

ako zmení blockchain dôveru v IT

Miroslav Pikus

*e*FOCUS



viera v softvér

- **najprv (v 90-tych rokoch) úplná**
- **teraz nulová**
 - 15 – 50 softvérových bugov na 1000 riadkov kódu (Steve McConnell)
 - (Windows má 50M riadkov, Firefox 16M riadkov)
 - 5 chýb per funkčný bod (Capers Jones)
- **nevyhnutnosť?**
 - SPARK, 250K riadkov, riadenie letovej prevádzky nad Anglickom

prečo sú diery

1. **agilita a čas dodania nadovšetko**
2. **nedajú sa otestovať *všetky* scenáre**
3. **bezpečnostných chýb je viac ako funkčných, lebo sa sústredí na funkčné**
4. **programuje hocikto a hocijako**

- + čulý obchod s 0-day
- + umelé security buggy
- + rozsiahla čierna aktivita nahráva súvislostiam
- + malá hárstka IT firiem

priority CIO

- 1. bezpečnosť**
- 2. kontinuálna prevádzka**
- 3. výkonnosť, kapacita**
- 4. nová funkcionality**
- 5. užívateľské požiadavky**

priority CIO

1. bezpečnosť
2. kontinuálna prevádzka
3. výkonnosť, kapacita
4. nová funkcionality
5. užívateľské požiadavky

spása v číslach

- **súkromie** – šifrovaním
- **overovanie identity** – digitálnymi podpismi a certifikátmi
- **integritu** – hešovaním a podpismi
- **neschopnosť poprieť udalosť** – podpisom odoslania správy či udalosti
- **nemožnosť nekontrolovane duplikovať informácie** – blockchainom
- **transparentnosť v práci s dátami** – blockchain

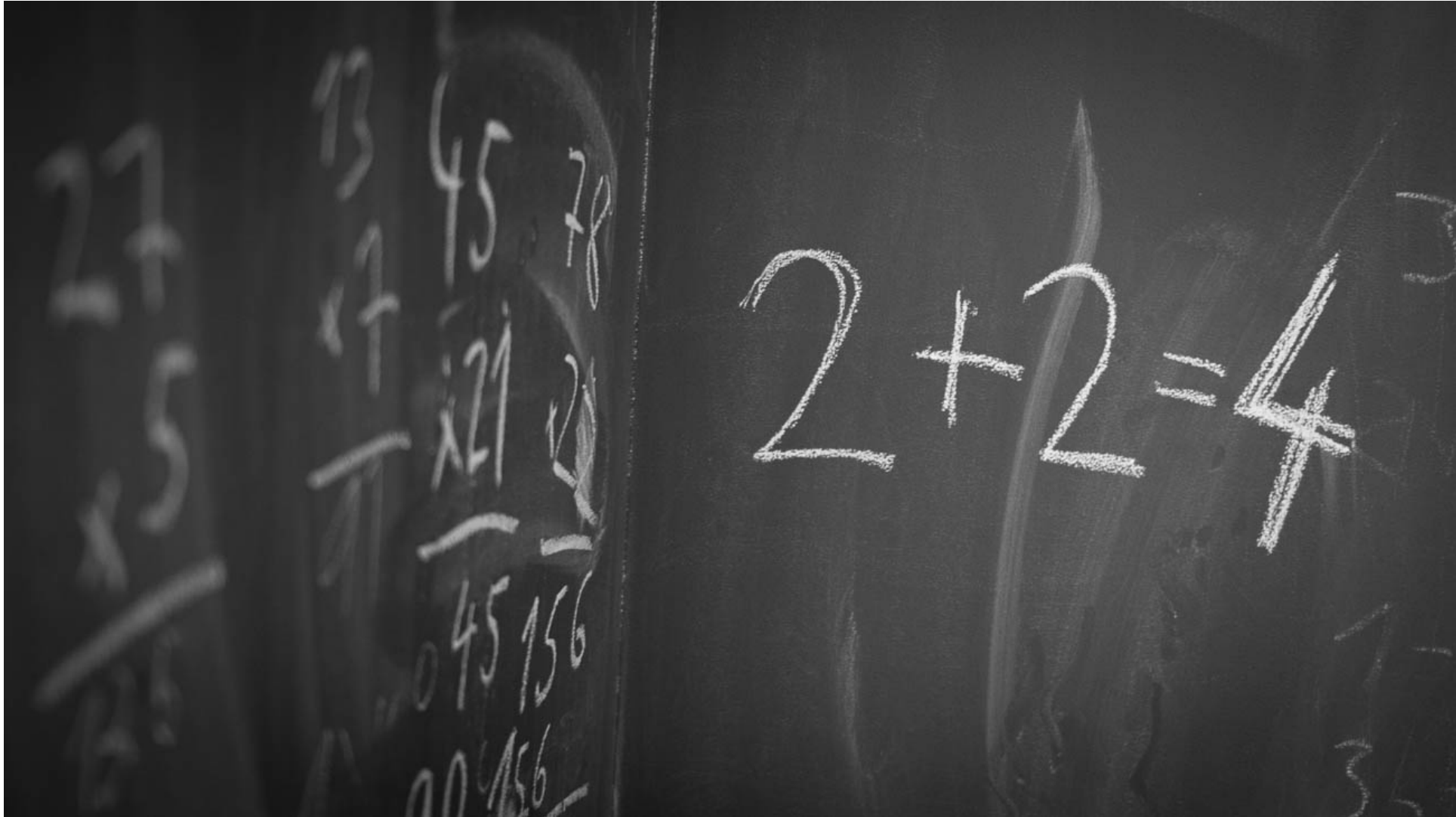
blockchain

- distribuovaná databáza chránená kryptografiou, ktorú neriadi centrálna autorita
- blockchain cloud?
- privátny blockchain – oxymoron?

spása v číslech



spása v číslach



Ďakujem za pozornosť

blog.hysteria.sk

miroslav.pikus@telekom.sk

