



Příklady využití AI v oblasti bezpečnosti

<https://themama.ai>
mama@themama.ai

Jiří Vrobel
Business Development

<https://www.linkedin.com/in/jirivrobel/>



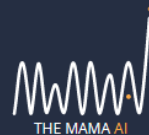


mSpeech platforma

Dokážeme analyzovat řeč lépe než to dokáží lidé.

Mining Bio Speech

- ✦ SIGINT: Využití bio signálů v řeči pro identifikaci klíčových biologických ukazatelů
- ✦ Porozumění náladě člověka pro empatickou komunikaci
- ✦ Měření stresu v hlasu
- ✦ Rozpoznání pohlaví a věkových skupin na základě hlasu



Real time

Audio file



WebRTC VAD	speech
Speech activity	speech
Gender	male (100%)
Language	czech (96%)
Age	sixties (52%)
Cadence	A noisy background or unnatural-sounding speech detected.
Cadence NN	4.91 (normal)
Energy	unk
SNR	unk
Emotion	happy (100%)

Mining Bio Speech

- ✦ Pro srovnání: takto vypadá můj hlasový otisk na konci dne, po několika prezentacích.
- ✦ Používáme neuronové sítě, které se zaměřují na specifickou část signálu, která je nositelem emocí a dalších ukazatelů.



Real time

Audio file



Stop

WebRTC VAD	no_speech
Speech activity	no_speech
Gender	male (100%)
Language	czech (44%)
Age	seventiesplus (38%)
Cadence	2.2
Cadence NN	2.87 (slow)
Energy	55.7
SNR	21.3
Emotion	sad (94%)

Využití:

- ⊕ Základní identifikace mluvčího: dítě, dospělý, pohlaví?
- ⊕ Hovoří ve stresu? Je pod tlakem? Má strach?
- ⊕ Přizpůsobení komunikace:
 - ⊕ Emočnímu stavu dotyčného
 - ⊕ Kadenci hovoru

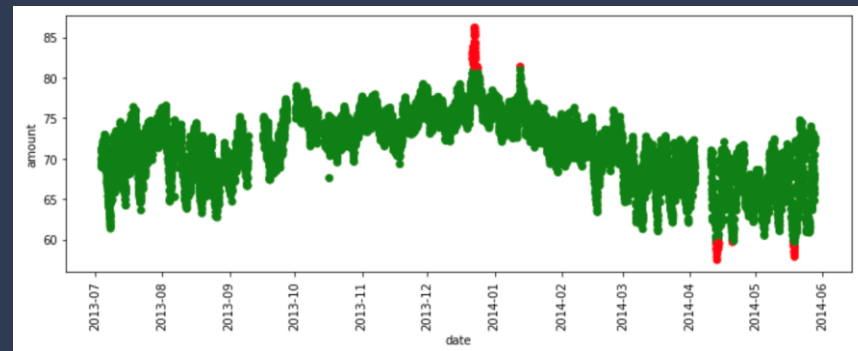
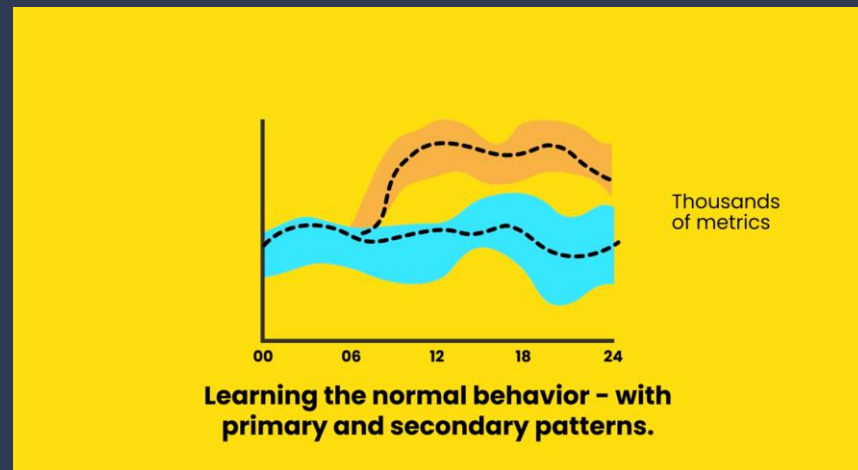


mAI0ps

Detekce anomálií

Detekce anomálií z časových řad

- mAI Ops má schopnost učit se ze signálů
- Umíme více přístupů:
 - Učíme se, co jsou anomálie pomocí detekce anomálií
 - Detekujeme anomálie tím, že se učíme, co je normální chování
- Využití:
 - Detekce nestandardního a potenciálně nebezpečného chování pomocí dat



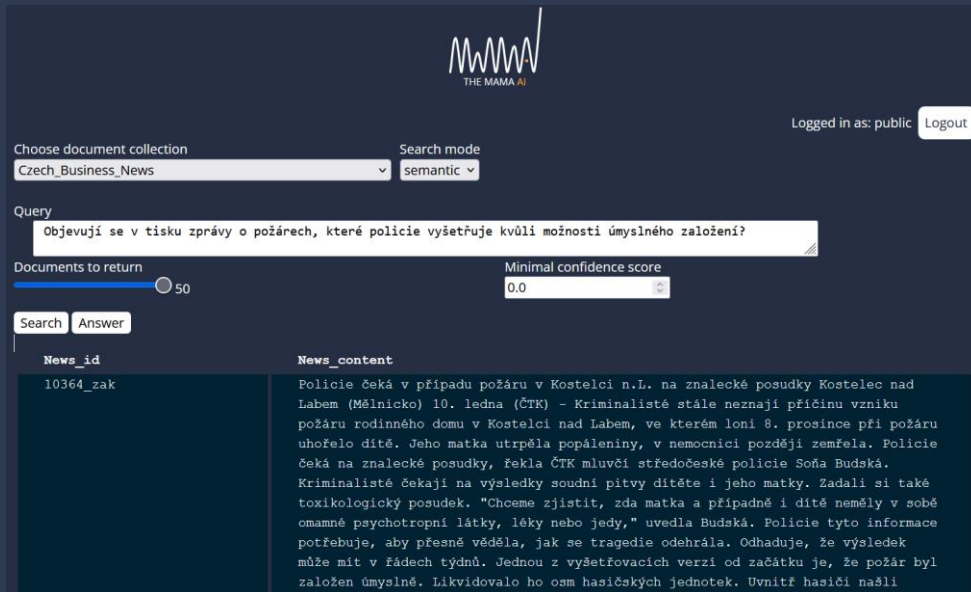


mSearch

Hledání odpovědí, nikoliv textu.

Vyhledávání napříč jazyky

- Zajímá vás, kde se ve spisech, článcích nebo v prepisech hovorů objevily zmínky o určitých tématech, které ale není možné specifikovat přesně?
- Hovory nebo články mohly být v různých jazycích. Není třeba hledat v každém jazyce specificky.
- A nalezených dokumentů může být hodně.



The screenshot shows a search interface with the following elements:

- Logo: THE MAMA AI (with a waveform icon)
- User status: Logged in as: public Logout
- Choose document collection: Czech_Business_News
- Search mode: semantic
- Query: Objevují se v tisku zprávy o požárech, které policie vyšetřuje kvůli možnosti úmyslného založení?
- Documents to return: 50
- Minimal confidence score: 0.0
- Buttons: Search Answer
- Table with columns: News_id, News_content

News_id	News_content
10364_zak	Policie čeká v případě požáru v Kostelci n.L. na znalecké posudky Kostelec nad Labem (Mělnicko) 10. ledna (ČTK) - Kriminalisté stále neznají příčinu vzniku požáru rodinného domu v Kostelci nad Labem, ve kterém loni 8. prosince při požáru uhořelo dítě. Jeho matka utrpěla popáleniny, v nemocnici později zemřela. Policie čeká na znalecké posudky, řekla ČTK mluvčí střeďočeské policie Soňa Budská. Kriminalisté čekají na výsledky soudní pitvy dítěte i jeho matky. Zadáli si také toxikologický posudek. "Chceme zjistit, zda matka a případně i dítě neměly v sobě omamné psychotropní látky, léky nebo jedy," uvedla Budská. Policie tyto informace potřebuje, aby přesně věděla, jak se tragédie odehrála. Odhaduje, že výsledek může mít v řádech týdnů. Jednou z vyšetřovacích verzí od začátku je, že požár byl založen úmyslně. Likvidovalo ho osm hasičských jednotek. Uvnitř hasiči našli

Objevují se v tisku zprávy o požárech, které policie vyšetřuje kvůli možnosti úmyslného založení?

Sumarizace nalezených článků pomocí LLM:

- Answer: V textu se objevují zprávy o několika požárech, které policie vyšetřuje. Jedním z nich je požár rodinného domu v Kostelci nad Labem, při kterém zemřelo dítě a jeho matka utrpěla popáleniny. Policie čeká na znalecké posudky a výsledky soudní pitvy, ale jednou z verzí od začátku je, že požár byl založen úmyslně. Dalším požárem je ten na skládce komunálního odpadu ve Vysoké Peci na Chomutovsku, která hořela podruhé za sedm měsíců. Hasiči zasahovali také při dalších požárech, které způsobily škodu, ale nikdo při nich nezemřel. Kromě toho se v textu objevuje informace o auditu na ministerstvu vnitra, který odhalil chyby při zadávání zakázek a některá zjištění jsou natolik závažná, že byla předána policii. Vyšetřování by se mělo týkat i ministra vnitra Radka Johna.

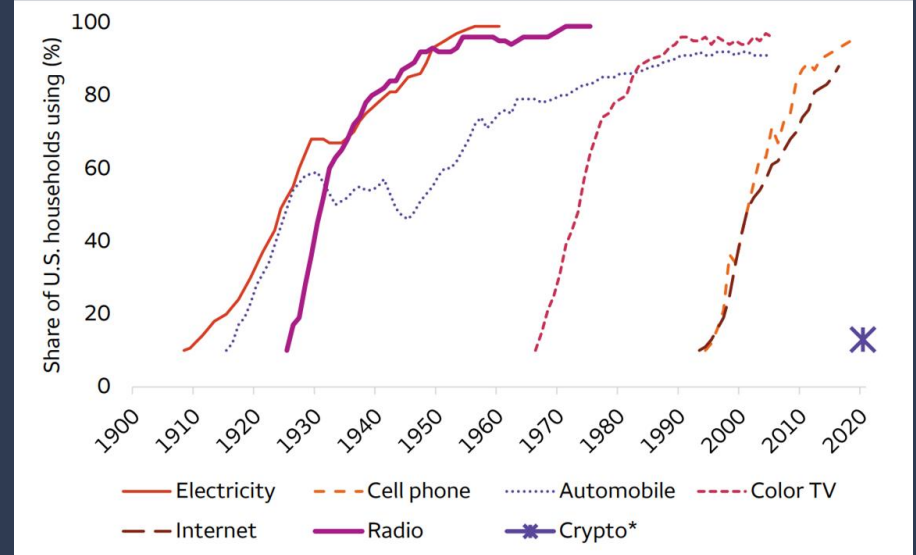
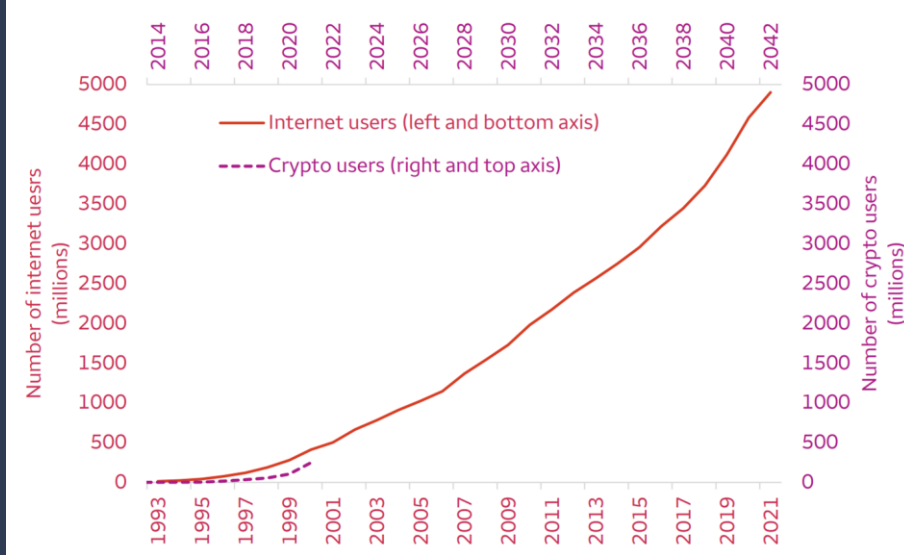
Využití: vyhledávání podobných situací ve spisech.



Web3? Krypto? Blockchain?

Nové technologie znamenají nová bezpečnostní rizika,
ale i možnosti, jak s nimi bojovat.

Web3? Krypto? Blockchain?



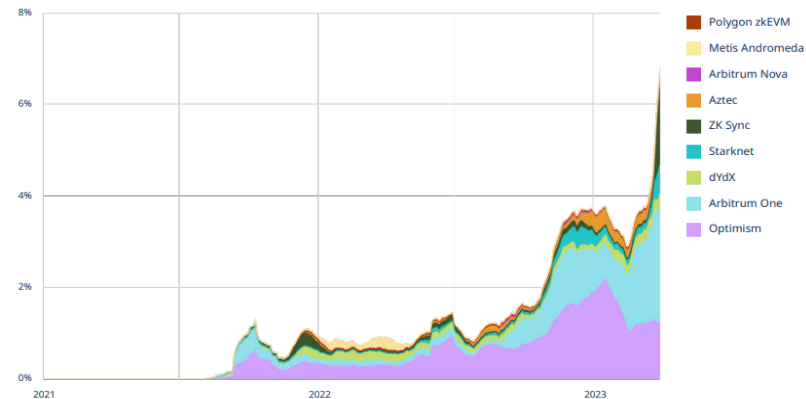
source: [Wells Fargo](#)

Je třeba se tím zabývat již teď?

Včera bylo pozdě.

Vznikají nové produkty, počet smart kontraktů roste.

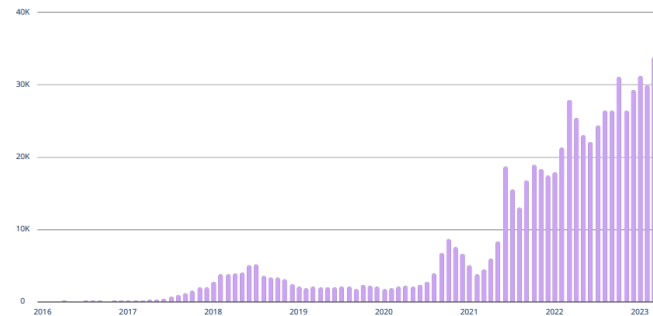
Fees paid by L2 rollups on Ethereum (% of all L1 fees, rolling 30D avg)



Verified smart contracts are at an all-time high, indicating a robust pipeline of product launches

Verified Smart Contracts

Number of smart contracts verified* during the month.



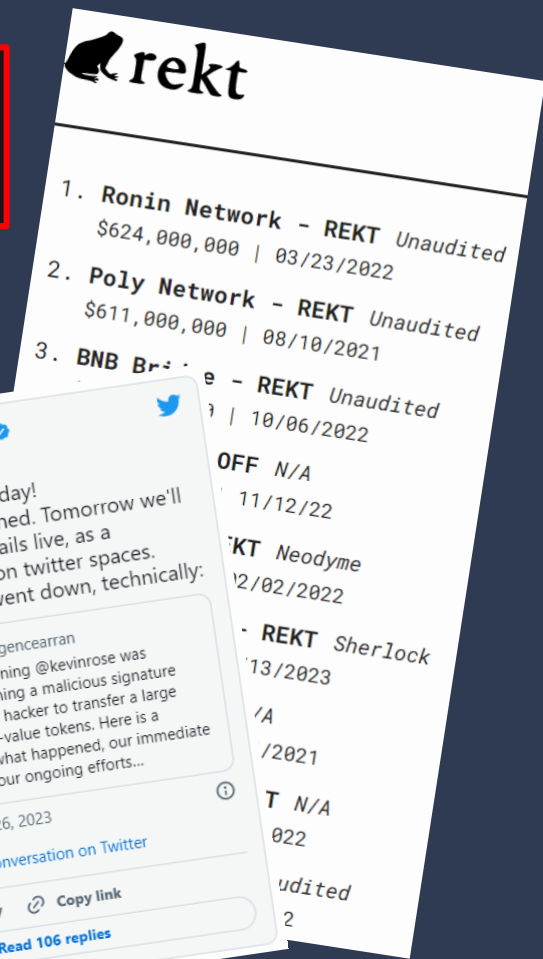
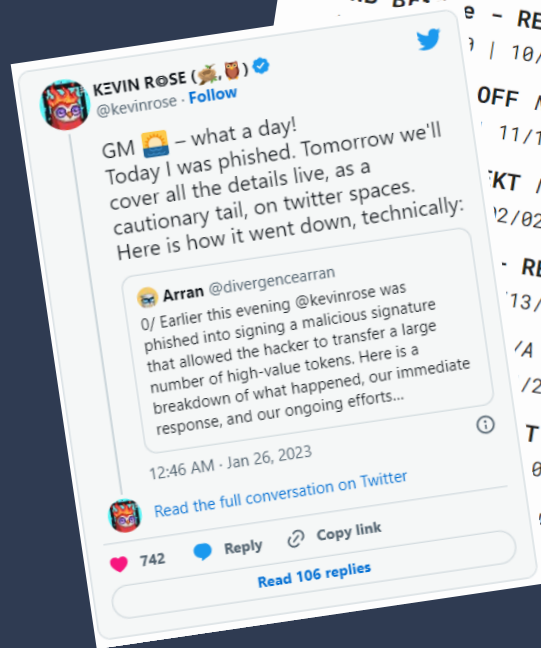
V čem je problém?

Total Value Hacked (USD)

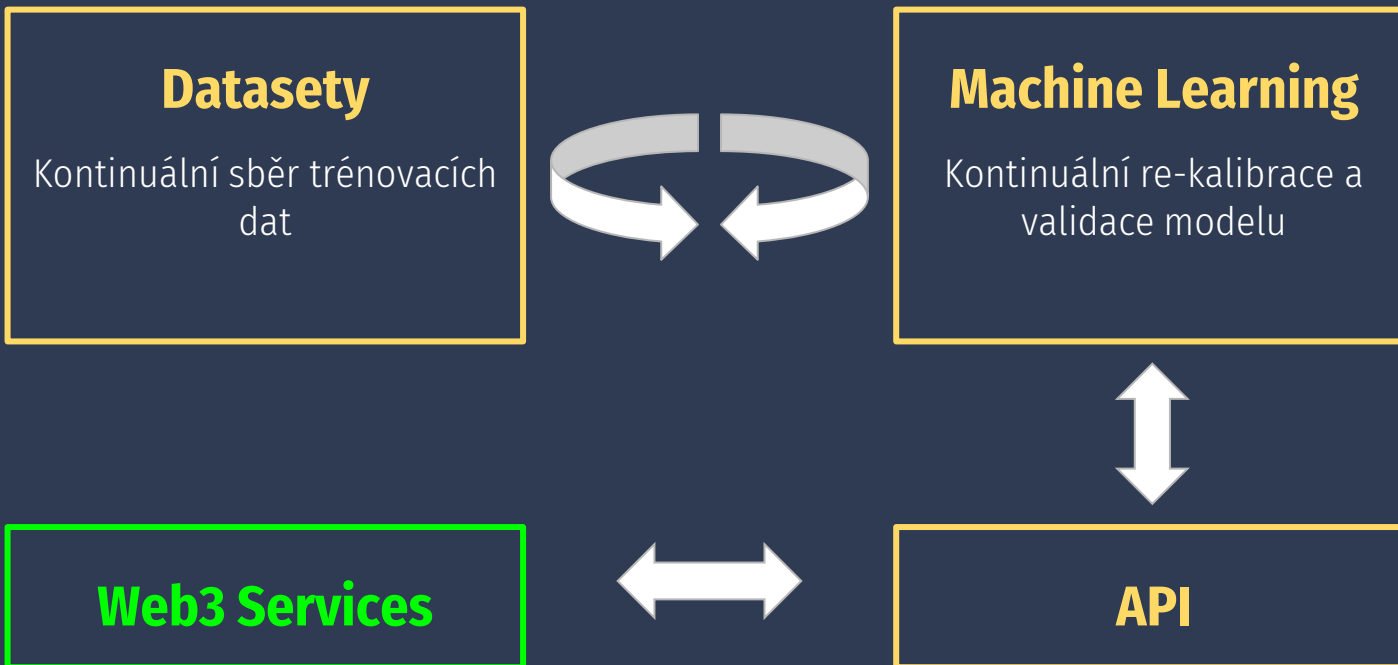
\$6.48b

Masivní přijetí krypta znamená nutnost škálovatelnosti, zlepšení UX a **bezpečnosti**.

- Phishingu mohou podlehnout i zkušení uživatelé
- Samotné DeFi protokoly mohou být předmětem hackingu
- Audit ještě neznamena bezpečnost



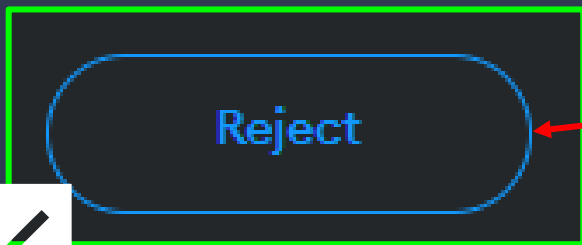
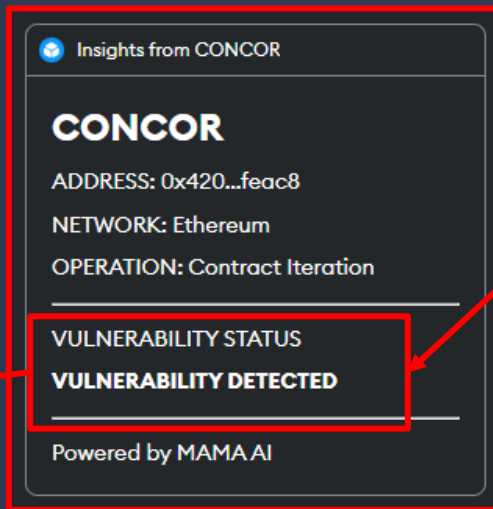
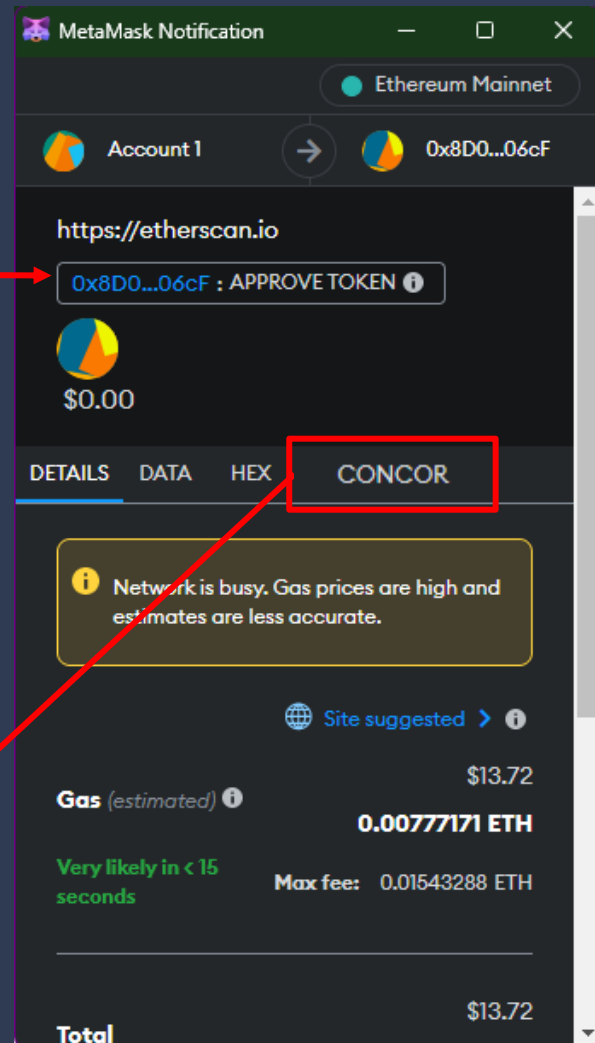
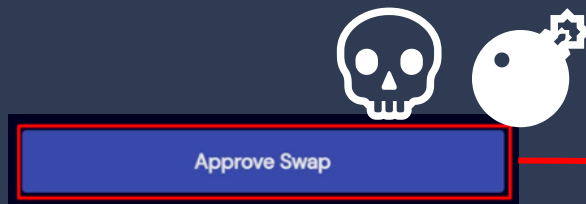
Jak využít strojové učení?



Řešení

Místo 

použít **ContractCortex (CONCOR)**

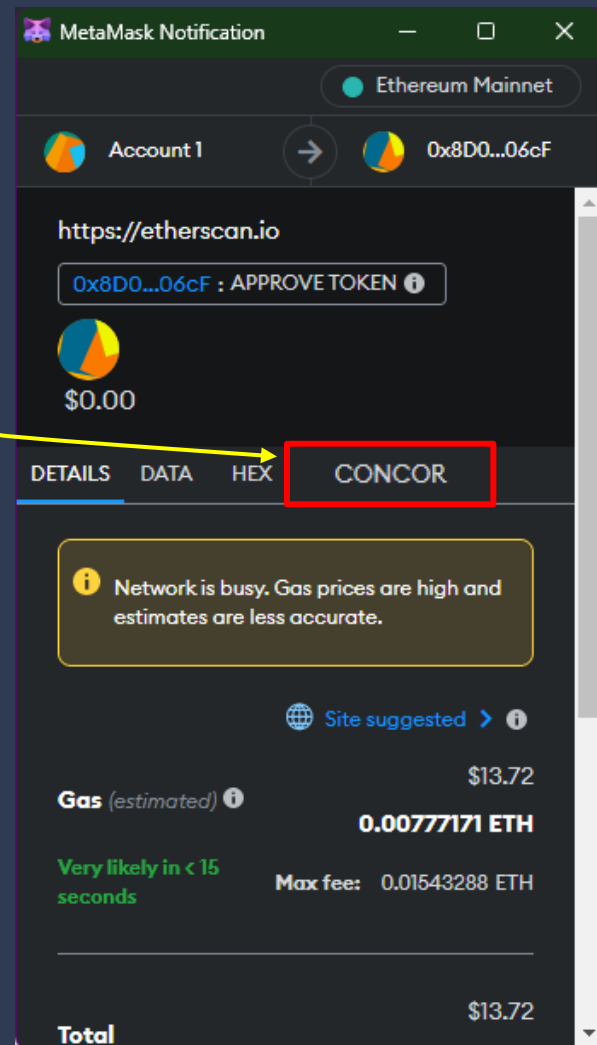


Řešení – aktuální stav

1. Fungující prototyp v Metamask: a ~~CONCOR~~ snap
2. Sběr dat zranitelných smart kontraktů
3. API na MAMA AI Cloudu pro klasifikaci zranitelnosti smart kontraktů

Využití:

Prevence trestné činnosti



Proč MAMA AI?

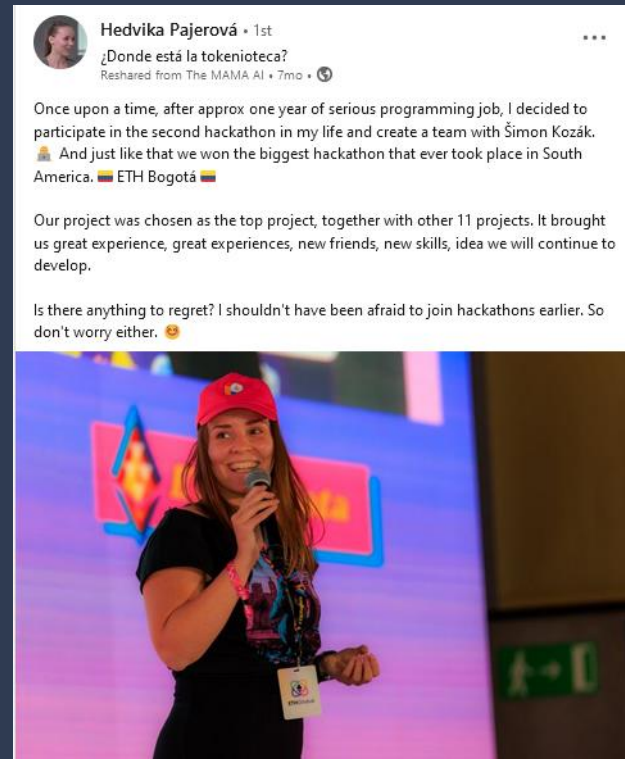


Naše zkušenosti s AI:

- 270 let ve výzkumu IBM,
- 80 let s Neural Networks a Deep Learning,
- 302 publikací, 95 patentů

Naše zkušenosti s web3:

- Vítězství v hackathonu (ETH Bogota),
- Akce, na kterých se podílíme (ETH Brno, Prague Blockchain Week, Security Meetup)





<https://themama.ai>
mama@themama.ai