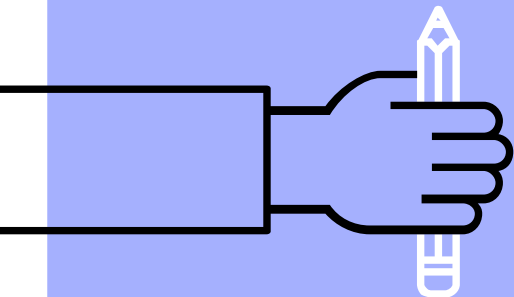
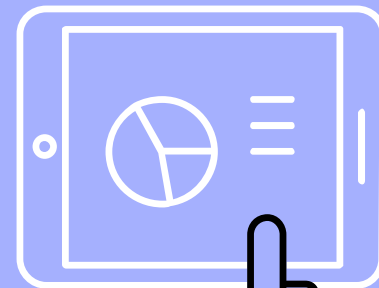
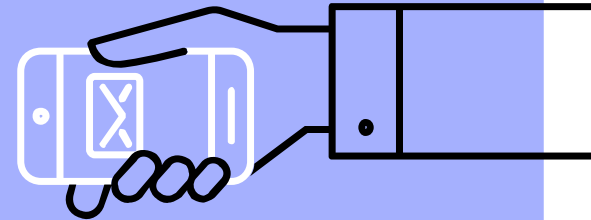
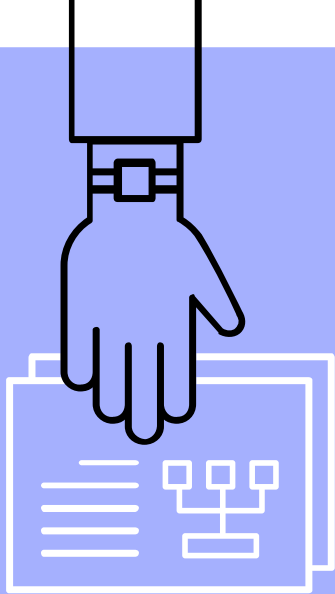


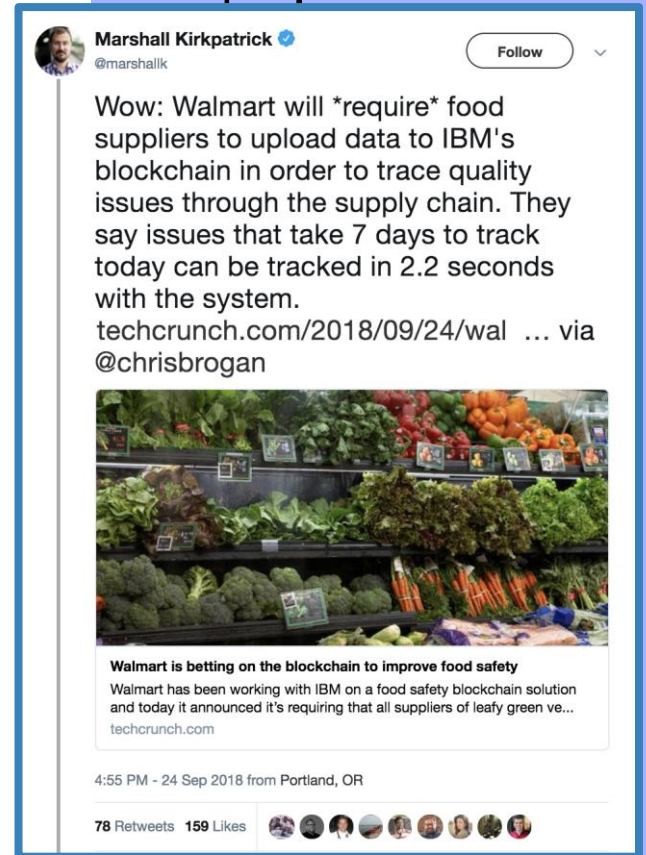
# Efektívny blockchain pre štátnu správu


[milan.pikula@nbu.gov.sk](mailto:milan.pikula@nbu.gov.sk)



# Nová doba a nové prísľuby


- ▶ dôveryhodnosť
- ▶ stabilita
- ▶ decentralizácia
- ▶ smart kontrakty



Marshall Kirkpatrick  [Follow](#)


[@marshallk](#)

Wow: Walmart will \*require\* food suppliers to upload data to IBM's blockchain in order to trace quality issues through the supply chain. They say issues that take 7 days to track today can be tracked in 2.2 seconds with the system.  
[techcrunch.com/2018/09/24/wal...](https://techcrunch.com/2018/09/24/walmart-requires-food-suppliers-to-use-ibm-blockchain/) ... via [@chrisbrogan](#)



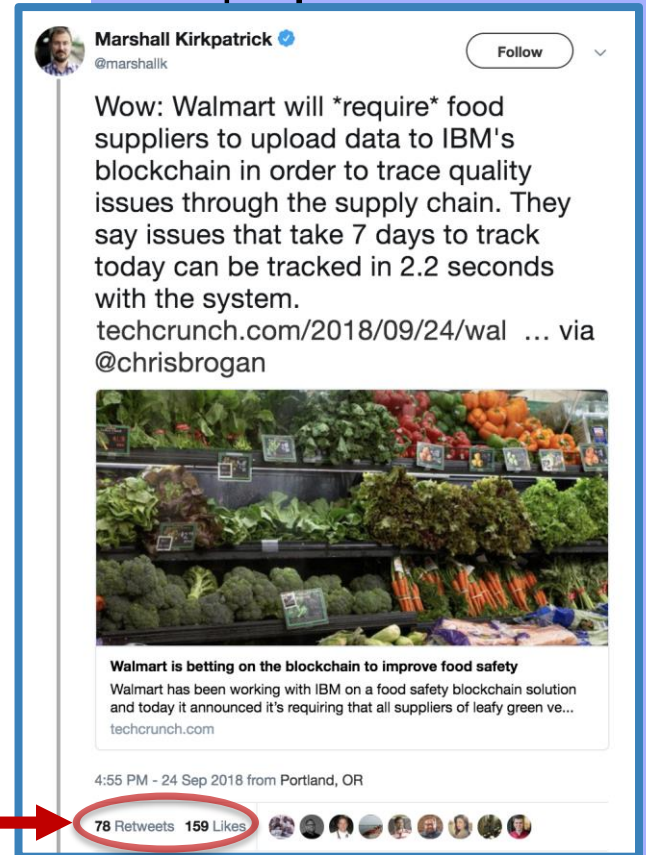
**Walmart is betting on the blockchain to improve food safety**  
Walmart has been working with IBM on a food safety blockchain solution and today it announced it's requiring that all suppliers of leafy green ve...  
[techcrunch.com](https://techcrunch.com)


4:55 PM - 24 Sep 2018 from Portland, OR

78 Retweets 159 Likes 


# Nová doba a nové prísľuby

- ▶ dôveryhodnosť
- ▶ stabilita
- ▶ decentralizácia
- ▶ smart kontrakty



Marshall Kirkpatrick  [Follow](#)

Wow: Walmart will \*require\* food suppliers to upload data to IBM's blockchain in order to trace quality issues through the supply chain. They say issues that take 7 days to track today can be tracked in 2.2 seconds with the system.  
[techcrunch.com/2018/09/24/wal...](https://techcrunch.com/2018/09/24/walmart-requires-suppliers-to-use-ibm-blockchain/) ... via @chrisbrogan



**Walmart is betting on the blockchain to improve food safety**  
Walmart has been working with IBM on a food safety blockchain solution and today it announced it's requiring that all suppliers of leafy green ve...  
[techcrunch.com](https://techcrunch.com)

4:55 PM - 24 Sep 2018 from Portland, OR

**78** Retweets **159** Likes

# Krutá pravda o novej dobe

- ▶ blockchain je **nová čivava**
- ▶ ... módna
- ▶ ... sexi
- ▶ ... nepochopená
  
- ▶ množia sa projekty
- ▶ **zatiaľ** plačú zodpovední vývojári



computer dipshit  
@davidcrespo

how is this different from making entries in a traditional database how is this different from making entries in a traditional database how is this different from making entries in a traditional database how is this different from making entries in a traditional database how is t

Marshall Kirkpatrick @marshallk  
Wow: Walmart will "require" food suppliers to upload data to IBM's blockchain in order to trace quality issues through the supply chain. They say issues that take 7 days to track today can be tracked in 2.2 seconds with the system. [techcrunch.com/2018/09/24/wal...](https://techcrunch.com/2018/09/24/wal...) via @christobrogan

Show this thread

8:04 AM - 25 Sep 2018

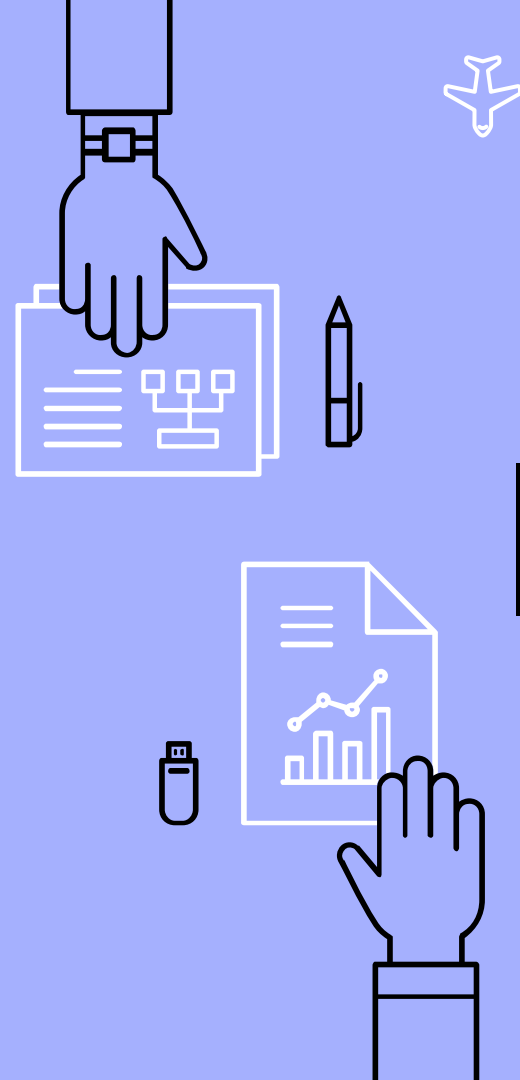
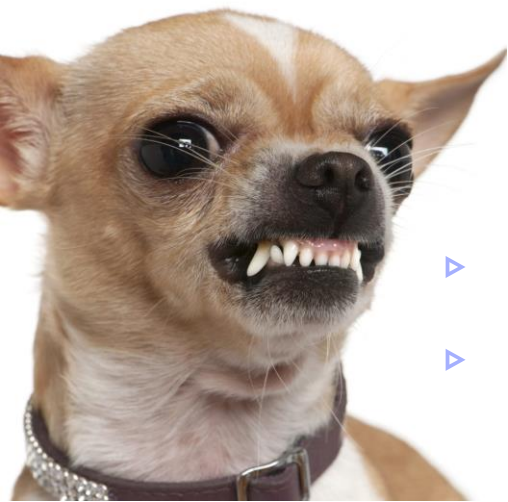
135 Retweets 356 Likes

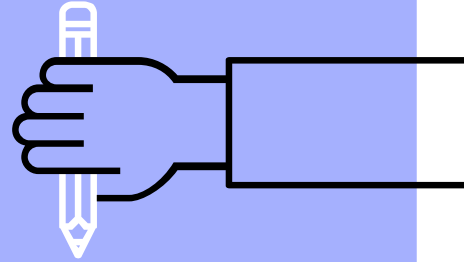
17 135 356

4

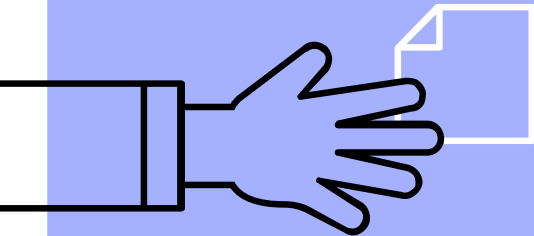
# Blockchain je...

- ▶ pomalý
- ▶ nebezpečný a nespořáhlivý
- ▶ drahý
  
- ▶ s malou kapacitou
- ▶ těžko pochopit a nepokazit.





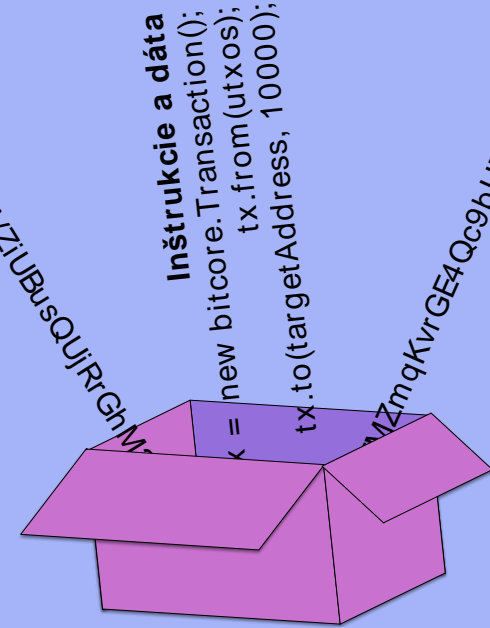
# Pochopme blockchain



Rýchly a nekorektný úvod do problematiky, ktorá si zaslúži týždeň.

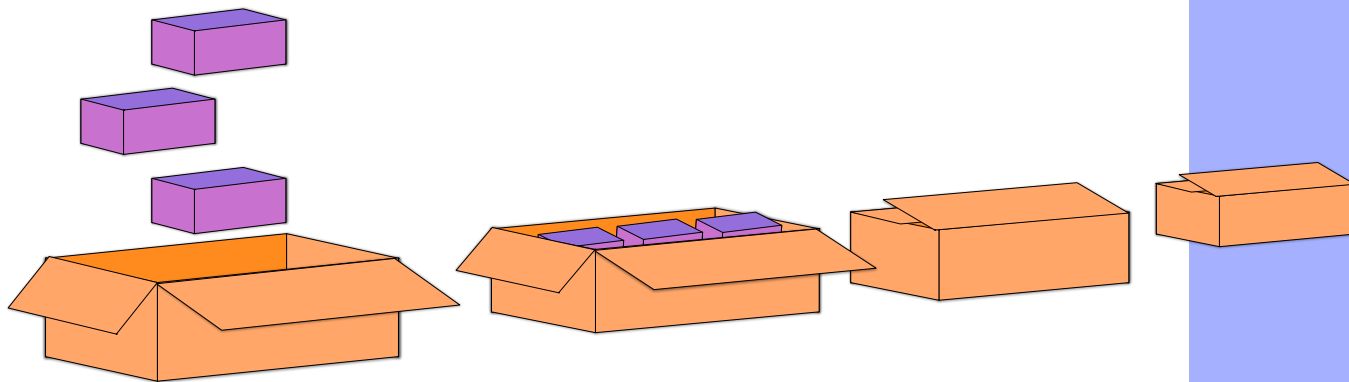
# 1. Adresa, kľúč a transakcia

- ▶ existuje **adresa** a možno aj iná adresa
  - ▶ často je adresa zároveň **verejný kľúč**
- ▶ z adresy na inú adresu môžem kopnúť tokeny, kryptomenu, ...
  - ▶ ak mám správny **privátny kľúč**
- ▶ toto je **transakcia**.



## 2. Blok a blockchain

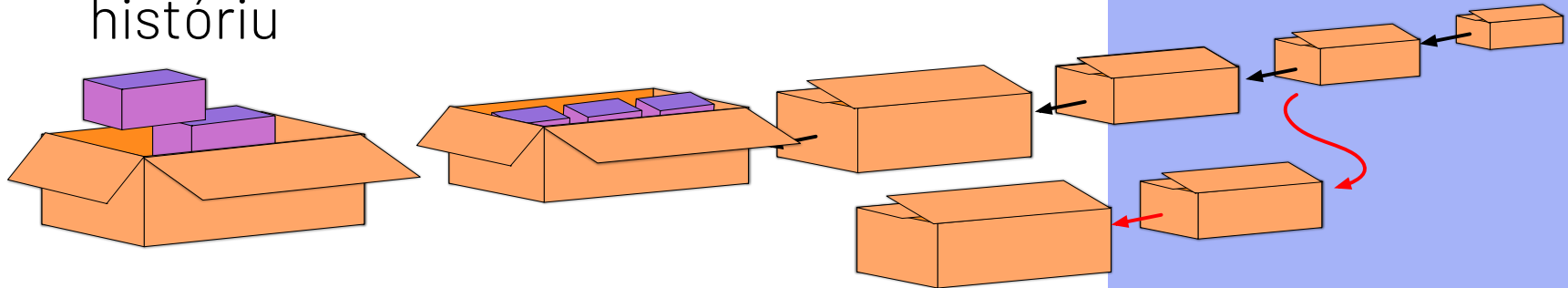
- ▶ **blockchain** je kniha tých transakcií
  - ▶ usporiadaných v **blokoch**,
  - ▶ ktorú vedie 30.000 ľudí... naraz.



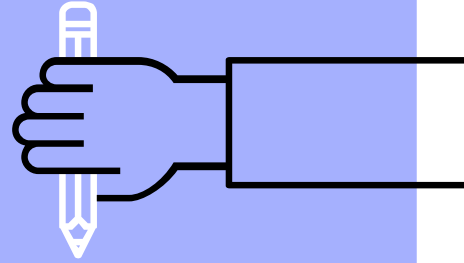
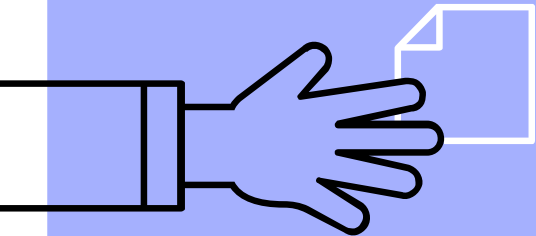


### 3. Ako sa robí dôveryhodnosť

- ▶ robí to veľa ľudí a ťaží sa veľmi, veľmi ťažko
- ▶ keď sa údaj "zahrabe" dosť hlboko, nikto nedokáže vyťažiť toľko, že prepíše históriu



Ale...



# Blockchain je **nebezpečný**

- ▶ Chcete robiť blockchain sami?
  - **riziko**: jednotky minerov je ľahké prebiť a zmeniť tak zapísanú históriu
  - **riziko**: sfaľujete dáta aj blockchain.  
Kto je **skutočný stakeholder**?
- ▶ Dôveryhodnosť fuč, rozpočet tiež.  
Použite verejný blockchain, kde sa to len dá!



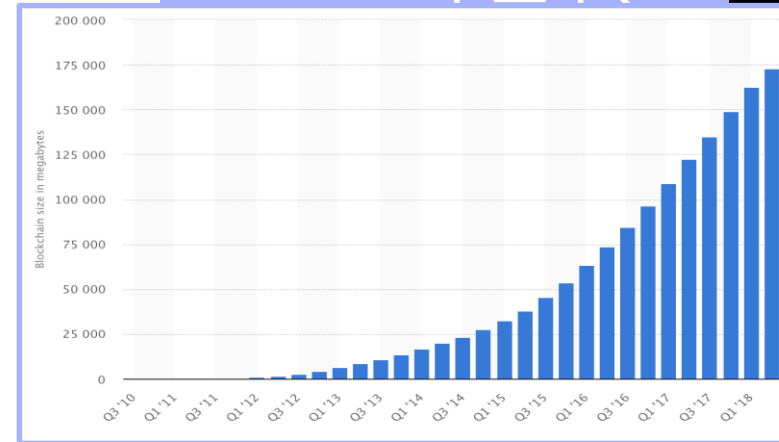
# Blockchain je **nebezpečný**

- ▶ **riziko**: transakcia sa pripíše... a zmizne
- ▶ **riziko**: smart kontrakt má chybu  
(The DAO - 50 mln US\$)
- ▶ **riziko**: ukradnú vám privátny kľúč  
(implementačná chyba, vírusy  
CryptoShuffler, ComboJack a ďalšie)
- ▶ Vyhnite sa detským chybám.  
Použite verejný blockchain!



# Zmestí sa doň **málo**

- ▶ blockchain musí držať celú históriu
  - lebo všetky dáta sú rovnako cenné
  - preto má krátke bloky (kB) a riadenú rýchlosť pripisovania blokov (minúty)
- ▶ blockchain je drahý na uloženie dát, idú tam len hashe. A hash takmer nikdy nie je citlivý. Použite...



# Blockchain je pomalý

- ▶ Transakcie sa pripíšu, len keď ktosi pridá nový blok
  - a to je raz za X minút
  - je veľa návrhov, dobré riešenie nie je
- ▶ Požadujete rýchlosť? Zabudnite na milisekundy.
- ▶ Použite... SQL alebo Elasticsearch! Na hashe DB verejný blockchain.



# Cvičenie

- ▶ Zvýšme dôveryhodnosť [data.gov.sk](https://data.gov.sk) ukladaním datasetov na blockchain
- ▶ Prvý nápad:
  - postavíme privátny blockchain
  - vo vládnom cloude
- ▶ Čo je na tomto návrhu zlé?



# Cvičenie

- ▶ Čo je na tomto návrhu zlé?
  - kto sú stakeholderi? Štát alebo spotrebiteľia dát?
  - privátny cloud stojí peniaze, dva krát
  - proof of...?
- ▶ zvyšuje vôbec dôveryhodnosť?
  - možno ho prepočítať od nuly, centralizovaný, potenciálne chyby





# Cvičenie

- ▶ Jednoduché riešenie
  - <https://github.com/milankowww/ckan2blockchain>
  - využíva existujúce CKAN API
  - ukladá hashe na verejný blockchain
  - vývoj: 4 MD
  - mesačné náklady: 4 EUR



“

*Jednoduché a efektívne  
riešenia existujú.*



# Efektívny blockchain pre štátnu správu

[milan.pikula@nbu.gov.sk](mailto:milan.pikula@nbu.gov.sk)

