موضوع پایان نامه:
طراحی سیستم کنترل دسترسی مدرن با بکارگیری قراردادهای هوشمند

استاد راهنما: آقای دکتر رضاخانی

دانشجو:مریم توکلی

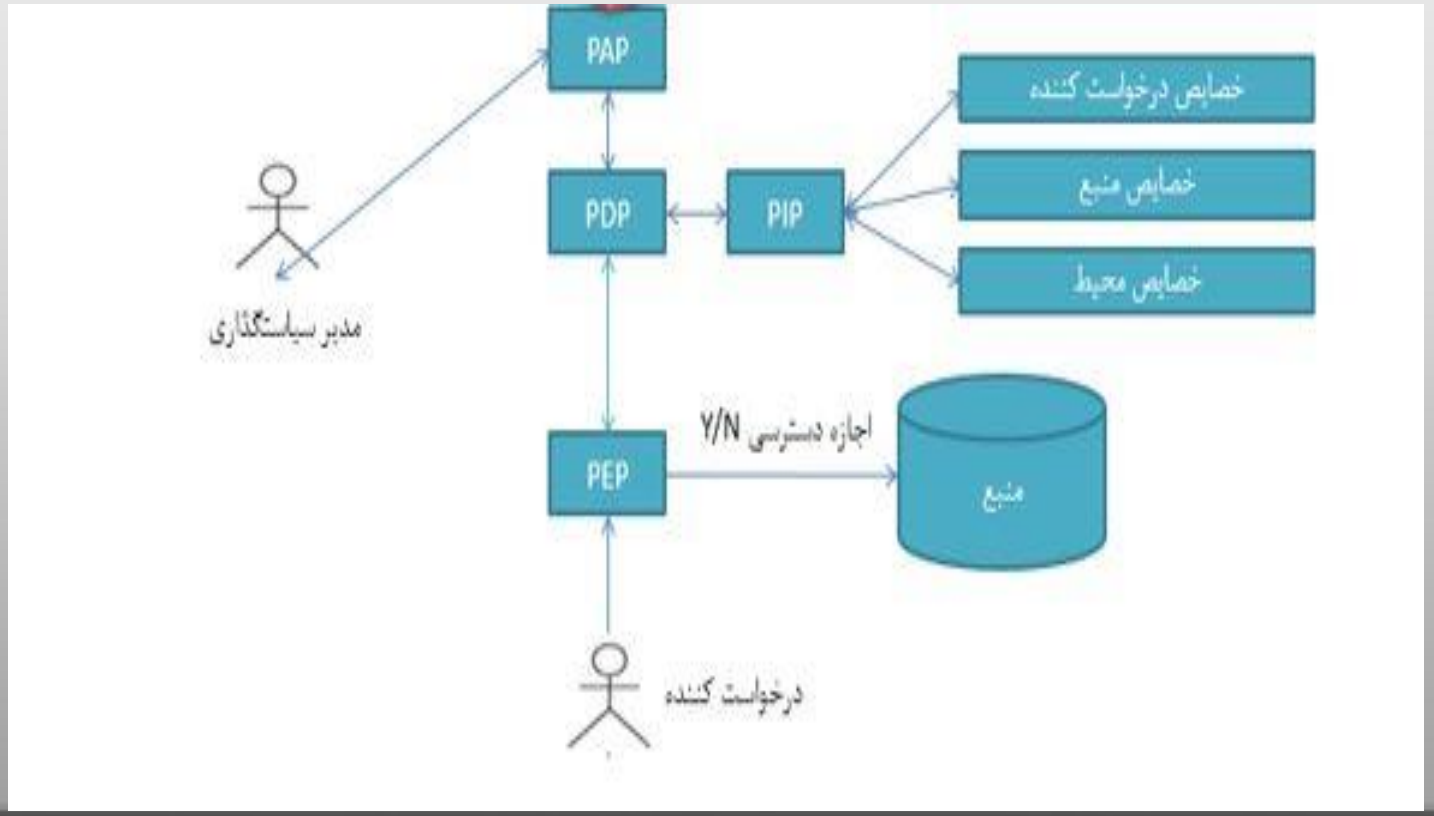
امروزه در قرن بیست و یکم که به آن عصر انفجار اطلاعات می گویند، پیشرفت تکنولوژی آنچنان جنبه های گوناگون زندگی ما را تحت تاثیر قرار داده و در متن زندگی ما نفوذ کرده است که گاها برای خودمان نیز هیجان آور و باور نکردنی است.

اما مساله مهم حفاظت از اطلاعات می باشد حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز

یک تعامل اولیه و خاص، بین یک درخواست کننده و یک منبع است که در نهایت منجر به برقراری جریان اطلاعاتی از یکی از آن‌ها به دیگری خواهد شد.

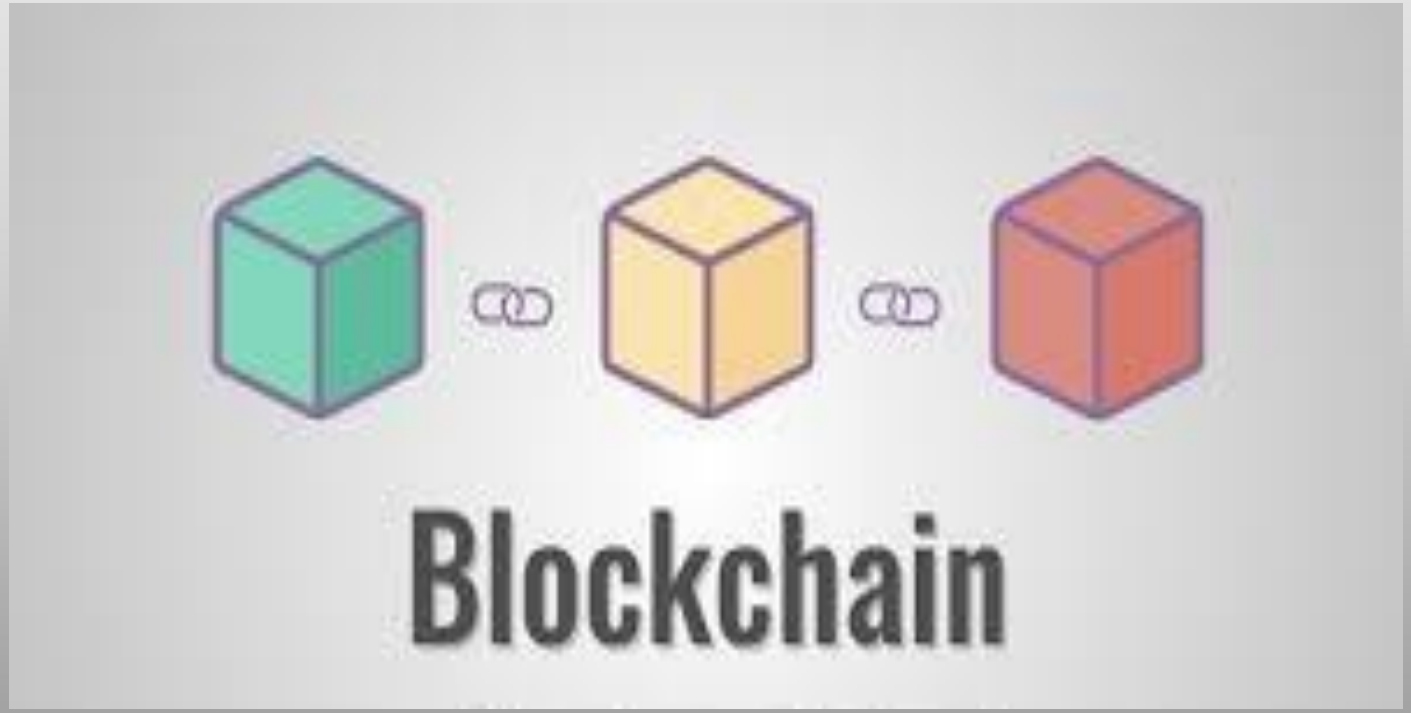
نکته: به‌طور کلی عناصری که توان انجام فعالیت و اجرای عملی روی چیز دیگری دارند عامل و عناصر دیگر را منبع می‌نامیم.

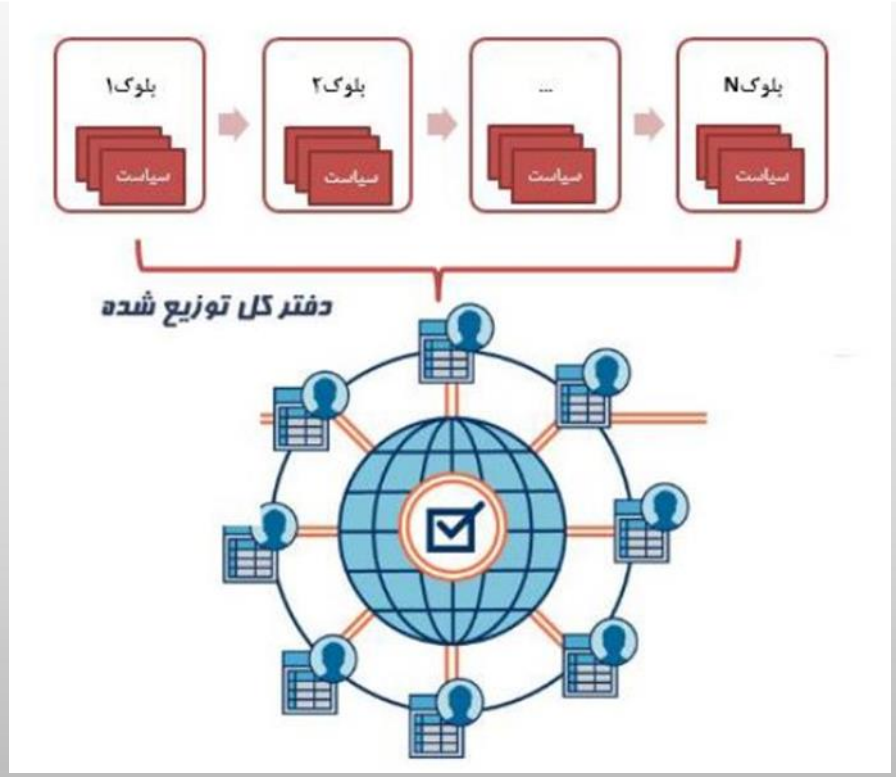
## کنترل دسترسی فعلی



**بلاکچین** یک نوع سیستم ثبت اطلاعات و گزارش است

**بیت کوین** اولین کاربرد از این فناوری بود و از بلاکچین برای ذخیره اطلاعات دارایی کاربران بهره برد.






داده‌های بلاکچین در یک کامپیوتر یا سرور خاص ذخیره نمی‌شوند. هر کامپیوتر یا سیستمی که به شبکه وصل شود یک نسخه از بلاکچین را دریافت می‌کند .

## احراز هویت با بلاکچین

- بعضی از سازمان‌ها سرویس تایید احراز هویت آنلاین در اختیار مردم می‌گذارند.
- با استفاده از این سرویس‌ها، می‌توانیم کارت احراز هویت را اسکن کنیم و اعتبار آن را بررسی کنیم. این کار خیلی پر هزینه است.
- اگر شما از بلاک‌چین استفاده کنید دیگر نیاز نیست هزینه‌ای بابت زیرساخت آن بپردازید. شما می‌توانید بعنوان مثال از بستر اتریوم برای ذخیره کردن جزئیات هویتتان استفاده کنید.

**رای گیری بلاکچین و تاثیر آن بر شفافیت انتخابات و اعتماد رای دهندگان**

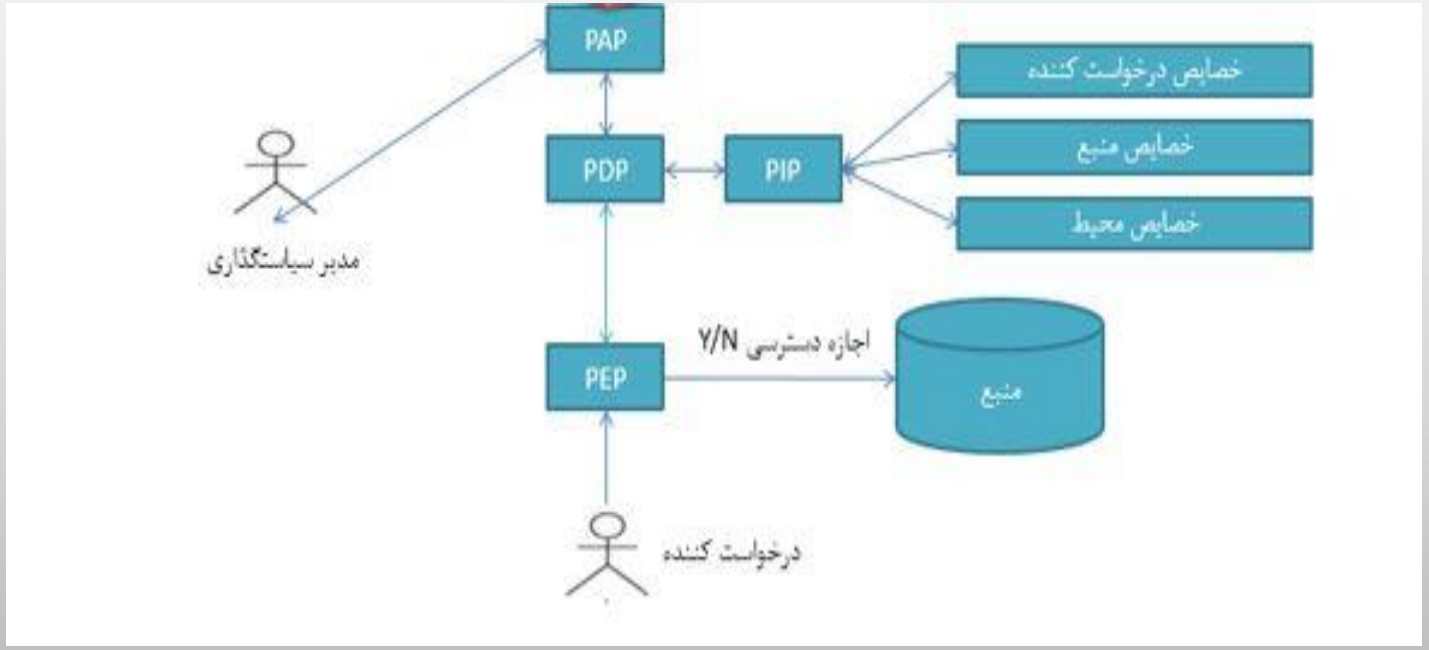
درست مانند مدیریت زنجیره تامین، وعده بلاکچین در مورد رای دهی، در حال جلب اعتماد کاربران است.
در حال حاضر، فرصت‌هایی که وابسته به انتخابات دولت‌ها است، در حال پیگیری هستند.


انجام این کار به طرز شفاف احتمال تقلب در انتخابات را کم می‌کند که در عین حال یک موضوع مهم در حضور سیستم‌های رای‌گیری الکترونیک است.

## دفتر اسناد رسمی

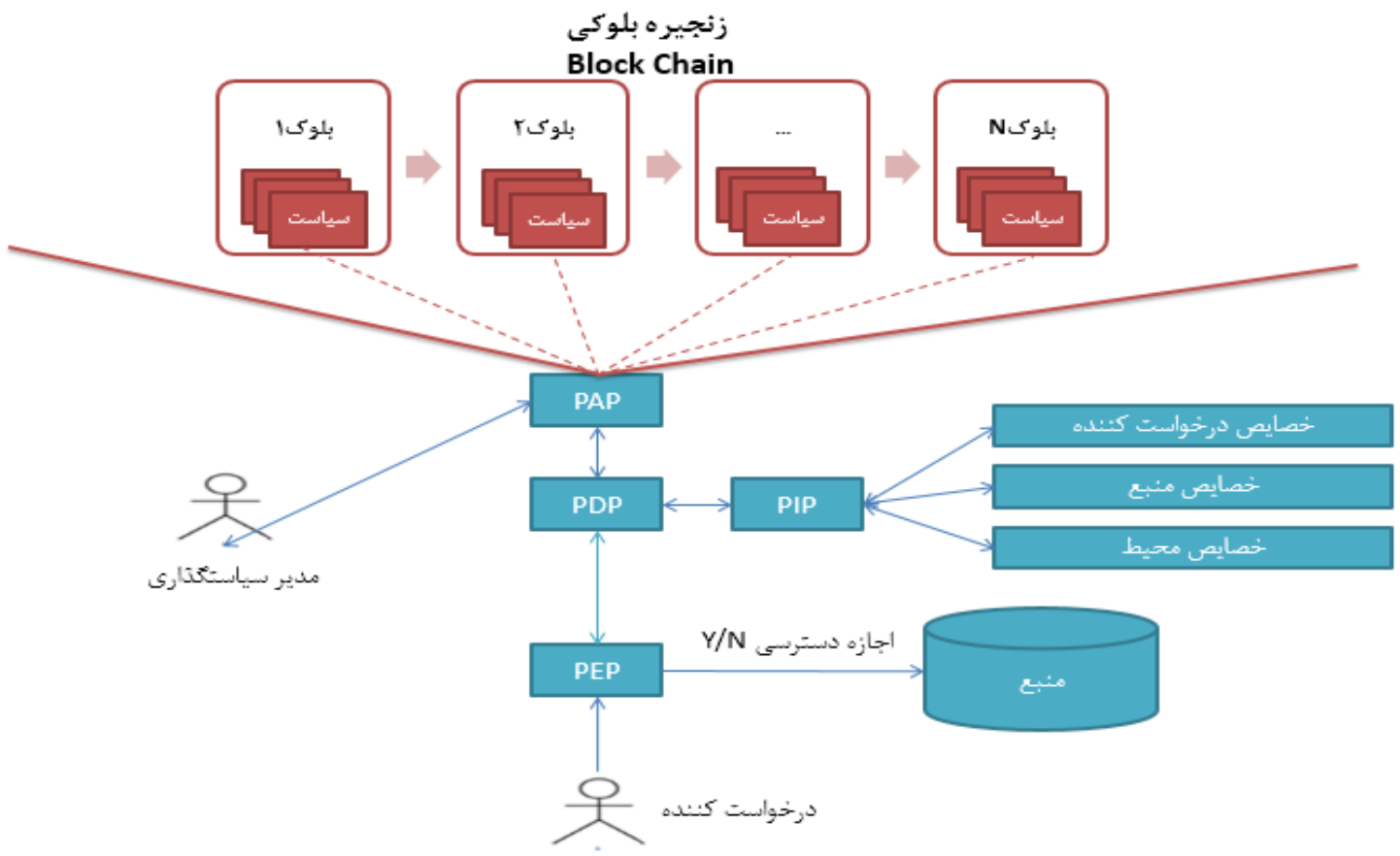
- امروزه اکثر سوابق مالکیت شما در کاغذ ذخیره می‌شوند و امکان دستکاری در این سوابق وجود دارد. از آنجایی که این تکنولوژی از کامپیوترها استفاده می‌کند، خطاهای انسانی کاهش می‌یابد.
- اگر کسی اطلاعات بلاک ها را دستکاری بکند و اطلاعات را تغییر دهد، عبارت هش تغییر خواهد کرد و این تغییر باعث شکستن توالی بلاک‌ها می‌شود.
- با این اوصاف کسی نمی‌تواند در این بلاک‌ها تغییر ایجاد کند. هر تغییری از دید همگان مخفی نخواهد ماند.

بررسی چالش سیستم های کنترل دسترسی فعلی




- ✓ سیاست های کنترل دسترسی در یک نقطه متمرکز هستند.
- ✓ احتمال حمله و از کار انداختن سیاستها وجود دارد.
- ✓ احتمال دسترسی غیرمجاز و تغییر یا از بین رفتن سیاستها هست.

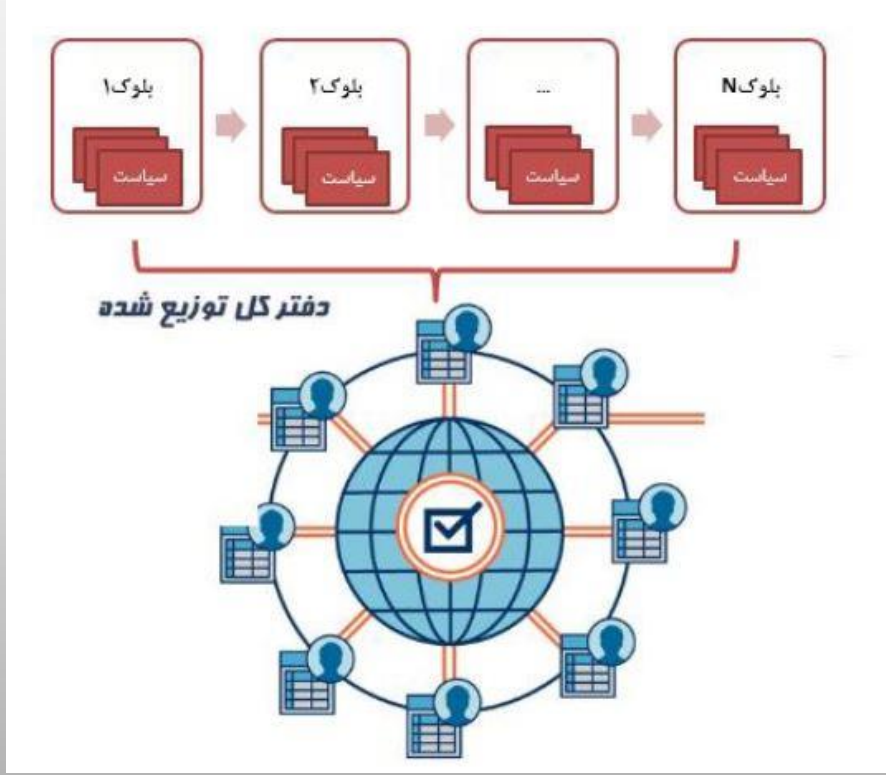
هدف ما در این پژوهش ایجاد ارتباط بین سیستم کنترل دسترسی از یک طرف و زنجیره بلوکی از طرف دیگر است



ساختار پیشنهادی برای قرارگیری سیاست های کنترل دسترسی


سیاست های کنترل دسترسی موجود در پایگاه سیاست PAP ، در بلوک ها ذخیره شده است و این زنجیره تحت عنوان دفتر کل در اختیار همه نودهای تعیین شده قرار می گیرد

نحوه قرار گیری سیاستها در دفتر کل توزیع شده



## پیاده سازی

برای پیاده سازی از دو ابزار استفاده می گردد. یکی از ابزار Acpt برای پیاده سازی سیاستهای کنترل دسترسی و دیگری blockchain که از ابزار Anders Brownworth استفاده می گردد.

## پیاده سازی (ادامه)

این ابزار توسط Nist طراحی و پشتیبانی می شود. نمایی از این ابزار بصورت شکل زیر است.

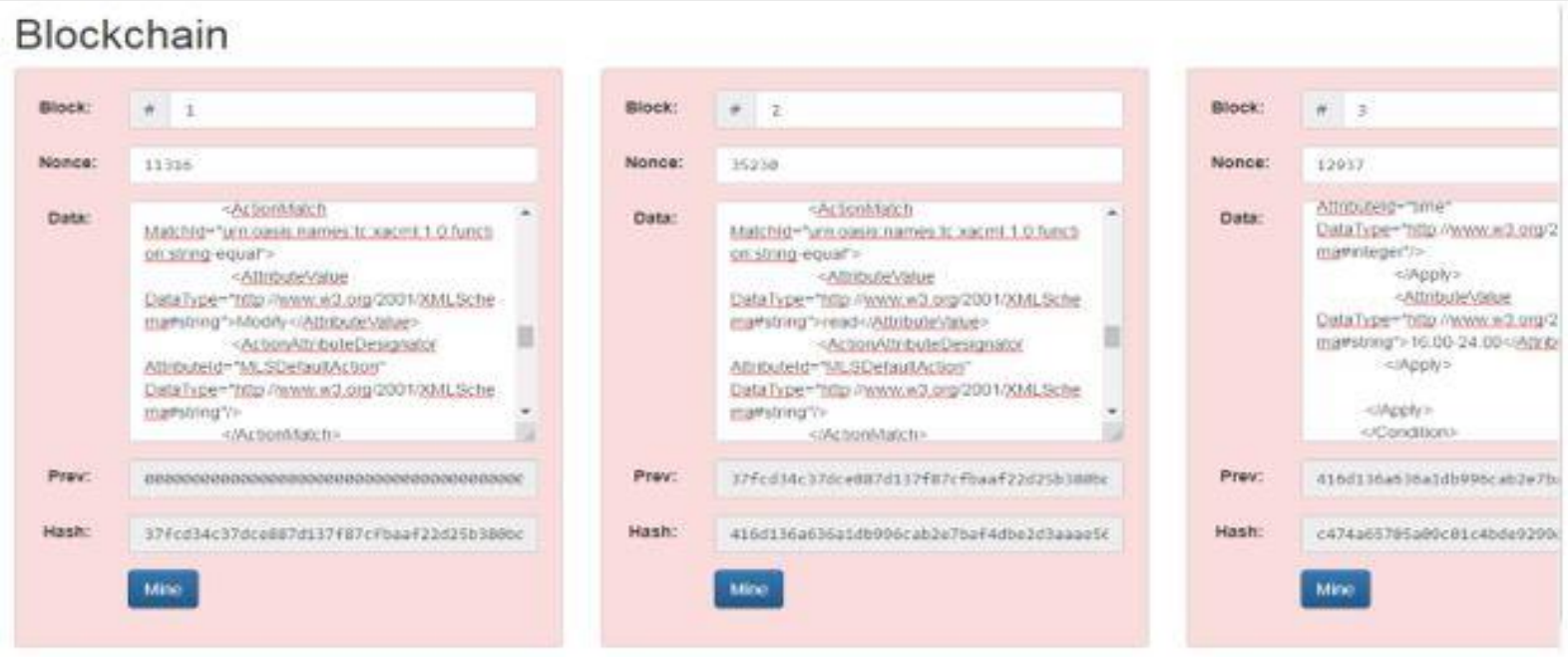
## پیاده سازی (ادامه)

نمونه سیاست های تولید شده به زبان XACML

```
<?xml version="1.0" encoding="UTF-8"?><!--## This XACML is the collection of policies (e.g., POLICY 1) to be merged (by users).-->
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" PolicySetId="MergedPolicySet" PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable">
  <Target/>
<!--## POLICY START1-->
   <Policy PolicyId="Example_policy" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
     <Target/>
<!-- ABAC Model: Example_policy-->
    <Rule RuleId="rule_1" Effect="Permit">
     <Target>
      <Subjects>
       <Subject>
```

## پیاده سازی (ادامه)

قرار گیری سیاستها در زنجیره بلوکی




اولین سیاست کنترل دسترسی در بخش data از بلوک اول قرار می گیرد. سیاست دوم در بلوک دوم و به همین صورت ادامه می یابد.

## ارزیابی

پارامترهای ارزیابی

- سرکوب خصایص
- نتیجه نامشخص
- تدوین سیاست‌های غیر متمرکز
- عدم حمله Dos به PAP
- سهولت پیاده سازی

## ارزیابی (ادامه)

| روش‌ها | سرکوب خصایص | نتیجه نامشخص | تدوین سیاست های غیرمتمرکز | عدم حمله Dos به PAP | سهولت پیاده‌سازی |
|---|---|---|---|---|---|
| روش Laurent [50] | NS | LS | NS | LS | NS |
| روش Guo [51] | LS | LS | NS | LS | NS |
| روش Maesa [52] | NS | LS | FS | LS | LS |
| روش Xue [53] | NS | LS | NS | LS | NS |
| روش پیشنهادی | LS | LS | FS | FS | FS |

FS: Full support

LS: Low support

NS: No support

## نتیجه گیری

قسمت نوآورانه این پایان نامه استفاده از زنجیره بلوکی برای استفاده از PAP بود.

تمام اطلاعات سیاستهای کنترل دسترسی بجای اینکه به صورت متمرکز در یک نقطه قرار بگیرند، بصورت کپی در بلوک های مختلف از زنجیره  قرار می گیرند.

- رویکرد پیشنهادی برای دادن مجوز دسترسی به منبع مطابق با ISO 10181 است.
- ماژول کنترل دسترسی مورد استفاده، از مدل Attribute based access control
- معماری بیان شده در ISO/IEC 10181 استفاده کند.

## کارهای آتی

- استفاده از تکنولوژی زنجیره بلوکی در پروسه تصمیم گیری در سیستم کنترل دسترسی
- استفاده از زنجیره بلوکی در PIP از سیستم کنترل دسترسی
- معماری کنترل دسترسی مبتنی بر ریسک امنیتی با استفاده از زنجیره بلوکی

منابع
مریم جوزدانی, & سعید مظفری. (۲۰۱۹). پذیرش بلاک چین به عنوان یک ضرورت در تجارت الکترونیک. فصلنامه علمی تخصصی رویکردهای پژوهشی نوین در مدیریت و حسابداری, ۳(۱۶), ۸۸-۹۶.
اکرم فیاض بخش. (۲۰۲۱). دستاوردی به نام «بلاک چین». فصلنامه علمی تخصصی رویکردهای پژوهشی نوین در مدیریت و حسابداری, ۵(۶۰), ۱-۸.
ابوالمعالی الحسینی, سیدوحید, علیزاده طباطبایی, & زهراسادات. (۲۰۰۹). حقوق امنیت اطلاعات شبکه. حقوق اسلامی, ۵(۱۹), ۱۳۷-۱۶۳.
حدادی هرندی, والمحمدی, چنگیز, & صالحی صدقیانی. (۲۰۱۹). مدیریت امنیت اطلاعات در کسب و کار هوشمند. علمی پژوهشی مدیریت بحران, ۸, ۲۵-۳۳.
میرزامحمدی, موسوی, سیدمجید, منصوری, & حمیدی. شناسایی عوامل تأثیرگذار بر امنیت اطلاعات در فضای مجازی. فصلنامه علمی تخصصی دانش انتظامی قزوین, ۱۳۹۹(۳۵), ۲۶-۵۶.
گودرزی, & تمتاجی. ارائه‌ی روش بهینه برای استقرار هم‌زمان نظام مدیریت خدمات فناوری اطلاعات و نظام مدیریت امنیت اطلاعات. مدیریت استاندارد و کیفیت, ۵, ۷۶-۸۳.
نصیری،طراحی یک سیستم قرارداد هوشمند مبتنی بر بلاک چین در حوزه مدیریت بهداشت و درمان،۱۳۹۹(۶۶-۶۳)
حیدریانیِ، ارائه روشی برای استقرار بلاک چین به منظور تأمین اطلاعات،ت ۱۳۹۸،(۵۸-۵۲)

**منابع**


Samarati, P., & de Vimercati, S. C. (2000, September). Access control: Policies, models, and mechanisms. In International School on Foundations of Security Analysis and Design (pp. 137-196). Springer, Berlin, Heidelberg.

Kalam, A. A. E., Baida, R. E., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., ... & Trouessin, G. (2003, June). Organization based access control. In Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks (pp. 120-131). IEEE.

Hu, V. C., Ferraiolo, D., & Kuhn, D. R. (2006). Assessment of access control systems. US Department of Commerce, National Institute of Standards and Technology.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

Wüst, K., & Gervais, A. (2018, June). Do you need a blockchain?. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45-54). IEEE.

## منابع


Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352-375.

Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016, October). Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 254-269).

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *Ieee Access*, *4*, 2292-2303.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475-491.

Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, *32*(5), 1754-1797.

## منابع


Kalodner, H., Goldfeder, S., Chen, X., Weinberg, S. M., & Felten, E. W. (2018). Arbitrum: Scalable, private smart contracts. In *27th {USENIX} Security Symposium ({USENIX} Security 18)* (pp. 1353-1370).

Nguyen, T. D., Pham, L. H., Sun, J., Lin, Y., & Minh, Q. T. (2020, June). sfuzz: An efficient adaptive fuzzer for solidity smart contracts. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering* (pp. 778-788).

Permenev, A., Dimitrov, D., Tsankov, P., Drachsler-Cohen, D., & Vechev, M. (2020, May). Verx: Safety verification of smart contracts. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 1661-1677). IEEE.

# با سپاس فراوان

- مقدمه
- کنترل دسترسی
- بلاکچین
- سوابق تحقیق
- روش پیشنهادی
- نتیجه گیری