



# Blockchain - základy

UPVII a MF SR

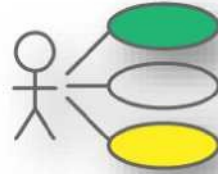
16. novembra 2018



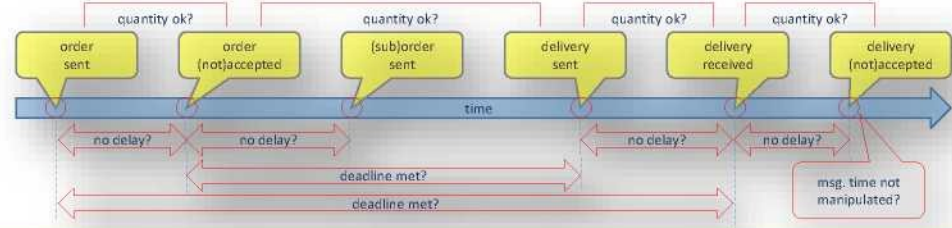
**EY**  
Building a better  
working world



1 Use case identification



2 Protocol design



3 Feasibility study / CBA



4 Working prototype



# EY prototyping tool

## Use case: Fighting mileage roll back fraud with Blockchain



<b>id_entity</b>	<b>id_occasion</b>
	01.1_car_registration
	01.2_car_accident
<b>01_police</b>	01.3_car_traffic_offense
	01.4_car_change
	01.5_car_deregistration
	<b>01.6_odometer_extract</b>
	02.1_emission_control
<b>02_control_station</b>	02.2_technical_control
	02.3_originality_control
<b>03_car_seller</b>	03.1_car_purchase
	03.2_car_sale
	04.1_regular_inspection
<b>04_car_service</b>	04.2_car_reparation
	04.3_tire_change_winter
	04.4_tire_change_summer
<b>05_other</b>	05.1_car_wash
	05.1_hotel_service
	05.3_other_service

### Use case key principles & rules:

- Records (events) are independent, i.e. no need for any logical relation between records The VIN code (unique vehicle ID) is potentially confidential => will be encrypted with public key of the "01\_police" user
- Special event "01.6\_odometer\_extract" is generated by the "01\_police" user; e.g. upon off-chain request and after payment of specific administrative fee
- The "01.6\_odometer\_extract" event records the maximum odometer value (km) for specific VIN (VIN code is not encrypted) recorded in the blockchain ledger and its note indicates if rollback fraud was detected
- Rollback is detected if: **(when\_taken.1 < when\_taken.2) and (km.1 > km.2)**
- The "01\_police" user can issue a detailed official report with the odometer reading history for specific VIN code
- The above can also be used as a generic "vehicle history" report since the records can contain different descriptions and notes
- Public can perform different statistical queries on the blockchain ledger (excluding the "what\_vin" and "how\_meny" data)

<b>id vehicle categ</b>	<b>id district</b>
01_L	BA_SK
02_M	BB_SK
03_N	BE_DE
04_O	KE_SK
05_T	MI_IT
...	...

entity identification and authentication via asymmetric crypto

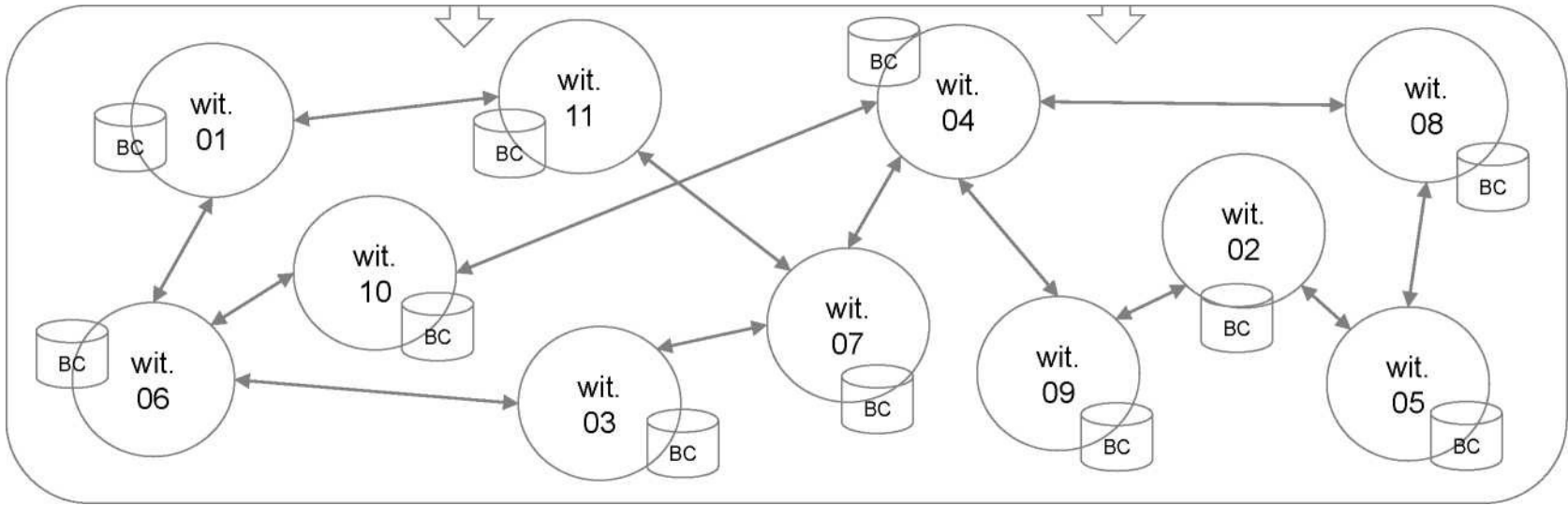
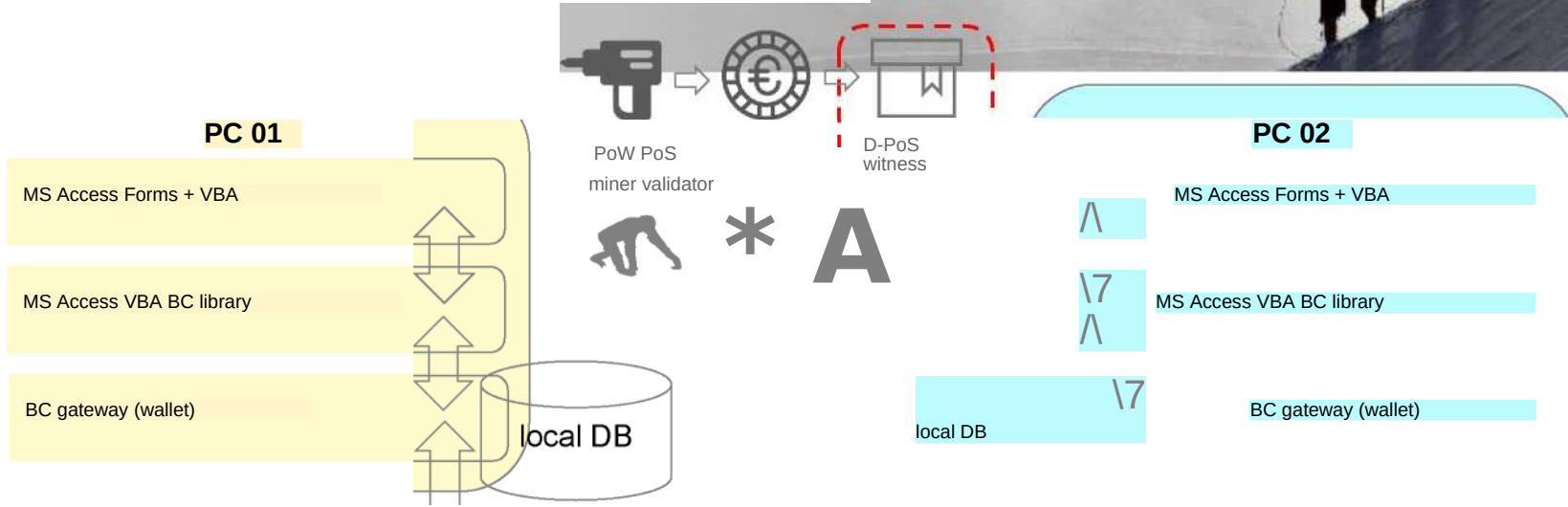
encrypted with public key of the "01 police" user

evidence document (e.g. photo of vehicle's dashboard with odometer) remains off-chain; only hash of the photo is stored on blockchain

blockchain ledger - sample records

id event	when taken	who took	why taken	what vin	what category	where taken	how many	evidence	notes
0001a	10.10.2017 09:14:59	03_car_seller	03.2_car_sale	WDB2030071 if 735126	02_M	MI_IT	3 500	[hash of dashboard.jpg]	sale of a demonstrator 1 vehicle
0002a	23.09.2018 11:10:05	04_car_service	04.1_regular_in spection	WDB2030071A 735126	02_M	BA_SK	15 000	[hash of dashboard.jpg]	oil and oil filter replacement
				<P					

# EY prototyping tool Architecture



# EY prototyping tool

## Fighting mileage roll back fraud with Blockchain



Odometer in Blockchain v2018-09-16 [a]

Filter: User: 01\_police Schema: uc\_odo\_event:1.0.0

Buttons: All records, My Records, Selected VIN

Records

ID	When	Who	Why	What VIN	What category	Where	KM	Evidence hash	
000	01.01.1111 00:00:00						0		Initiation
0009a	25.09.2018 16:24:49	02_control_station	02.1_emission_control	WDB2030071A735126	02_M	BA	23 400		
0009a	27.09.2018 17:21:54	02_control_station	02.2_technical_control	7b22056e63727970746564496e	02_M	BA	270 000	frcs120b5ddc52e912b6fe1a	linked dc
0010a	27.09.2018 17:24:16	01_police	01.6_odometer_extract	7b22056e63727970746564496e	02_M	n/a	12		rollback f
0011a	27.09.2018 17:24:52	01_police	01.6_odometer_extract	7b22056e63727970746564496e	02_M	n/a	270 000		rollback f
0012a	29.09.2018 08:55:54	01_police	01.6_odometer_extract	7b22056e63727970746564496e	02_M	n/a	270 000		rollback f
0013a	29.09.2018 08:57:45	01_police	01.6_odometer_extract	7b22056e63727970746564496e	02_M	n/a	270 000		rollback f
0014a	29.09.2018 08:58:33	01_police	01.6_odometer_extract	WDB2030071A735126	02_M	n/a	270 000		rollback f
0015a	29.09.2018 14:41:23	01_police	01.2_car_accident	7b22056e63727970746564496e	02_M	BR	1 234		
0016a	29.09.2018 14:46:43	01_police	01.4_car_change	7b22056e63727970746564496e	02_M	BB	13 241 234		
0017a	29.09.2018 14:52:37	01_police	01.6_odometer_extract	WDB2030071A735126	02_M	n/a	13 241 234		rollback f
0018a	29.09.2018 14:52:54	01_police	01.6_odometer_extract	WVGZZZ7L260652028	02_M	n/a	1 234		rollback f
0019a	29.09.2018 19:15:54	01_police	01.3_car_traffic_offense	7b22056e63727970746564496e	02_M	BB	14		
0020a	10.10.2018 12:11:42	01_police	01.2_car_accident	7b22056e63727970746564496e	02_M	BA_SK	45 000	a01f32a0c1f0876485948d1	linked dc

Odometer in Blockchain, v2018-09-16

### Fighting mileage roll back fraud with Blockchain

EY, 2018, All rights reserved

EY Building a better working world

View record

Details

Record ID: 0009a

When: 27.09.2018 17:21:54

Who: 02\_control\_station

Why: 02.2\_technical\_control

What VIN: WDB2030071A735126

What category: 02\_M

Where: BA

KM: 270 000

Evidence hash: frcs120b5ddc52e912b6fe1a1e6e8304f1e873d5298a52c9c4ff1b28fd1b75d8f743b6918de32bf017cd74ba13bb272b1de7101b15a70464ae87376031bed459

Note: linked document: mercedes\_mza\_267719.jpg

Signature: GynQz2BvnyOjB9FXWUjCQnoC3abkxnlUR73BRWwB0F2Bc22436+OHe12Non7L95prQh=FBUca0i1FWvJ8-

Decision: Confirm action

Blockchain monitor

Transactions of application [Odometer in Blockchain v2018-09-16] and schema [uc\_odo\_event:1.0.0]

uc_id	uc_when	uc_who	uc_why	uc_what_vin	uc_what_category	uc_when
000	01.01.1111 00:00:00					
0009a	25.09.2018 16:24:49	02_control_station	02.1_emission_control	WDB2030071A735126	02_M	BA
0009a	27.09.2018 17:21:54	02_control_station	02.2_technical_control	7b22056e63727970746564496e	02_M	BA
0010a	27.09.2018 17:24:16	01_police	01.6_odometer_extract	7b22056e63727970746564496e	02_M	n/a
0011a	27.09.2018 17:24:52	01_police	01.6_odometer_extract	7b22056e63727970746564496e	02_M	n/a
0012a	29.09.2018 08:55:54	01_police	01.6_odometer_extract	7b22056e63727970746564496e	02_M	n/a
0013a	29.09.2018 08:57:45	01_police	01.6_odometer_extract	7b22056e63727970746564496e	02_M	n/a
0014a	29.09.2018 08:58:33	01_police	01.6_odometer_extract	WDB2030071A735126	02_M	n/a
0015a	29.09.2018 14:41:23	01_police	01.2_car_accident	7b22056e63727970746564496e	02_M	BR
0016a	29.09.2018 14:46:43	01_police	01.4_car_change	7b22056e63727970746564496e	02_M	BB
0017a	29.09.2018 14:52:37	01_police	01.6_odometer_extract	WDB2030071A735126	02_M	n/a
0018a	29.09.2018 14:52:54	01_police	01.6_odometer_extract	WVGZZZ7L260652028	02_M	n/a
0019a	29.09.2018 19:15:54	01_police	01.3_car_traffic_offense	7b22056e63727970746564496e	02_M	BB
0020a	10.10.2018 12:11:42	01_police	01.2_car_accident	7b22056e63727970746564496e	02_M	BA_SK

Witness activity

Blocks interval loaded

First block: 1 487 388

Last block: 1 795 066

Blocks count: 307 678

Blocks per TX: 21 977,00

Blocks / min: 12

Transactions confirmed

TX from: 22.9.2018 14:47:20

TX to: 10.10.2018 10:11:50

TX days: 17,81

TX count: 14

TX per block: 0.000046

Status: [Green dot]

Actions: Selected record: 1 / 14, Blocks to reload: 1 440

EY logo

# Čo je blockchain?

Bitcoin?

Cryptocurrency?

Chain of blocks?

Distributed database?



# Základné stavebné bloky blockchainu

## Kryptografická HASH funkcia

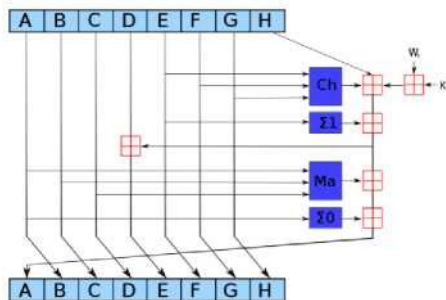


- ▶ Hash je jednosmerná funkcia, ktorá zo vstupného reťazca akejkol'vek dĺžky vypočíta výstupný (obvykle krátky) reťazec fixnej dĺžky
- ▶ Podobné, ale nevyhovujúce: parita, CRC, MD5, obvykle používané: SHA256
- ▶ HASH viem rýchlo vypočítať, ale z daného HASHu nevieme vypočítať aký bol vstupný text
- ▶ Iný vstup produkujúci rovnaký HASH viem teoreticky vypočítať, ale len s extrémnym výpočtovým výkonom, no nájdený vstup nebude dávať zmysel
- ▶ Malá zmena vstupu (napr. 1 bit) spôsobí veľkú zmenu HASHu:

```

abc © EDEAAFF3F1774AD2888673770C6D64097E391BC362D7D6FB34982DDF0EFD18CB abC ©
CD655CE2BE7D42A0D7255326DAFDE8F87F17DF5131247819F715D9223FEF2662 ab c ©
D1BCD337B7A3F564F38AFC5888A638A30343398FD686580628C480EED0354CB9
  
```

- ▶ V blockchaine slúži obvykle na previazanie blokov blockchainu, ich zabezpečenie proti zmene, pre PoW výpočet alebo uloží krátky odtlačok súboru, kedy samotný súbor je uložený off-chain



$$Ch(E, F, G) = (E \oplus F) \oplus (\sim E \wedge G)$$

$$Ma(j4, B, C) = (A \oplus B) \oplus (A \oplus C) \oplus (B \oplus C)$$

$$E_0(v4) = (43g > 2) \oplus (A \wedge 13) \oplus (4 \wedge 22)$$

$$(E) - (F \wedge 6) \oplus (E \wedge 11) \oplus (E \wedge 25)$$

The bitwise rotation uses different constants for SHA-512. The given numbers are for SHA-256.

The red **ffl** is addition modulo  $2^{32}$  for SHA-256, or  $2^{64}$  for SHA-512

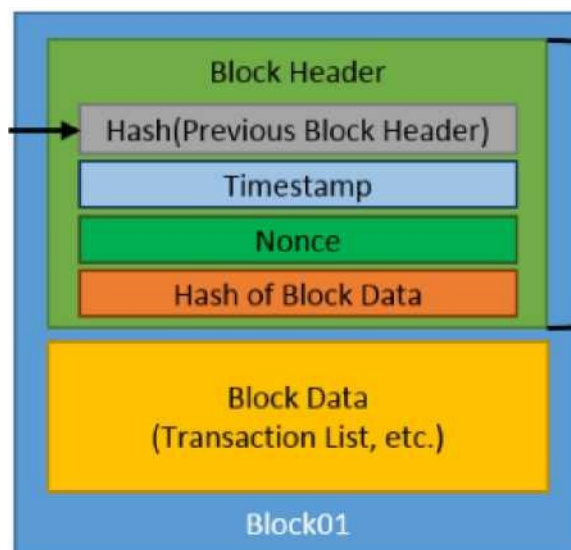


# Základné stavebné bloky blockchainu

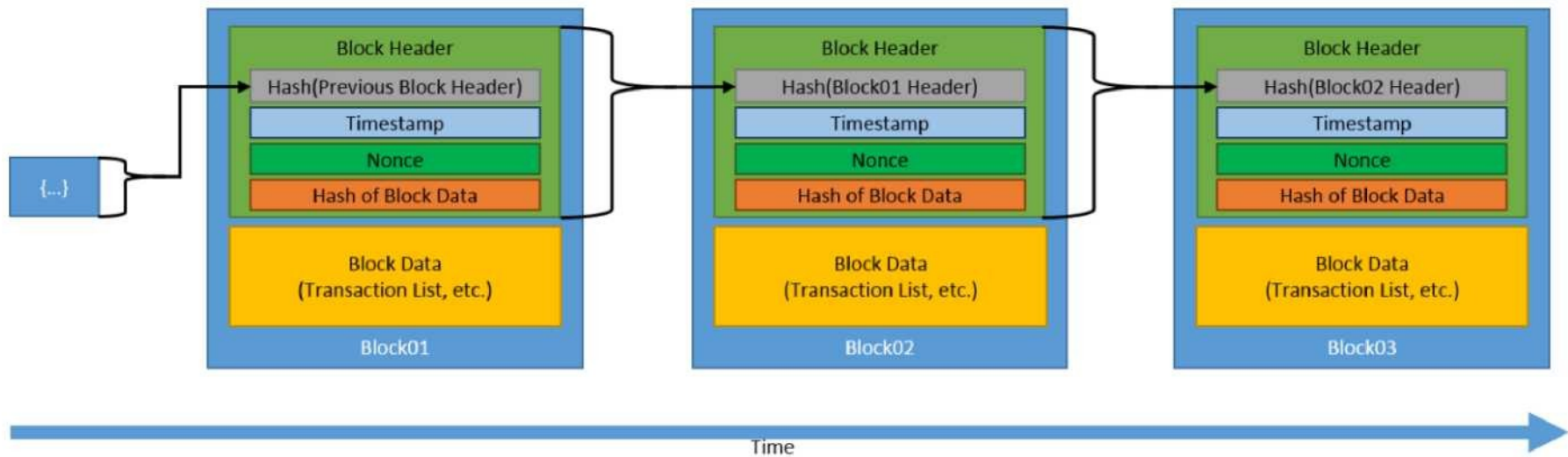
## Blok



- ▶ Blok vzniká periodicky (aj prázdny) vždy presne danom čase pre každý blockchain (Bitcoin 10 minút, moderné blockchajny aj 10 sekúnd)
- ▶ Obsahuje hlavičku a samotné transakcie za dané časové obdobie
- ▶ Hlavička obsahuje časovú známku, HASH predchádzajúceho bloku a HASH uložených transakcií



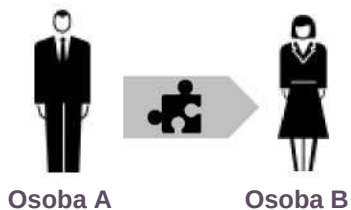
# Blockchain ako Merkle tree



# Ako vzniká blockchain



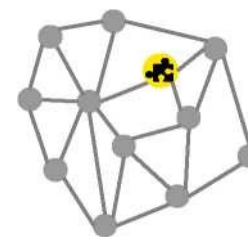
Vznik transakcie, ktorú chceme zapísať do blockchainu



Transakcia je zaslaná niektorému z uzlov siete; tento ju pošle ostatným uzlom; transakcie za daný čas sú zoskupené do bloku



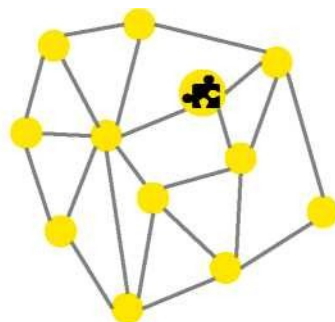
Uzly overia transakcie v aktuálnom bloku. Pomocou dohodnutého konsenzuálneho algoritmu sa vyberie 1 uzol, ktorý zostaví nový blok a získa za to odmenu.



Potvrdenie o zapísaní transakcie



Všetky uzly dostanú nový blok a zaradia si ho do svojej kópie blockchainu

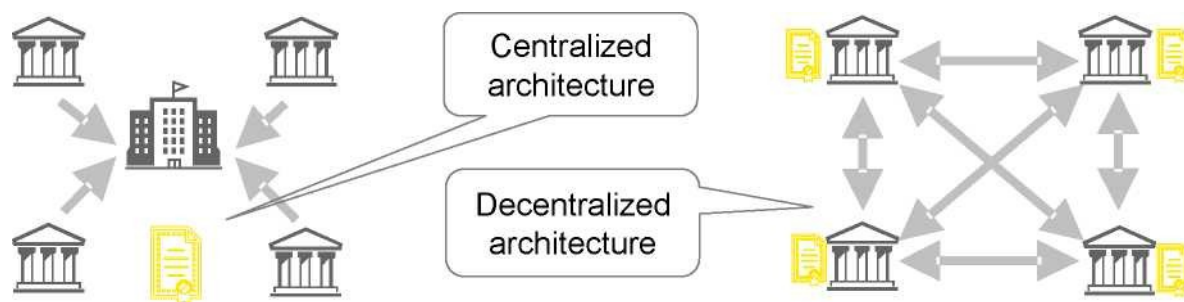


Nový blok sa pridá na koniec blockchainu a odošle sa ostatným uzlom

# Čo je blockchain



- ▶ Blockchain je distribuovaná databáza rozumne zvolených malých záznamov (transakcií, správ alebo udalostí)
- ▶ Záznamy sú uožené do kryptograficky prepojených blokov a tým sú chránené pred zmenením alebo zmazaním
- ▶ Nový blok je replikovaný na všetky uzly siete
- ▶ Blockchainová sieť tým týmto zabezpečuje dostupnosť, autentickosť a nepopierateľnosť uložených dát a nastoľuje všeobecnú dôveru
- ▶ Dáta sú viditeľné všetkých užívateľom siete, niektoré však môžu byť chránené šifrovaním
- ▶ Užívatelia sa jednoznačne zhodnú na autenticite a pravdivosti záznamov v blockchaine bez potreby centrálnej autority (sudcu, arbítra)
- ▶ Ďalšie potrebné dáta, ktoré nechceme uložiť do blockchaine z dôvodu dôvernosti alebo veľkosti, môžu byť uložené off-chain a v blockchaine len ich HASH a tým zabezpečiť nepopierateľnosť



# Blockchain - ďalšie témy



- ▶ Konsenzuálne algoritmy - PoW, ine PoS a

## Proof of Work vs Proof of Stake

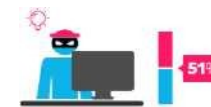
- ▶ Kryptomeny a tokenizácia assetov

- ▶ SMART contracts - Ethereum, 2015

- ▶ Zero knowledge proof

it'ZZ fl

proof of work is a requirement to define on expensive Computer calculation. also c a U e d mining



A reward is given to the first miner who solves each blocks problém.

Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth. a/so defined as stake.



The PoS system there is no block reward. so. the miners take the transaction fees.

m

Network miners compete to be the first to find a solution for the mathematical problem

\*T

Proof of Stake currencies can be several thousand times more cost effective.

# Information security in Blockchain

## Decentralised vs centralised processing



Are audited data:

- **C**omplete?
- **E**xisting?
- **A**ccurate?



We have to ensure:

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

Asymm. encryption

		<b>D</b>	<b>O</b>	<b>C</b>	<b>I</b>
Authentic Non repudiable Immutable	<b>C</b>	✓	X X	n/a	✓
	<b>I</b>	✓	✓	✓	✓
Permanent Redundant Fast	<b>A</b>	✓	n/a	X	n/a

I need solution:

- Fast
- Cheap
- No 3<sup>rd</sup> party



BC  
inventor  
|| p

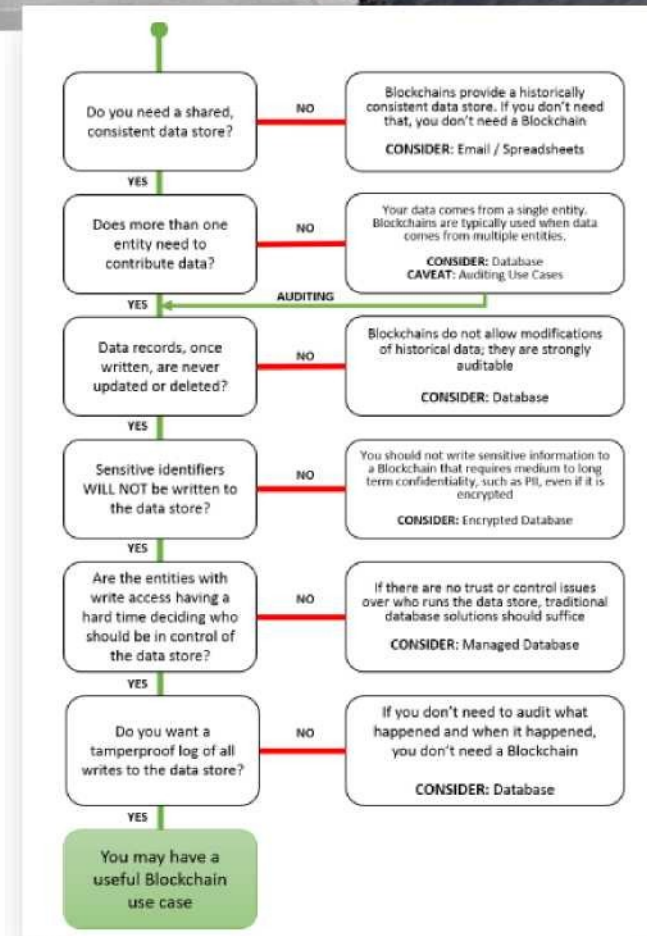
My solution leads to:

- **D**istributed • **O**pen
- **C**onsensual
- **I**mmutable

# When to use blockchain

## Typical "symptoms"

- ▶ When it is necessary to maintain and track important transactions or events in a **transparent, reliable, permanent and incontestable manner**
- ▶ When a reliable **audit trail** or time stamp are needed with respect to records of these transactions or events
- ▶ When the data in question is **generated and shared by several organizations** (entities who do not share information system)
- ▶ When organizations do not plan to use a **central trustworthy authority** for the purposes above.



Blockchain Technology OverView  
NISTIR 8202: <https://nvlpubs.nist.gov>





**Questions?**



# Contact



**EY**

**Žižkova 9**

**811 02 xxxxx**

**+421 2 3333 9111**

**[ev@sk.ev.com](mailto:ev@sk.ev.com)**

**[ey.com/sk](http://ey.com/sk)**



The information contained in this presentation is intended to provide general guidance. It is not intended to replace the specific advice which should be sought from an appropriate professional advisor before taking any particular course of action.

## **EY | Assurance | Tax | Transactions | Advisory**

### **About EY**

**EY is a global leader in assurance, tax, transaction and advisory Services. The insights and quality Services we deliver help build trust and confidence in the Capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.**

**EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide Services to clients. For more Information about our organization, please visit [ey.com](http://ey.com).**

**© 2018 EYGM Limited.  
All Rights Reserved.**

**[ey.com/sk](http://ey.com/sk)**

