بلاکچین در معرض حملات ماینرهای خودخواه تبادل‌گر
 - آسیب‌پذیری شبکه در برابر حملات
- استراتژی خودخواهانه طولانی‌تر شدن شاخه خصوصی از شاخه‌های عمومی فعلی و معتبر شدن آنها

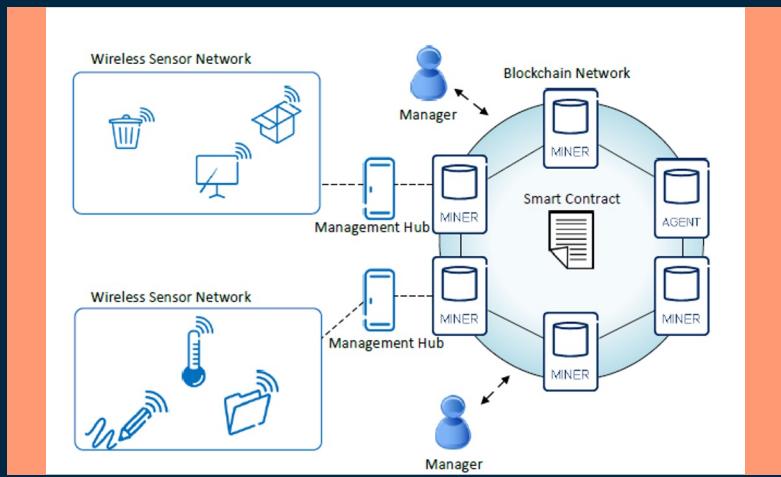
مقالات پیشنهادی

03

■ حركت به سمت بلاکچين بهينه سازی شده برای اينترنت اشيا

- افزایش علاقه عمومی برای پذیرش بلاکچین در اینترنت اشیا برای حفظ امنیت و حریم خصوصی
- چالش بزرگ: گران بودن بلاکچین از نظر محاسباتی و داشتن overhead های پهنای باند و تاخیر بالا
- راهکار: ایجاد یک معماری سبک وزن مبتنی بر بلاکچین
- استفاده دستگاههای اینترنت اشیا از یک ledger خصوصی غیرقابل تغییر و مدیریت آن به صورت مرکزی
- استفاده معماري پيشنهادي، از اعتماد توزيع شده برای کاهش زمان پردازش اعتبار بلاکها
- کاهش قابل توجه overhead پکت و پردازش در اين روش در مقایسه با اجرای بلاکچین در بيتكوين در بررسیها

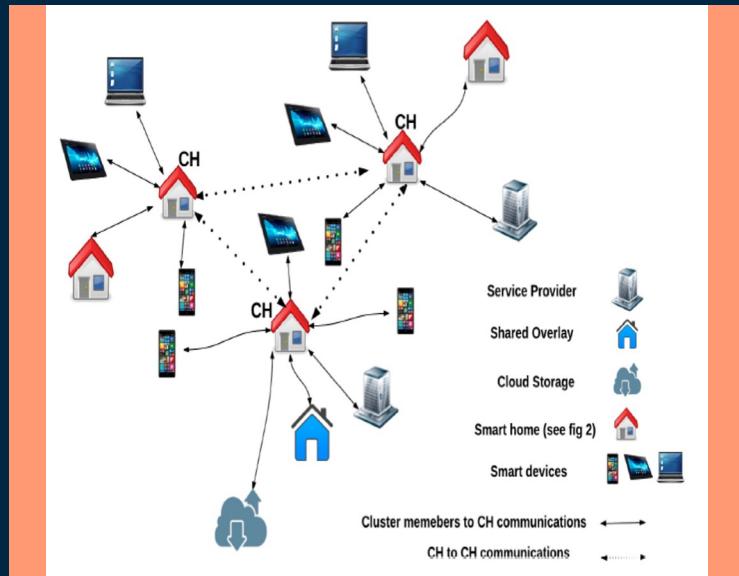
معماری برای مدیریت مقیاس پذیر دسترسی در اینترنت اشیا



شکل ۳. سیستم کنترل دسترسی غیر متمرکز

- خروج اینترنت اشیا از مراحل اولیه خود و رسیدن به بلوغ کامل
- چالش بزرگ استقرار میلیاردها دستگاه در سراسر جهان \leftarrow توانایی مدیریت
- اگرچه فناوری‌های مدیریت دسترسی در اینترنت اشیا وجود دارند؛ اما به دلیل متمرکز بودن، انواعی از محدودیت‌های فنی را بوجود می‌آورند.
- یک سیستم کنترل دسترسی جدید و کاملاً توزیع شده مبتنی بر فناوری بلاک‌چین برای مدیریت نقش‌ها و مجوزها در این معماری
- اساس پیاده سازی این معماری \leftarrow Proof-of-Concept

مجتمع سازی بلاکچین و اینترنت اشیا



شکل ۶. نمایی از معماری مبتنی بر بلاکچین

- اینترنت اشیا: اتصال دستگاه‌های هوشمند به هم برای جمع‌آوری داده‌ها و تصمیم‌گیری هوشمندانه
- چالش بزرگ: فقدان اقدامات امنیتی ذاتی در برابر تهدیدات
- راهکار: استفاده از بلاکچین با پارامتر "security by design" برای رفع مشکل امنیت قابلیت‌های بلاکچین در این حوزه: تغییرناپذیری، شفافیت، قابلیت حسابرسی، رمزگذاری داده‌ها، انعطاف‌پذیری عملیاتی
- نوآوری این مقاله در حوزه ادغام بلاکچین با اینترنت اشیا :

 - پوشش حوزه‌های کاربری مختلف
 - معرفی دو الگوی استفاده، یعنی دستکاری دستگاه و مدیریت داده
 - گزارش درباره سطح توسعه برخی از راهکارهای ارائه شده

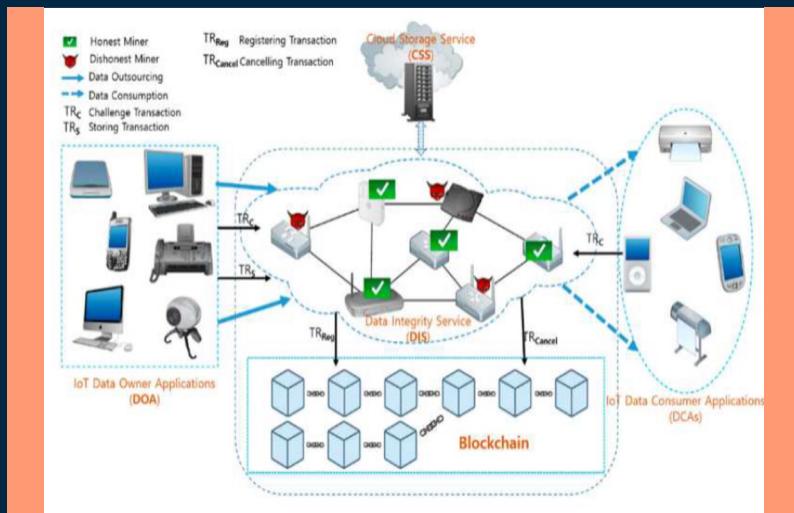
□ بلاکچین برای تامین امنیت و حریم خصوصی اینترنت اشیا

- بررسی یک خانه هوشمند به عنوان مثالی برای چالش اصلی باقیمانده اینترنت اشیا: حفظ امنیت و حریم خصوصی
- دلیل این چالش: ماهیت توزیع شده و مقیاس گسترده دستگاه های اینترنت اشیا
- فراهم شدن امنیت و حریم خصوصی غیر متمرکز در رویکرد استفاده از بلاکچین همراه انرژی، تاخیر و سریار محاسباتی زیاد
- رویکرد در یک خانه هوشمند نمونه همراه با سه لایه :
 - ذخیره سازی ابری
 - پوشش
 - خانه هوشمند
- هر خانه هوشمند مجهز به یک دستگاه همیشه آنلاین و با منابع بالا به نام "ماینر"
- وظیفه ماینر → مدیریت تمام ارتباطات درون و بیرون خانه
- حفظ یک بلاکچین خصوصی و امن توسط ماینر برای کنترل ارتباطات
- این بودن این چارچوب مبتنی بر بلاکچین، از نظر اهداف امنیتی اساسی؛ در برابر هزینه های overhead مختلف بسیار ناچیز

سیستم کنترل دسترسی در اینترنت اشیا با رویکرد مبتنی بر permissioned blockchain

- تولید داده‌های ارزشمند زیاد توسط دستگاه‌های اینترنت اشیا و اشتراک گذاری آنها با طرف‌های خارجی برای خدمات مفید
- مرکزیت بودن سیستم‌های کنترل دسترسی سنتی اینترنت اشیا و عدم شمول همه ذی‌نفعان در فرآیند تصمیم‌گیری کنترل دسترسی
- پیشنهاد سیستم کنترل دسترسی مبتنی بر بلاکچین مجاز برای اینترنت اشیا برای پرکردن این شکاف
- سطوح متفاوتی از کنترل دسترسی مانند ایجاد خط مشی دسترسی و تصمیم‌گیری کنترل دسترسی بر اساس اجماع همه سهامداران در این سیستم
- طراحی و اجرای کنترل دسترسی مبتنی بر ویژگی (ABAC) در یک بلاکچین مجاز به نام Hyperledger fabric برای دقیق‌تر بودن

بهره‌گیری از بلاکچین برای تضمین امنیت در محیط اینترنت اشیا و فضای ابری



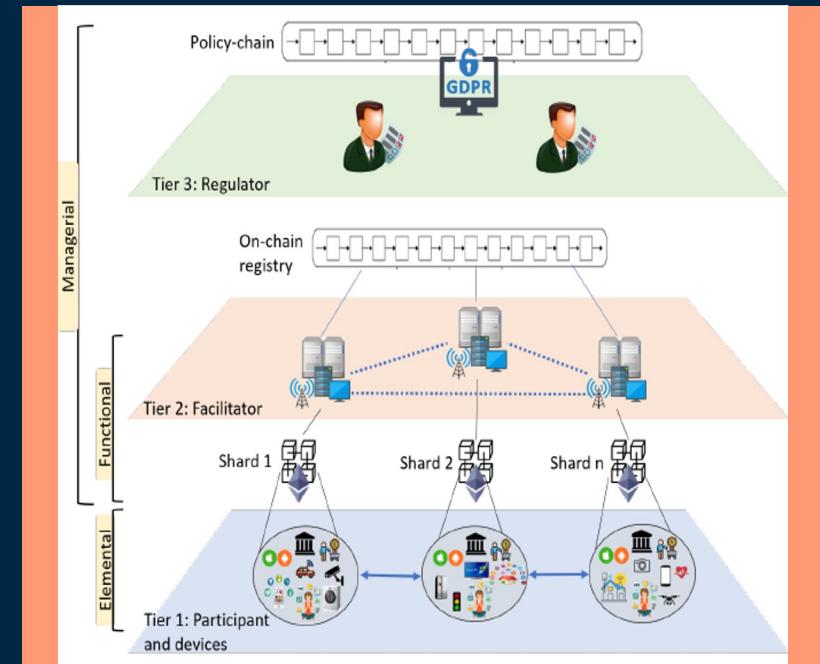
شکل ۵. مثال‌هایی امنیت نامناسب دستگاه‌های اینترنت اشیا

- توسعه سریع فناوری ابری و اینترنت اشیا
- ایجاد نگرانی‌های در مورد امنیت فناوری‌ها، هم‌زمان با پیشرفت آنها
- ارائه راه حل‌های امنیتی با دو هدف بخصوص:
 - حفاظت از تمامیت داده‌ها
 - حفاظت از حریم خصوصی
- استفاده از بلاکچین برای ارائه خدمات امنیتی متنوع
- استفاده از یک معماری سلسله‌مراتبی غیرمت مرکز مبتنی بر ساختار P2P
- افزایش امنیت از طریق:
 - کاهش نقاط آسیب‌پذیری
 - رفع مشکل مت مرکز بودن

حرکت به سمت یک بازار داده تقویت شده با بلاکچین برای اینترنت اشیا

- ایجاد اقتصاد مبتنی بر داده به واسطه‌ی تولید داده‌ی سابقه، توسط اینترنت اشیا
- عدم اشتراک‌گذاری حجم قابل توجهی از داده‌ها توسط کاربران، به دلیل بی‌اعتمادی آنها به امن بودن سیستم فعلی
- نمایان شدن قدرت واقعی اینترنت اشیا با به وجود آمدن یک بازار داده قابل اعتماد
- متمرکز بودن معماری بازارهای داده فعلی، مشکل اصلی آنها
- ایجاد چالش‌های متنوع به خاطر معماری مرکزی مانند تبدیل شدن پلتفرم مرکزی به یک گلگاه، پرهزینه بودن، خطای تک نقطه‌ای، آسیب‌پذیر بودن
- طراحی سخت بازار داده اینترنت اشیا به خاطر ویژگی‌های اینترنت اشیا مانند منابع و قدرت محاسباتی محدود mobility، دستگاه‌ها

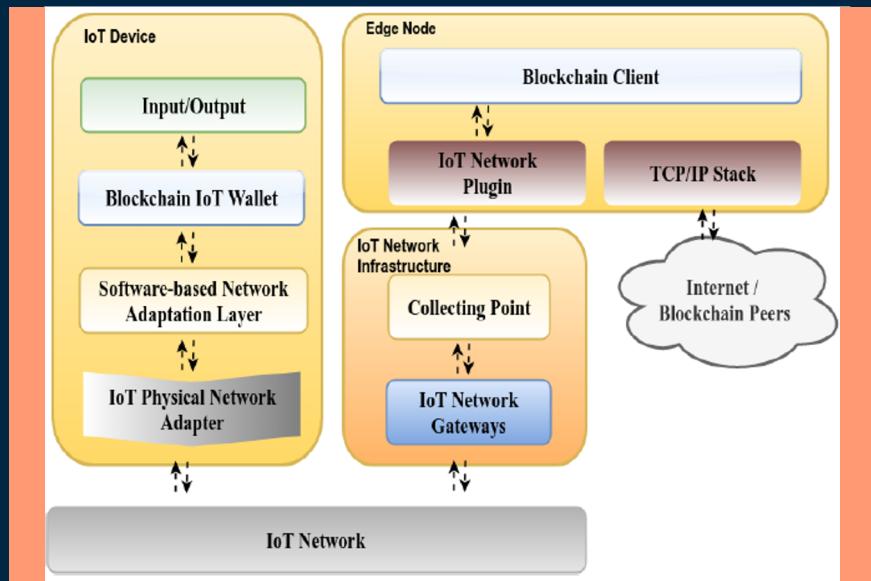
حرکت به سمت یک بازار داده تقویت شده با بلاکچین برای اینترنت اشیا



شکل ۶. معماری سه لایه پیشنهادی

- استفاده از بلاکچین برای طراحی یک بازار داده امن برای اینترنت اشیا
- استفاده از یک معماری سه لایه ایجاد بازار داده امن:
 - لایه پایه
 - لایه عملکردی
 - لایه مدیریتی

استفاده از بلاکچین های مبتنی بر PoS برای جریان های داده اینترنت اشیا



شکل ۷. اعضای معماری لایه‌ای پیشنهادی برای بهبود عملکرد اینترنت اشیا

- نامناسب بودن بلاکچین‌های مبتنی بر PoW
- نرخ تراکنش پایین و استفاده از انرژی بالا

- بلاکچین مبتنی بر Bazo:
- روش‌های Sharding و تجمیع تراکنش‌ها

- استفاده از یک معماری لایه‌ای و مازولار به منظور کارآمدتر کردن تبادل‌های داده‌ها

Edgence یک پلتفرم محاسبه لبه‌ای با قابلیت بلاکچین برای برنامه‌های هوشمند و توزیع شده اینترنت اشیا

- مدیریت مقیاس پذیر شبکه‌های اینترنت اشیا گلوگاه پیشرفت اینترنت اشیا
- دشواری مدیریت به دلایلی از جمله پراکندگی جغرافیایی، مالکیت پراکنده و افزایش روزانه دستگاه‌های اینترنت اشیا
- مدیریت هوشمند برنامه‌های غیر مرکز اینترنت اشیا به کمک Edgence:

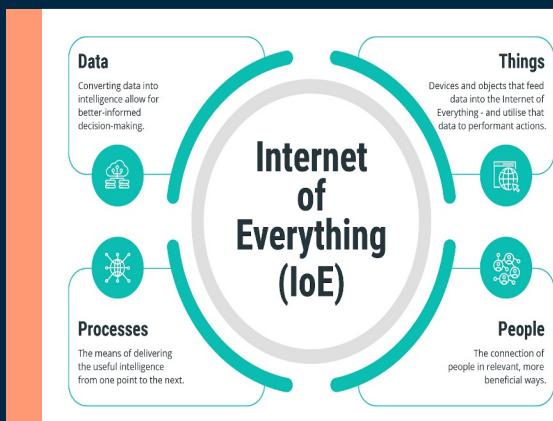
 - استفاده از Edge clouds برای دسترسی به دستگاه‌ها و کاربران اینترنت اشیا
 - استفاده از بلاکچین داخلی خود برای تحقق خودگردانی و نظارت بر خود

- استفاده از فناوری master node به منظور ایجاد ارتباط بین سیستم بلاکچین بسته و دنیای واقعی
- استفاده از سیستم اعتبارسنجی سه لایه‌ای شامل:
 - اعتبارسنجی اسکریپت
 - اعتبارسنجی قرداد هوشمند
 - اعتبار سنجی master node

IOTA

04

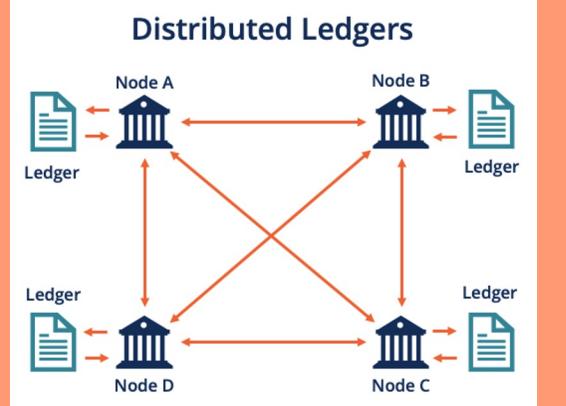
آیوتا چیست؟



. شکل ۱ . IoE

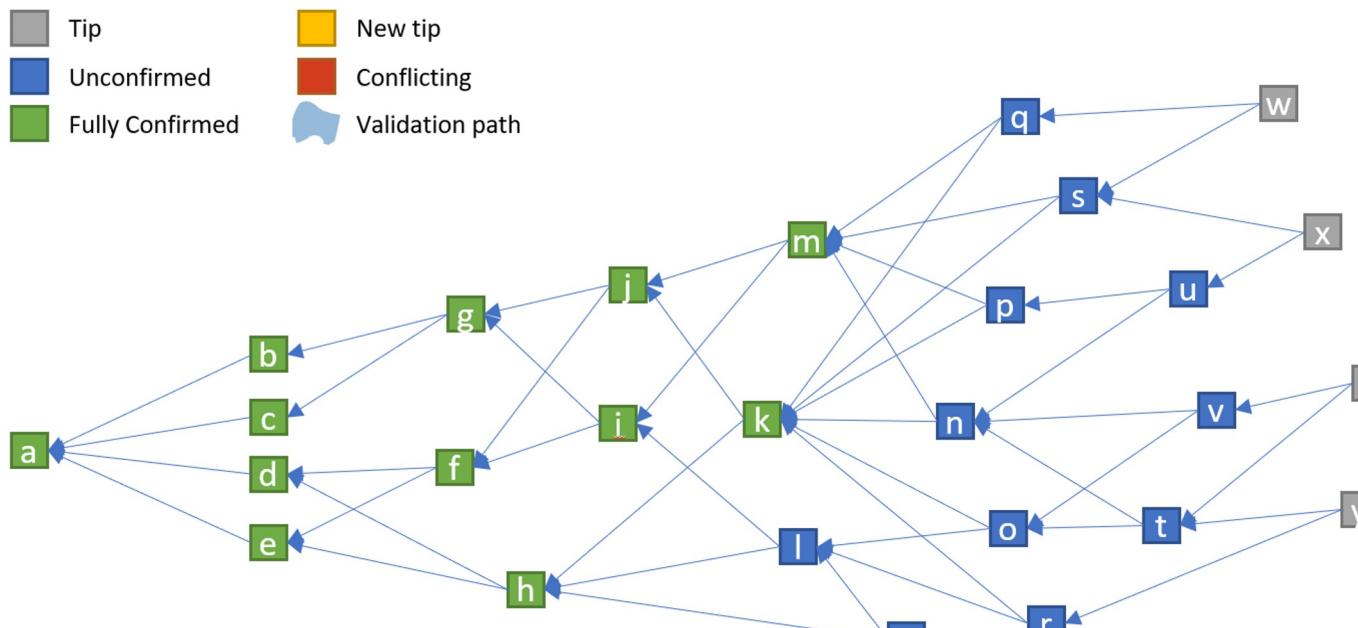


. شکل ۹ . MIOTA Cryptocurrency



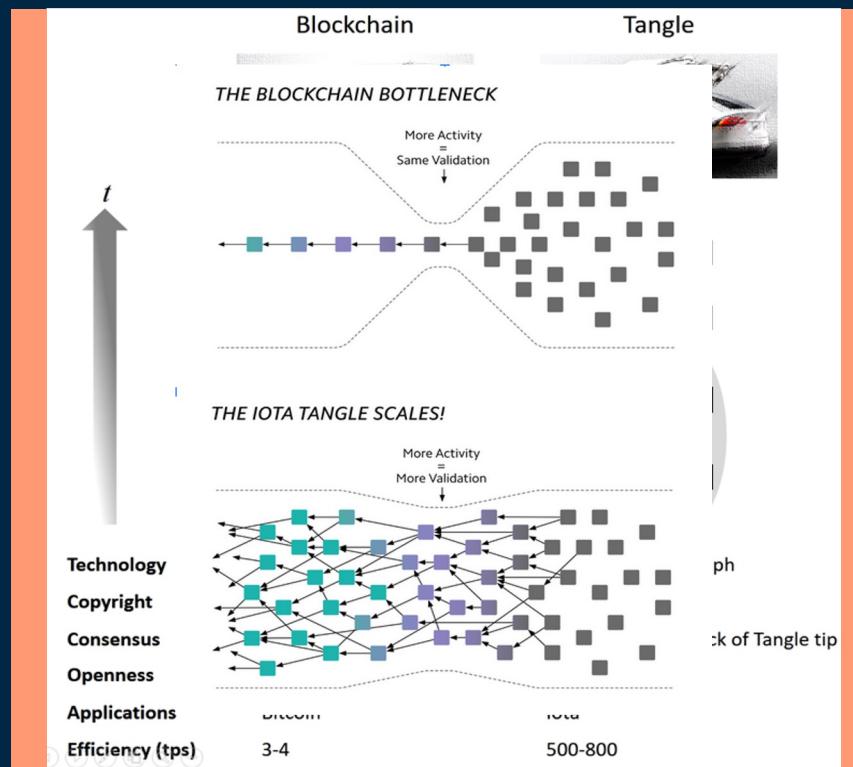
. شکل ۸ . Distributed Ledger

TANGLE



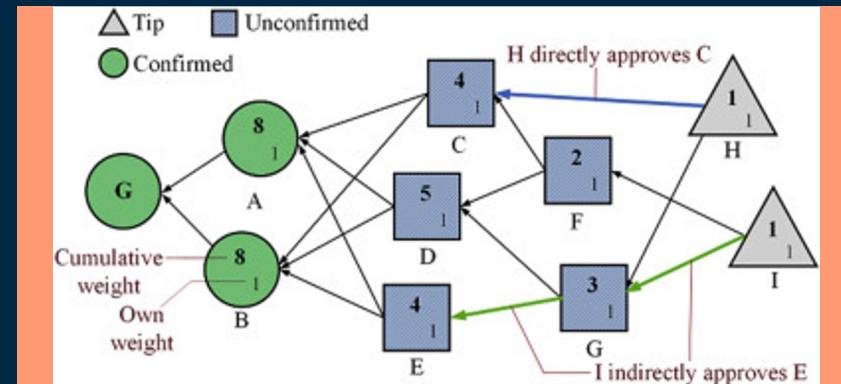
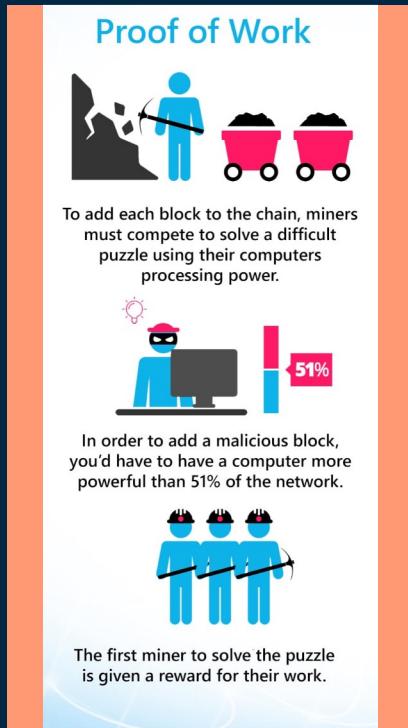
. Directed Acyclic Graph in Tangle شكل ١١

TANGLE vs BlockChain



. BlockChain and Tangle Comparison شکل ۱۲

TANGLE vs BlockChain: Consensus



. شکل ۱۳ . Tangle Consensus

. PoW شکل ۱۴

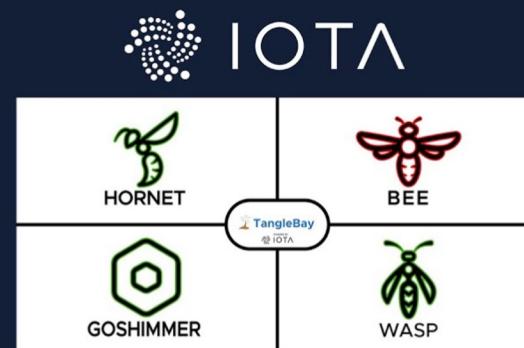
چرا تراکنش در آیوتا بدون هزینه است؟

- Consensus
- Designed for IoT

چرا آیوتا برای IoT مناسب است؟

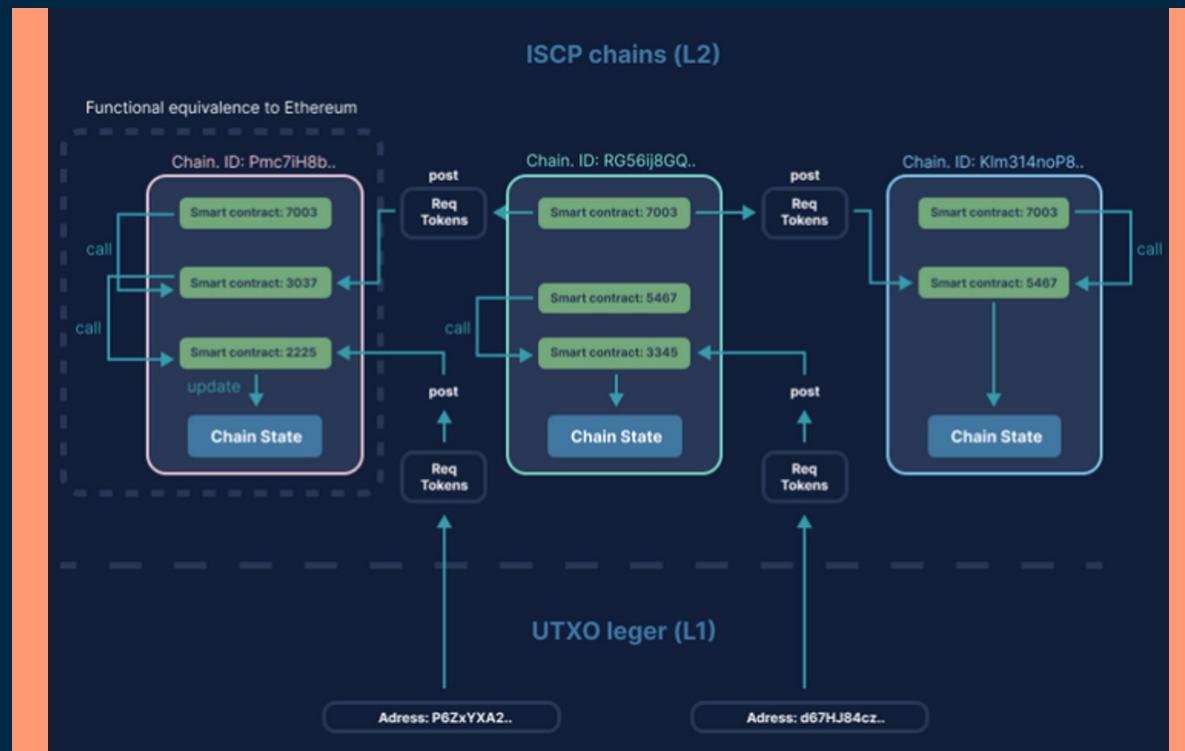
- حذف هزینه تراکنش و حذف عملیات پیچیده PoW
- حذف گلوبال های مرسوم در شبکه های بلاک چینی با استفاده از Tangle
- انرژی کارآمد
- Smart Contract

معماری کلی



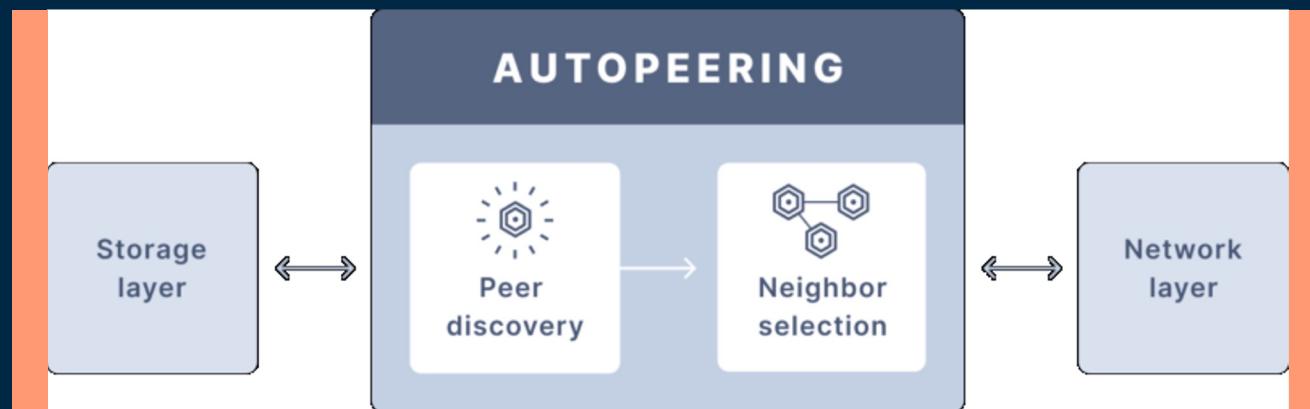
. شکل ۱۵ IOTA Nodes

Smart Contract



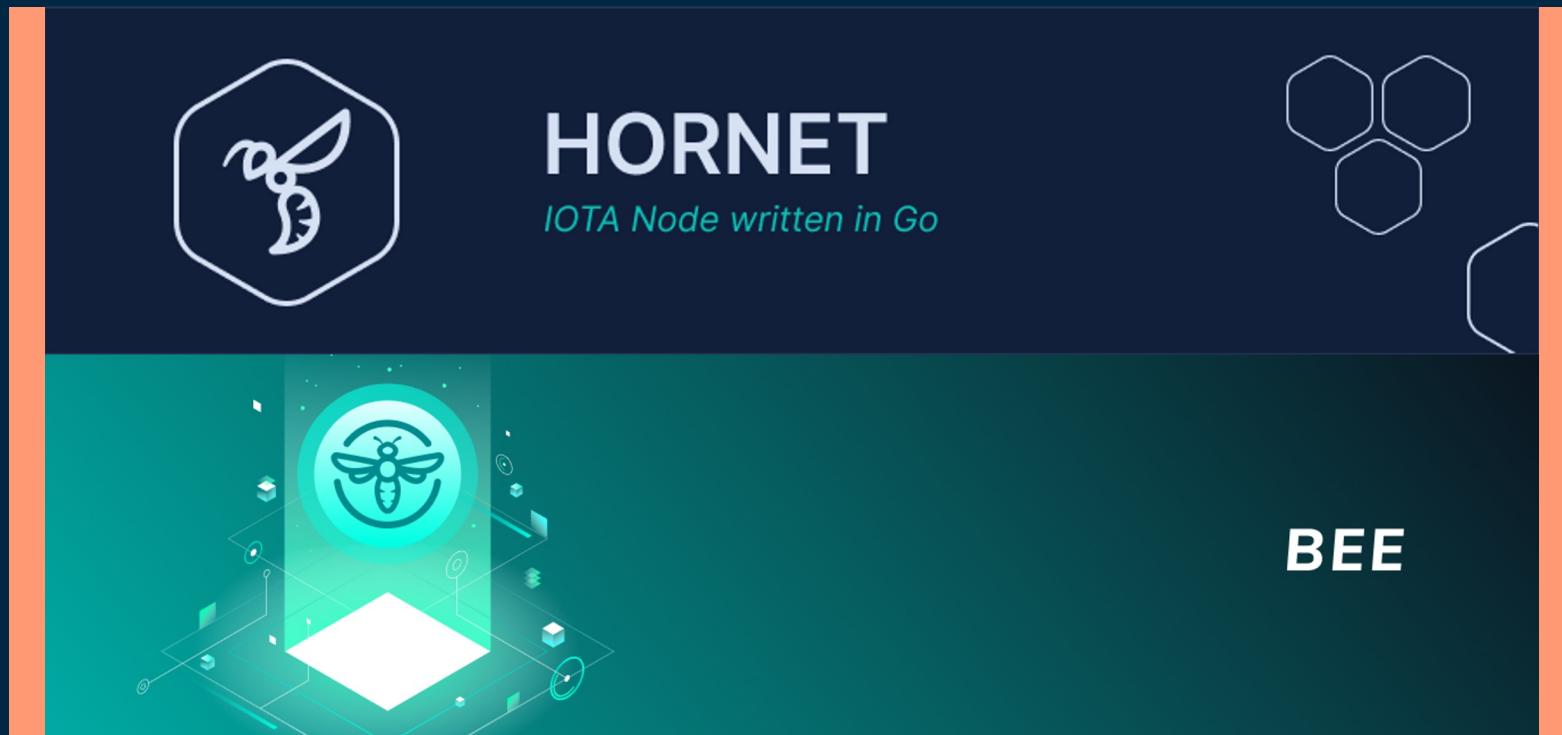
• IOTA Smart Contracts multichain architecture ﺵ ﻢـ ﻪـ

GoShimmer



. Autopeering Module in GoShimmer شکل ۱۷

Hornet & Bee Node



. Hornet Node & Bee Node \ ١٨ شکل

کاربردهای آیوتا

- تاثیرات اجتماعی (Social Impact)
- استفاده در دستگاه‌های در حال حرکت مانند خودرو خودران
- شهرهای هوشمند
- تجارت جهانی
- هویت دیجیتال

Federated learning

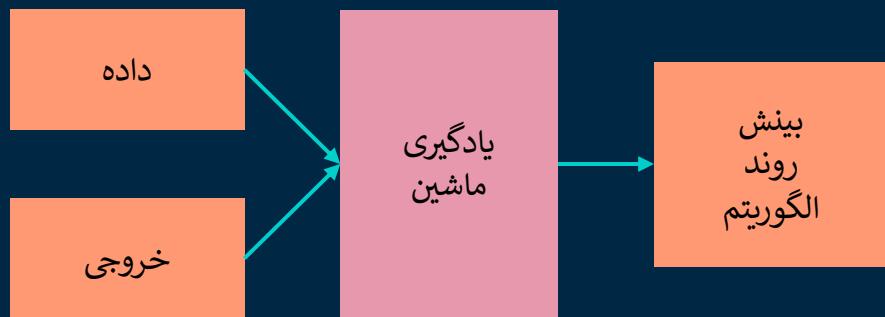
05

چرا یادگیری ماشین؟

- حجم عظیم داده‌ها از میلیون‌ها دستگاه اینترنت اشیا

- نیاز به تجزیه و تحلیل داده‌ها
- بھبود عملکرد شبکه
- تبلیغات
- پیش‌بینی آینده

- مدل‌سازی و تمرین مدل



شكل ۱۹. کارکرد یادگیری ماشین

یادگیری ماشین معمول و متمرکز



شکل ۲۰. مدل سازی با رویکرد ML عادی

چالش اصلی

حریم خصوصی

رویکرد توزیع شده پادگیری ماشین



شکل ۲۱. مدل سازی با رویکرد FL

Federated Averaging

Algorithm 1 FederatedAveraging. The K clients are indexed by k ; B is the local minibatch size, E is the number of local epochs, and η is the learning rate.

Server executes:

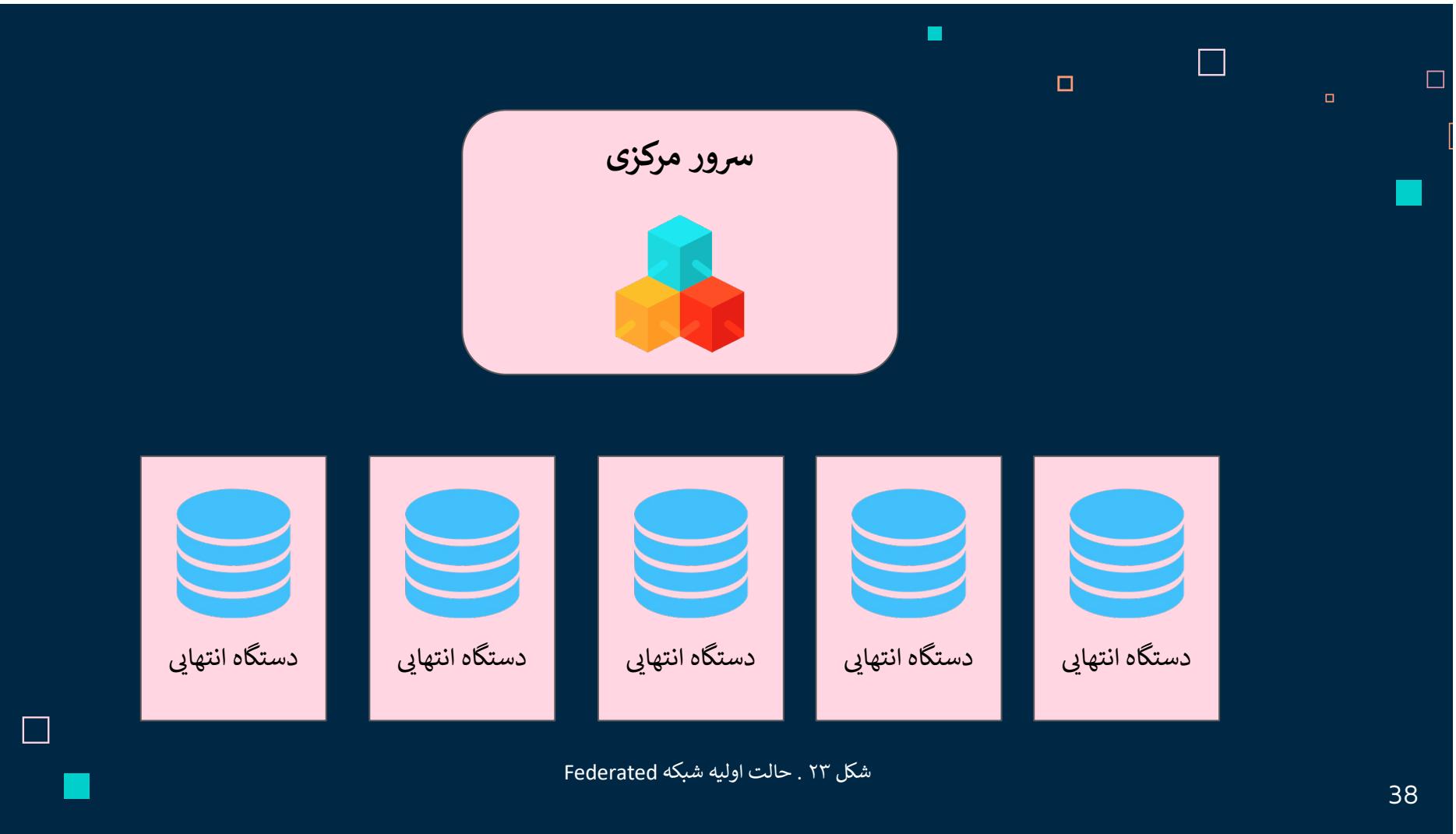
```
initialize  $w_0$ 
for each round  $t = 1, 2, \dots$  do
     $m \leftarrow \max(C \cdot K, 1)$ 
     $S_t \leftarrow (\text{random set of } m \text{ clients})$ 
    for each client  $k \in S_t$  in parallel do
         $w_{t+1}^k \leftarrow \text{ClientUpdate}(k, w_t)$ 
     $w_{t+1} \leftarrow \sum_{k=1}^K \frac{n_k}{n} w_{t+1}^k$ 
```

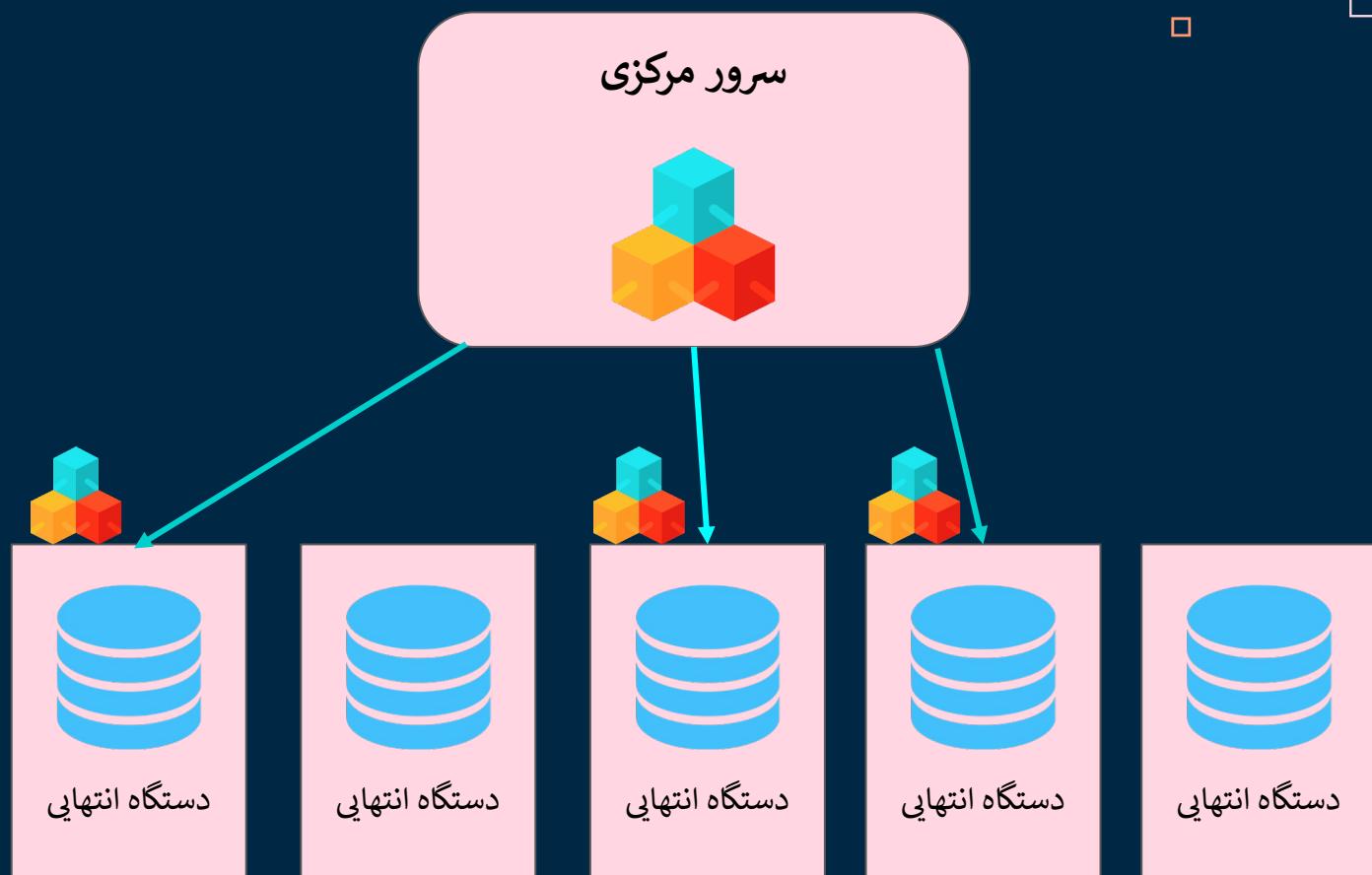
```
ClientUpdate( $k, w$ ): // Run on client  $k$ 
 $\mathcal{B} \leftarrow (\text{split } \mathcal{P}_k \text{ into batches of size } B)$ 
for each local epoch  $i$  from 1 to  $E$  do
    for batch  $b \in \mathcal{B}$  do
         $w \leftarrow w - \eta \nabla \ell(w; b)$ 
return  $w$  to server
```

یکی از مهمترین الگوریتم‌های Federated Learning

- مبنا برای الگوریتم‌های ارائه شده بعد از آن

شکل ۲۲. سودوکوی Federated Averaging

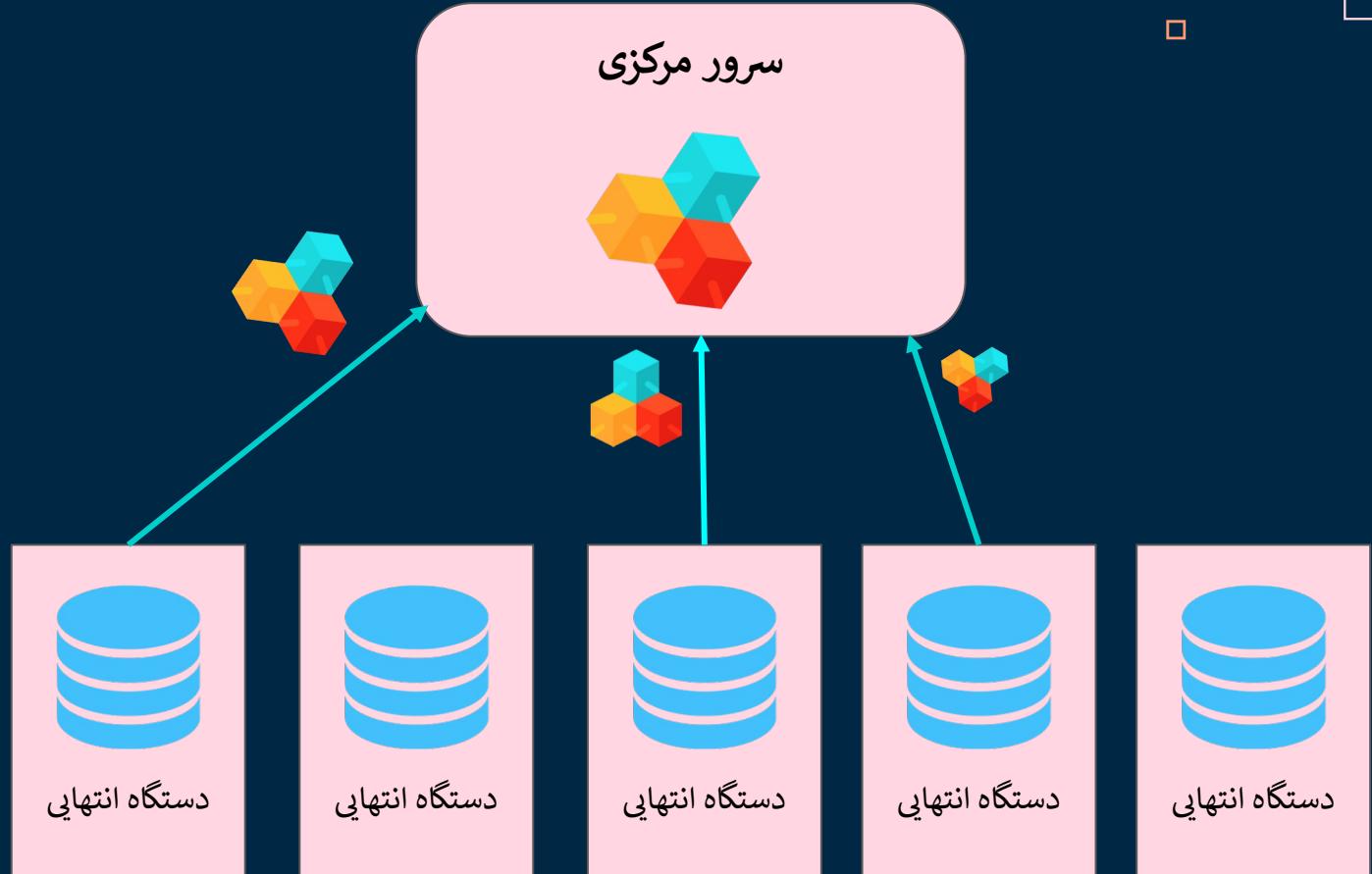




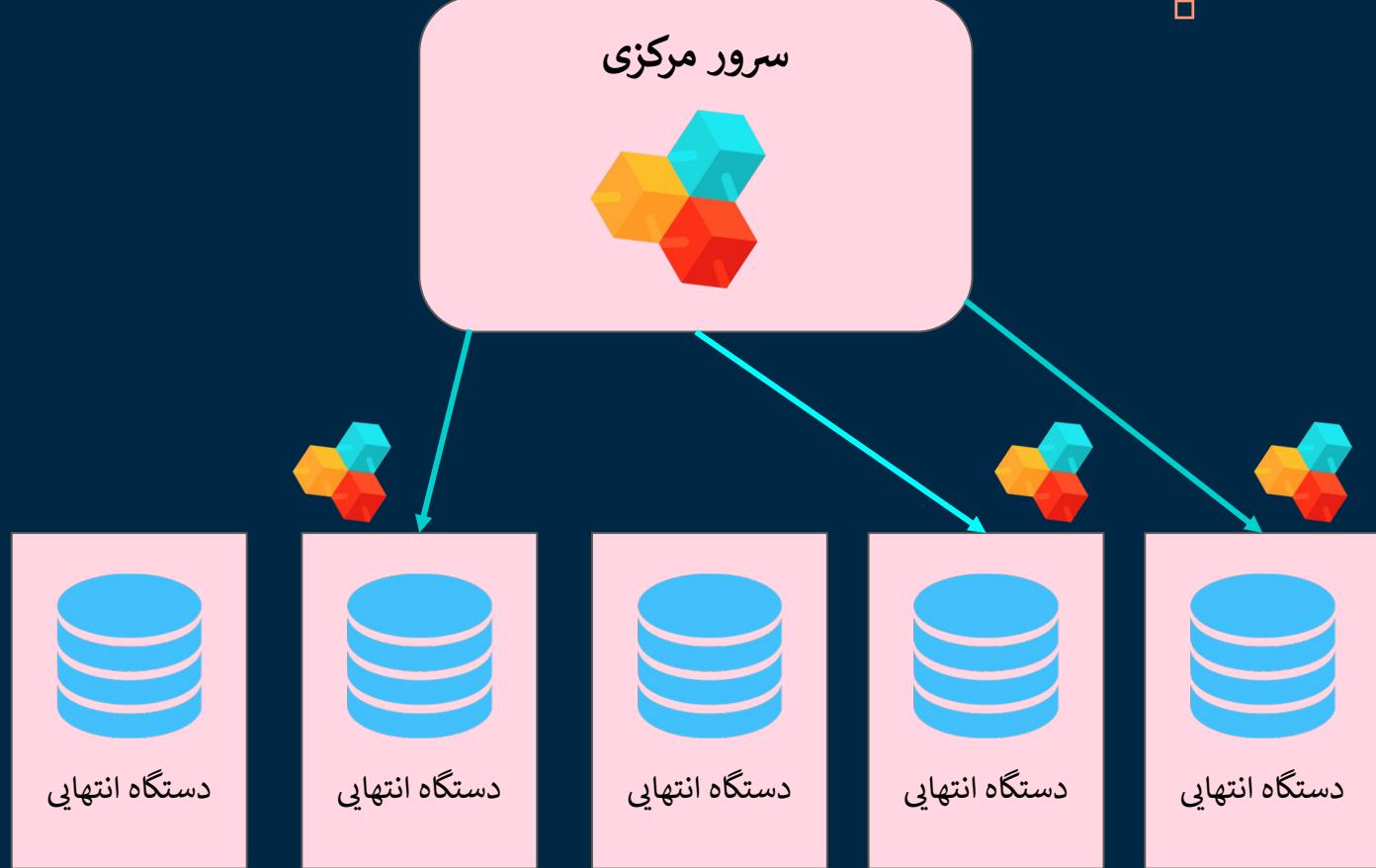
شکل ۲۴. ارسال مدل به دستگاه‌های انتهایی



شکل ۲۵ . بروزرسانی مدل‌های محلی



شکل ۲۶ . ارسال مدل‌های محلی برای سرور مرکزی



شکل ۲۷. ادامه روند مدل سازی

مجتمع‌سازی و بلاکچین Federated learning



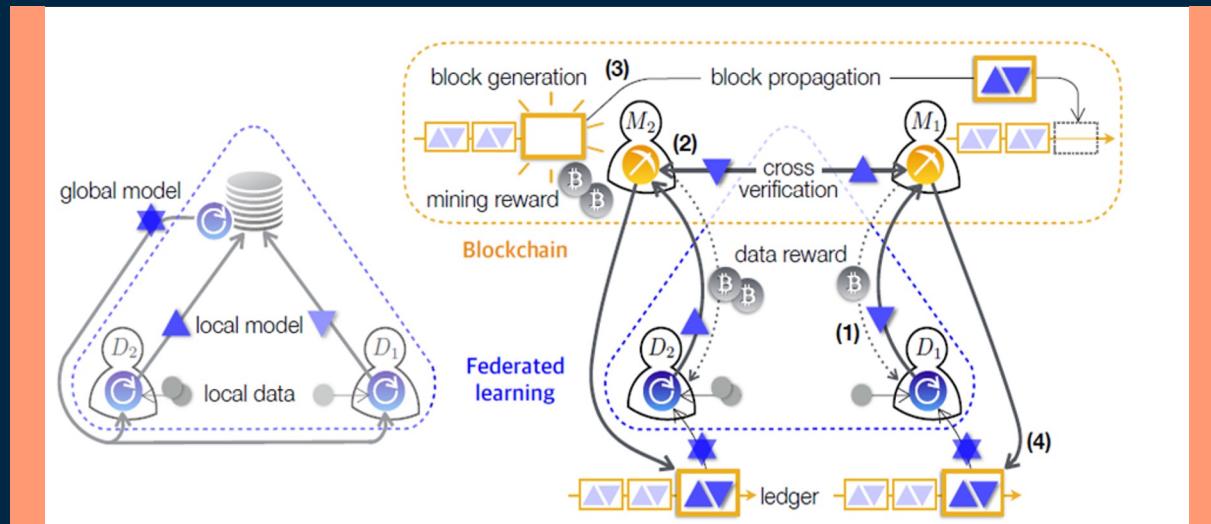
شکل ۲۸ . چالش‌های Federated learning

- ارتباطات هزینه‌بر
- ناهمگونی دستگاه‌ها
- حفظ امنیت

مجتمعسازی Federated learning و بلاکچین (ادامه)

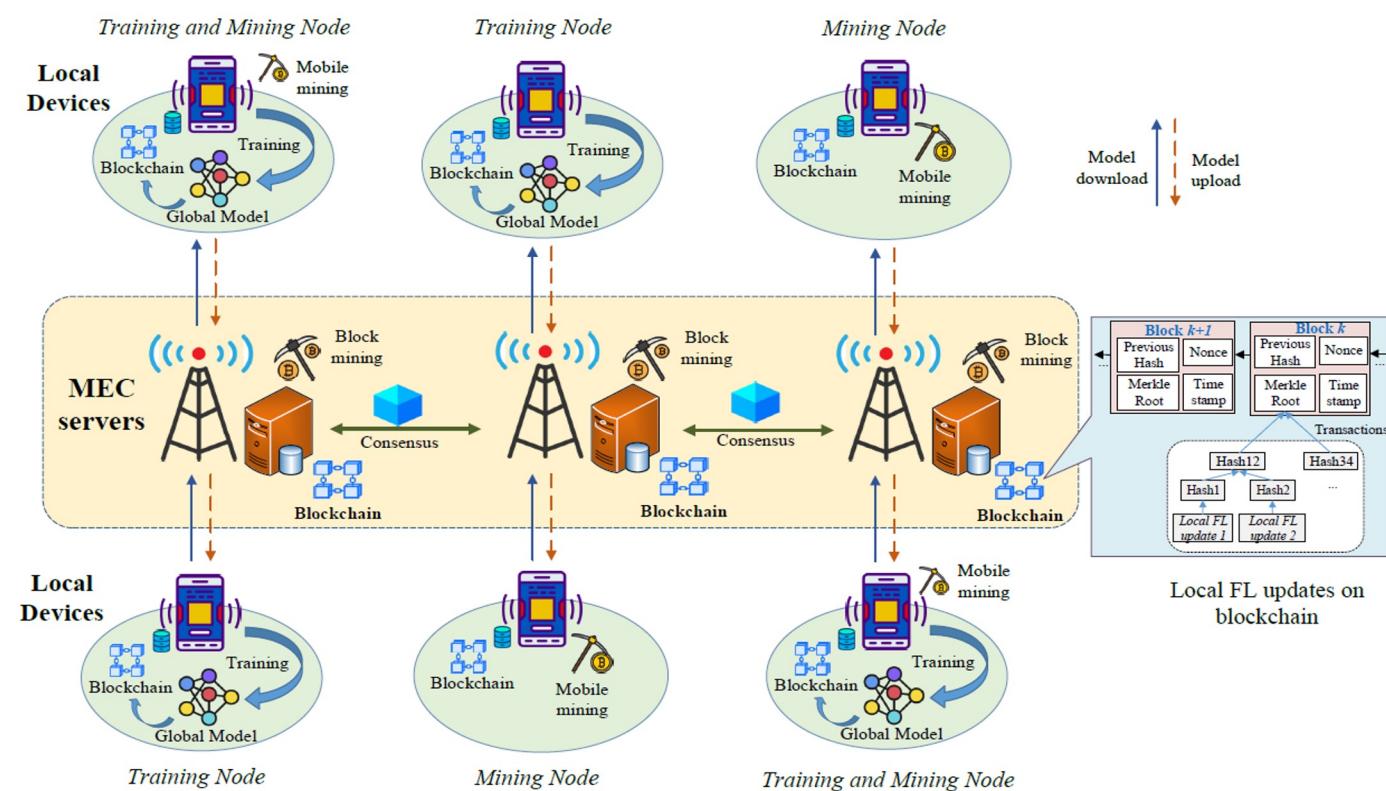
قابلیت‌های منحصر به فرد بلاکچین

- حذف سرور مرکزی
- تغییرناپذیر ledger
- سیستم پاداش دهنده



شکل ۲۹. نمایی از یک معماری پیشنهادی برای ترکیب Federated learning با بلاکچین

FLchain

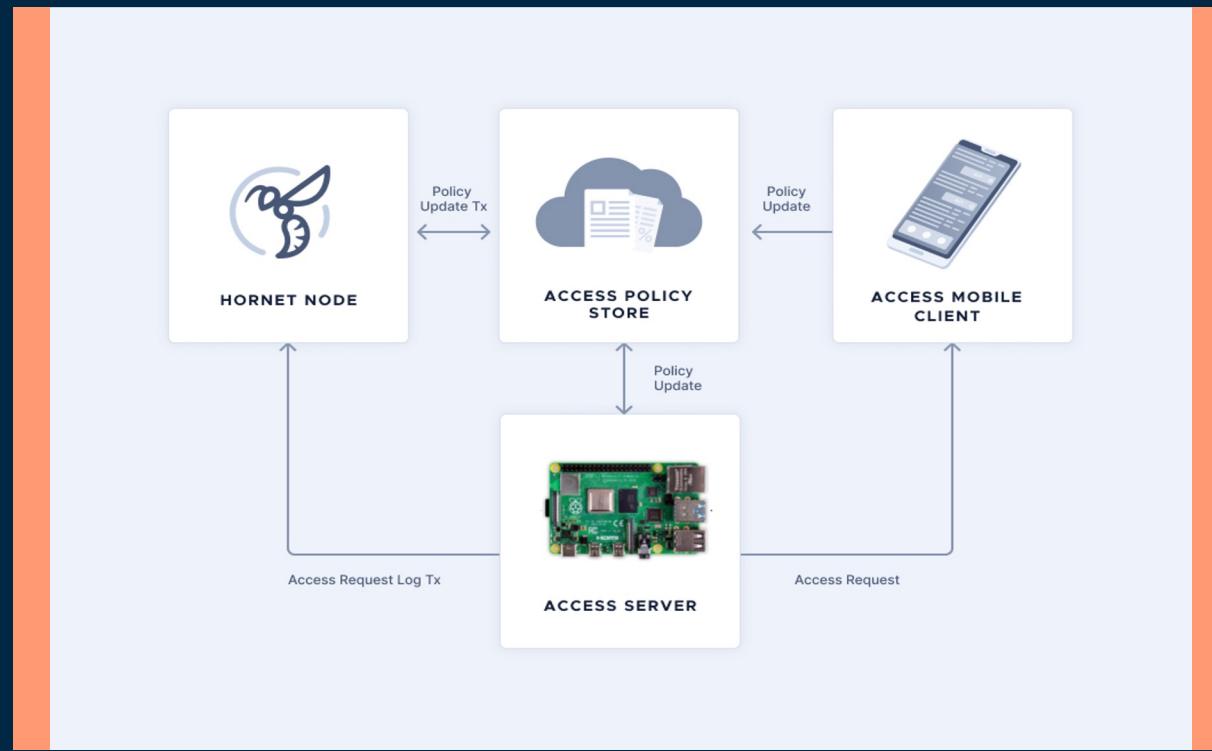


شکل ۳۰. معماری FLchain

Future works

06

Raspberry Pi



شكل ٣١. معماري شبكة داخلی

Smart Contracts

- بررسی مثال قرارداد هوشمند موجود در داکیومنت سایت
- آشنایی بیشتر با VM های مختلف و خصوصیت های هر کدام
- نوشتن یک قرارداد هوشمند برای یک کاربرد خاص در زمینه IoT
- استفاده از federated learning در یکی از کاربردهای مرتبط با IoT

منابع

- [1] Lee, In, Lee, Kyoochun. "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." In *Business Horizons*, Volume 58, Issue 4, Pages 431-440, July–August 2015.
- [2] Novo, Oscar. "Blockchain meets IoT: An architecture for scalable access management in IoT." *IEEE internet of things journal* 5.2 (2018): 1184-1195.
- [3] Zheng, Zibin, Wang, Huaimin, Xie, Shaoan, Dai, Hong-Ning. " Blockchain challenges and opportunities: a survey." In *International Journal of Web and Grid Services* 14(4): 352 – 375, DOI:10.1504/IJWGS.2018.10016848, October 2018.
- [5] Dorri, Ali, Salil S. Kanhere, and Raja Jurdak. "Towards an optimized blockchain for IoT." In Proc. IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), 2017.
- [6] Panarello, Alfonso, et al. "Blockchain and iot integration: A systematic survey." *Sensors* 18.8, 2018.
- [7] Dorri, Ali, et al. "Blockchain for IoT security and privacy: The case study of a smart home." In Proc. IEEE international conference on pervasive computing and communications workshops (PerCom workshops) , 2017.

منابع (ادامه)

- [9] V. A. Gasimov and S. K. Aliyeva, "Using blockchain technology to ensure security in the cloud and IoT environment," In Proc. 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2021.
- [10] P. Gupta, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "Towards a blockchain powered IoT data marketplace," In Proc. International Conference on COMmunication Systems & NETworkS (COMSNETS), 2021, pp. 366-368.
- [11] S. R. Niya et al., "Adaptation of Proof-of-Stake-based Blockchains for IoT Data Streams," In Proc. IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2019.
- [12] J. Xu, S. Wang, A. Zhou and F. Yang, "Edgence: A blockchain-enabled edge-computing platform for intelligent IoT-based dApps," in China Communications, vol. 17, no. 4, pp. 78-87, April 2020.
- [13] Tsiknas, K, Taketzis, D, Demertzis, K, Skianis, C. "Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures." in MDPI, 163–186, 2021.
- [15] Abreha, H.G, Hayajneh, M, Serhani, M.A. "Federated Learning in Edge Computing: A Systematic Survey." in MDPI, 2022.

منابع (ادامه)

- [16] McMahan, H.B, Moore, E, Ramage, D, Hampson, S, Agüera y Arcas, B. "Communication-Efficient Learning of Deep Networks from Decentralized Data." in PMLR, vol. 54, 2017.
- [8] M. A. Islam and S. Madria, "A Permissioned Blockchain Based Access Control System for IOT," In Proc. IEEE International Conference on Blockchain (Blockchain), 2019, pp. 469-476.
- [17] Li, T, Sahu, A.K, Talwalkar, A, Smith, V. "Federated Learning: Challenges, Methods, and Future Directions." in IEEE Signal Processing Magazine, Vol 37, Issue 3, August 2019.
- [18] Nguyen, C.D, Ding, M, Pham, Q, Pathirana, P, Le, L.B, Seneviratne, A, Li, J, Niyato, D, Vincent Poor, H. "Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges." in IEEE Internet of Things Journal, Vol 8, Issue 16, 2021.
- [19] Kim, H, Park, J, Bennis, M, Kim, S.L " Blockchained On-Device Federated Learning." in IEEE Communications Letters, Vol 24, Issue 6, July 2019.
- [20] IOTA Foundation. (2021). IOTA Smart Contracts [White paper].

با تشکر از توجه شما

