Blockchain - základy

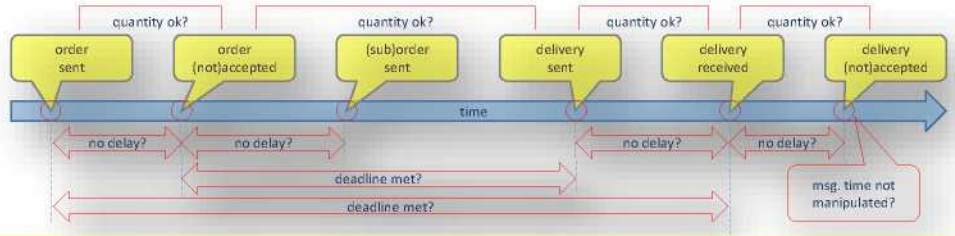
UPVII a MF SR

Building a better working world

EY Serveices

1 Use case identification

2 Protocol design



3 Feasibility study / CBA

4 Working prototype

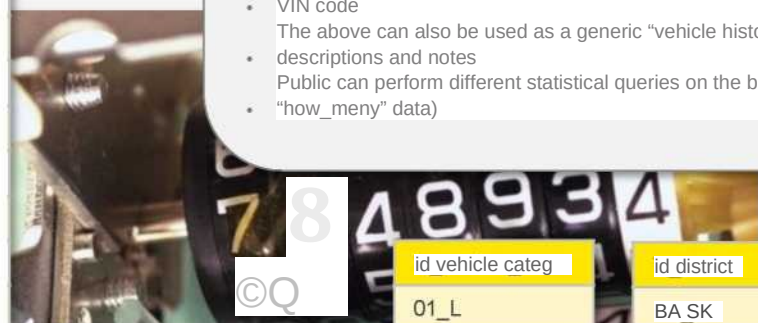
EY prototyping tool

Use case: Fighting mileage roll back fraud with Blockchain

id_entity	id_occasion
01_police	01.1_car_registration
	01.2 car accident
	01.3 car traffic offense
	01.4_car_change
	01.5_car_deregistration
	01.6 odometer extract
	02.1 emission control
02 control station	02.2 technical control
	02.3_originality_control
03 car seller	03.1_car_purchase
	03.2 car sale
04 car service	04.1_regular_inspection
	04.2_car_reparation
	04.3_t i re_cha ng e_wi nt e r
	04.4_tire_change_summer
05 other	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 tne “what_vin” and
- “how_meny” data)



id vehicle categ
01_L
02 M
03 N
04 O
05 T
…

id district
BA SK
BB SK
BE DE
KE SK
MI IT
…

entity identification and authentification via assymetric 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 vín	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 demonstratiotr\ 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

PoW PoS
miner validator

D-PoS
witness

PC 01

MS Access Forms + VBA

MS Access VBA BC library

BC gateway (wallet)

local DB

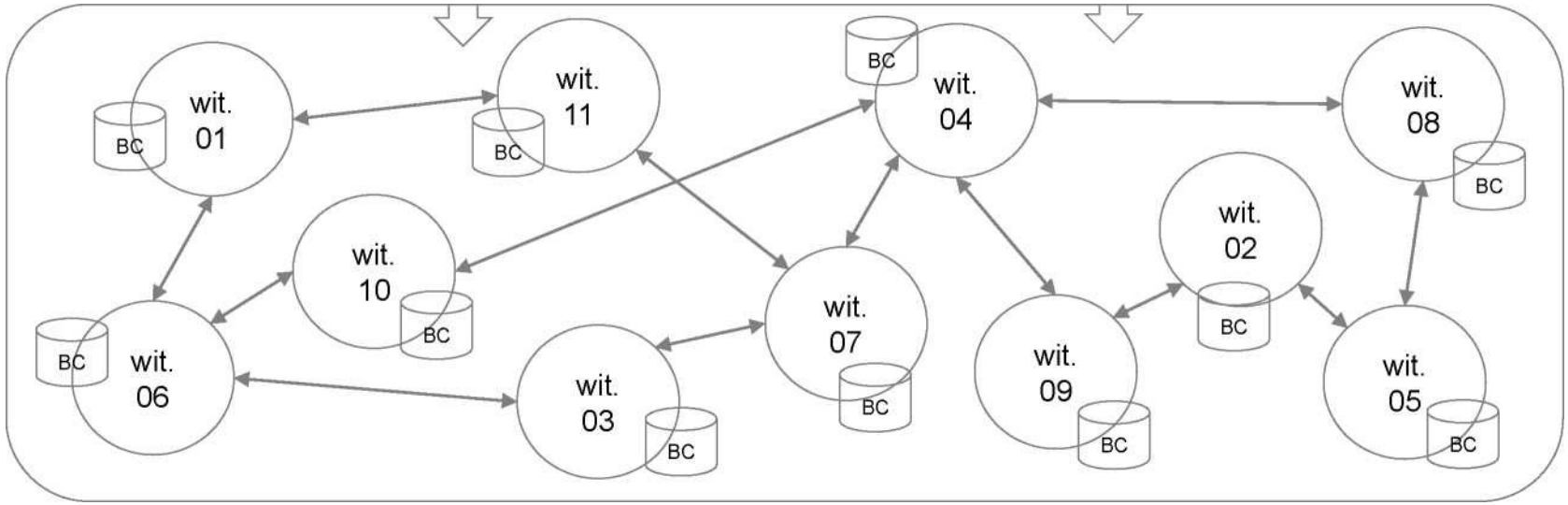
PC 02

MS Access Forms + VBA

MS Access VBA BC library

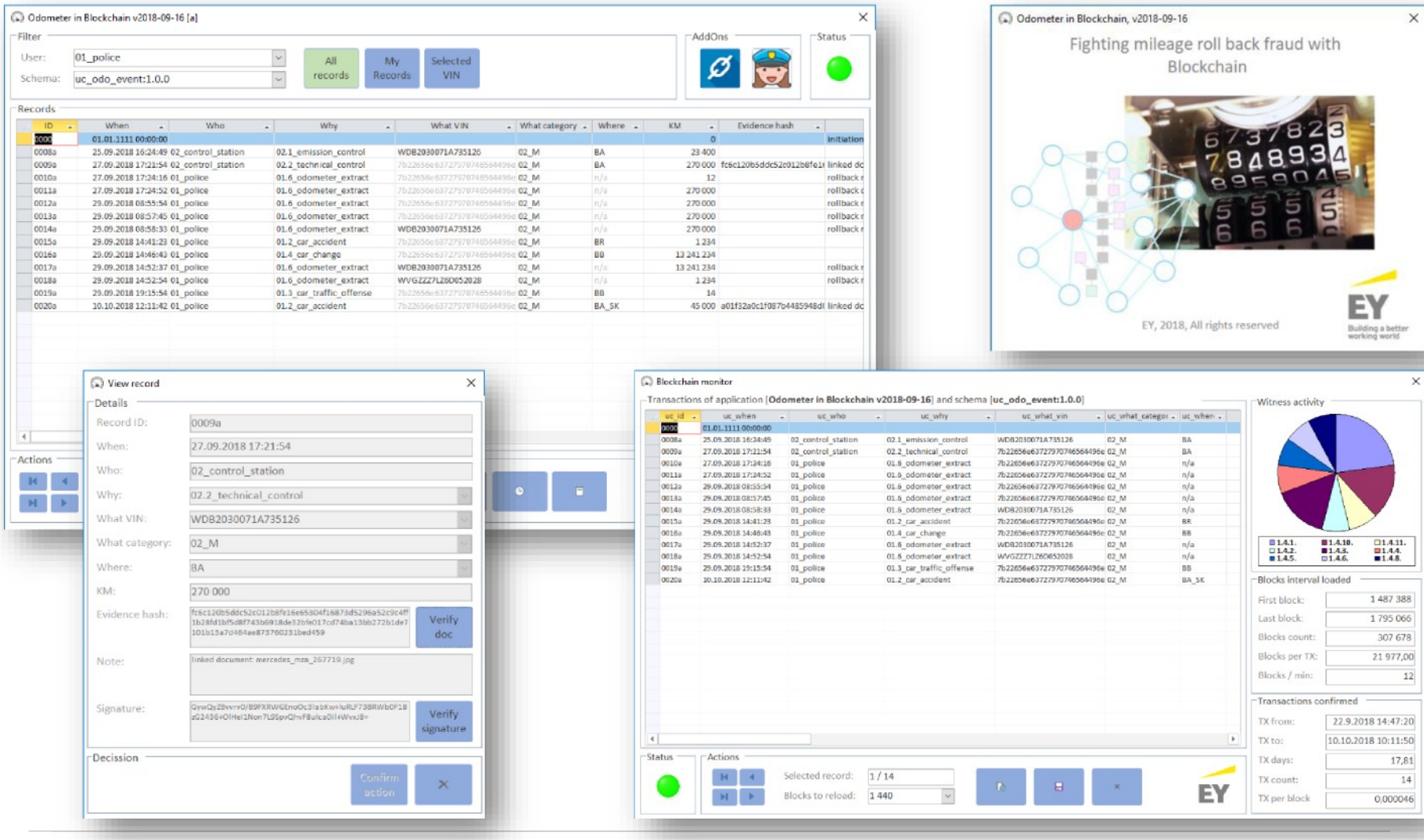
BC gateway (wallet)

local DB

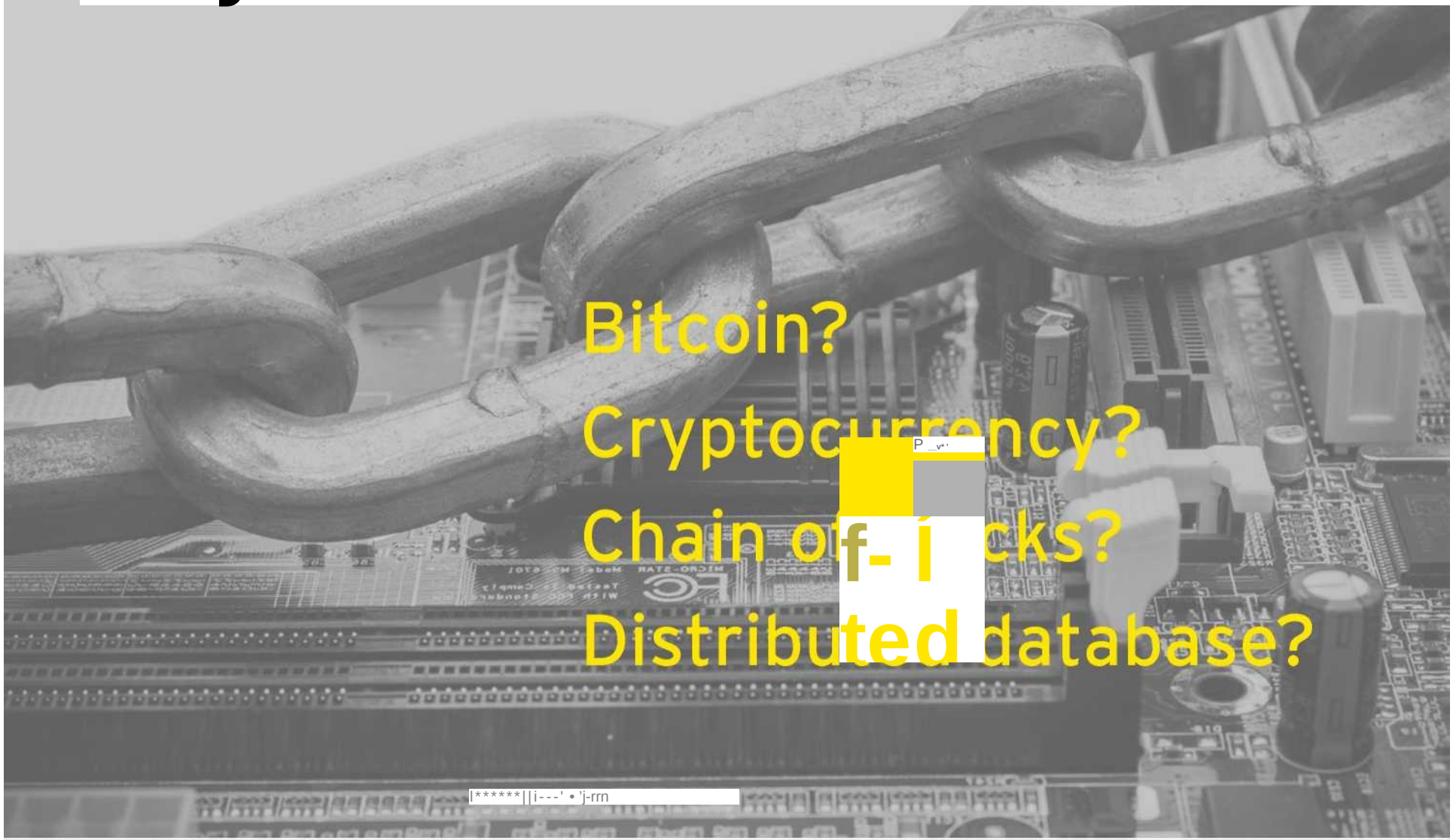


EY prototyping tool

Fighting mileage roll back fraud with Blockchain

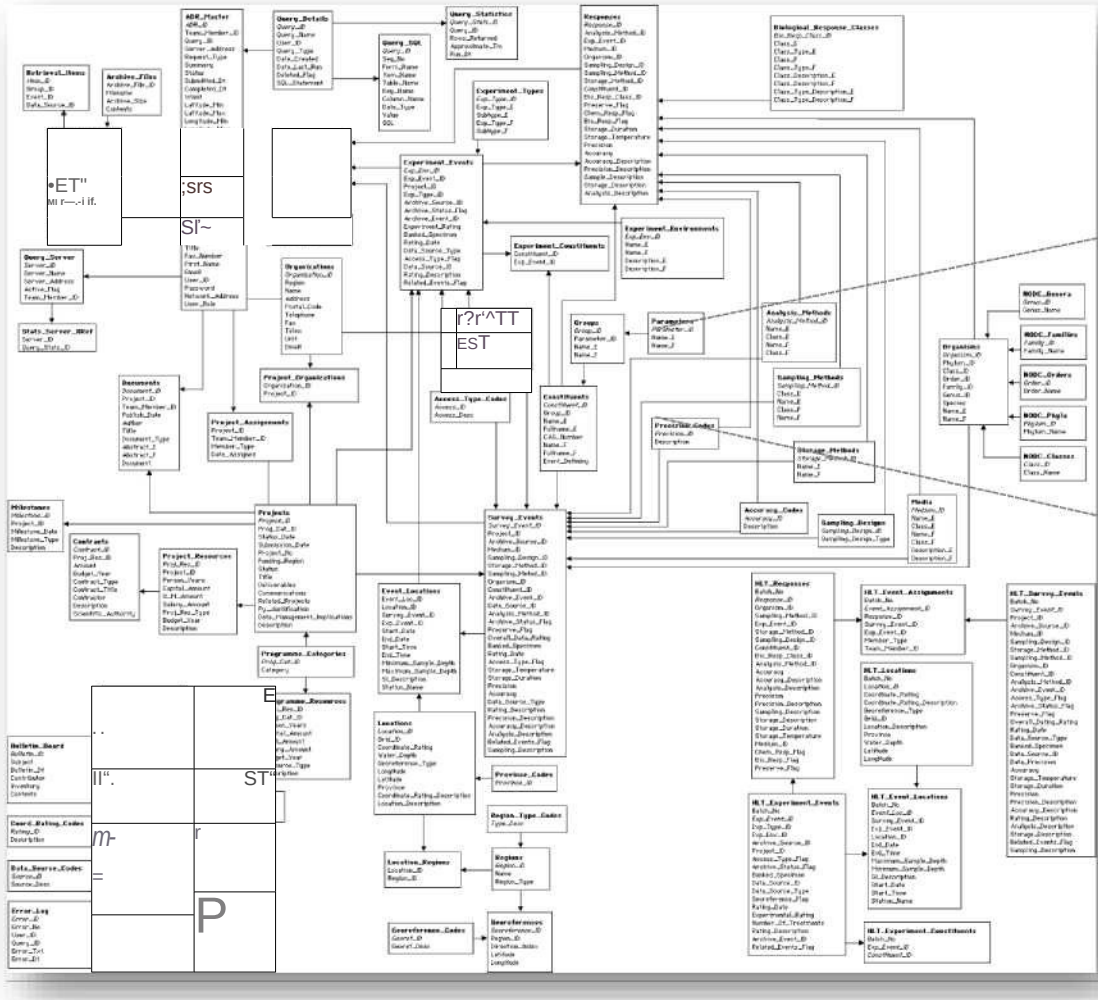


Čo je blockchain?

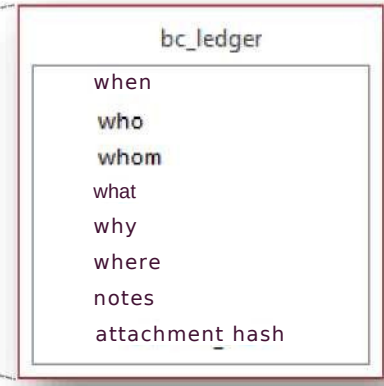


Blockchain ako jednoduchá databáza

Relačná databáza



Jednoduchá databáza

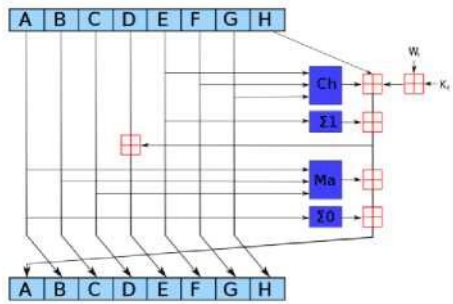


Základné stavebné bloky blockchainu
Kryptografická HASH funkcia

- Hash je jednosmerná funkcia, ktorá zo vstupného reťazca akejkoľvek 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 uložnie krátkeho odtlačku súboru, kedy samotný súbor je uložený off-chain

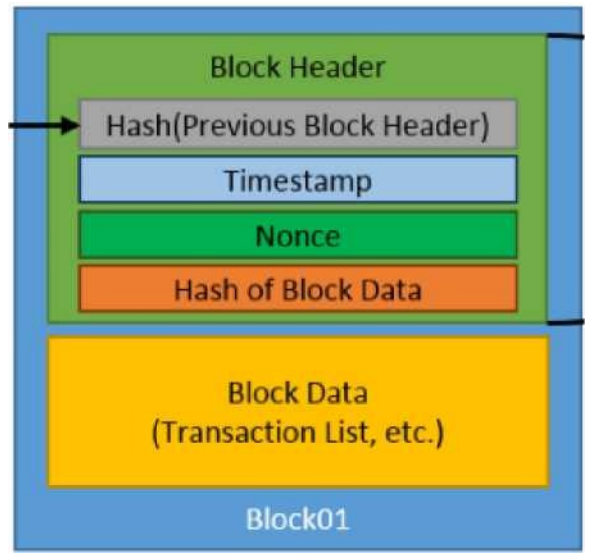


Ch(£, *F, G)* = *(E* A *F)* © *(~>E A G)*
Ma(j4, *B, C)* = *(A* A *B)* © (.4 A *C)* © *(B* A *C)*
E_0(v4) = (43g>2) © (A^>13) © (4^22)
(£l') - (F^6)©(£;^>ll)©(£l'^>25)
The bitwise rotation uses different constants for SHA-512. The given numbers are for SHA-256.
The red ffl is addition modulo 2^{32} for SHA-256, or 2^{64} for SHA-512

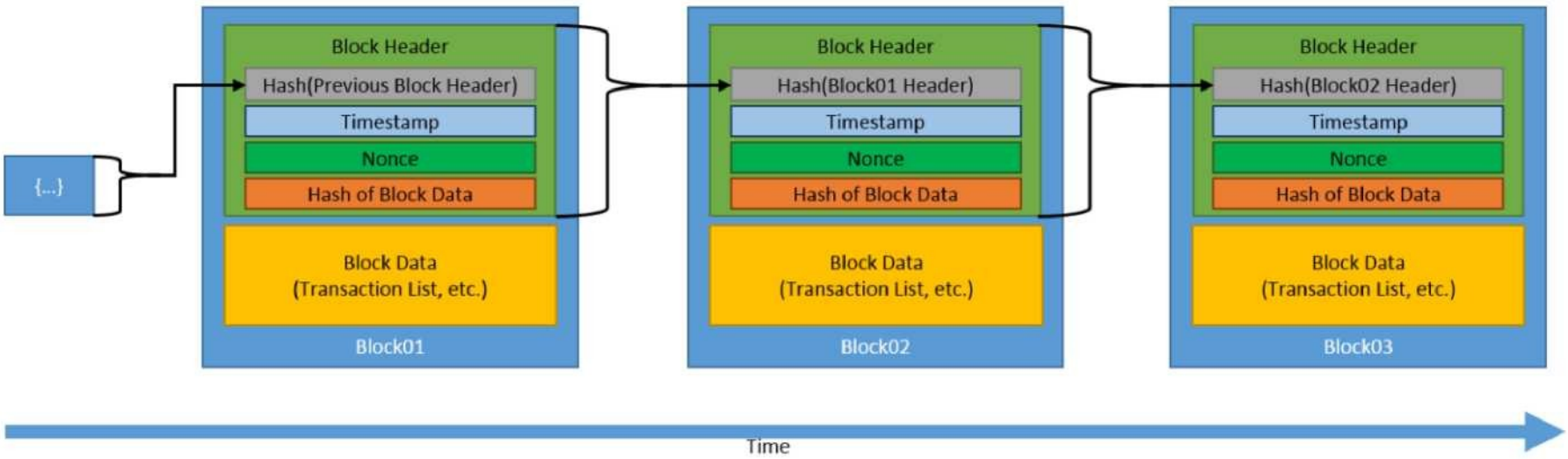
EY

Základné stavebné bloky blockchainu
Blok

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

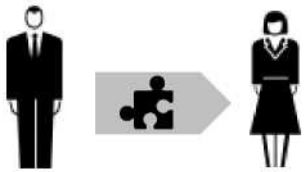


Blockchain ako Merkle tree



Ako vzniká blockchain

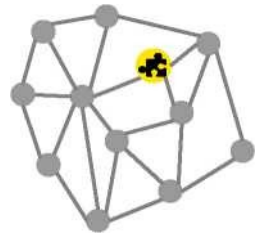
Vznik transakcie, ktorú chceme zapísať do blockchainu

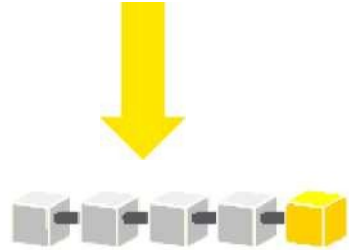


Osoba A Osoba B

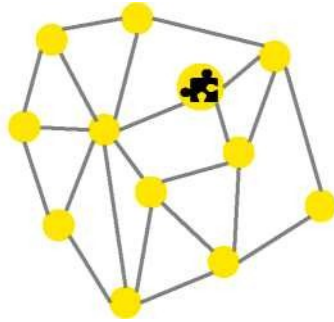
Transakcia je zaslaná niektorému z uzlov siete; tento ju pošle ostatným uzlom; transakcie za daný čas sú zoskupené do bloku

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



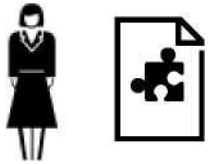


Nový blok sa pridá na koniec blockchainu a odošle sa ostatným uzlom



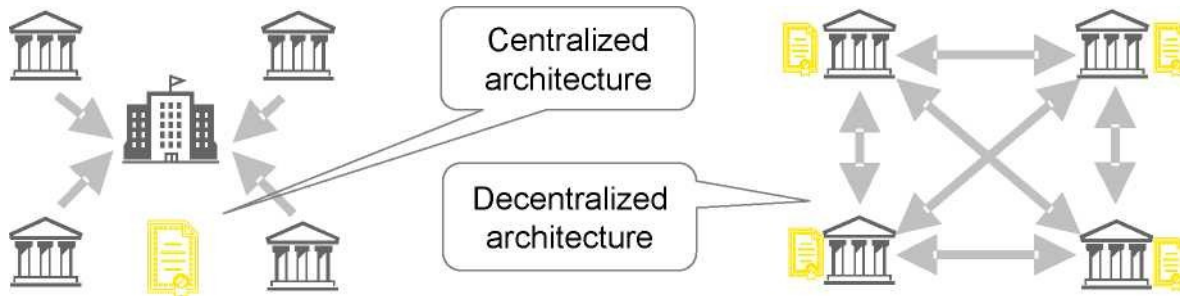
Všetky uzly dostanú nový blok a zaradia si ho do svojej kópie blockchainu

Potvrdenie o zapísaní transakcie



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 uživateľom 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 blockchainu z dôvodu dôvernosti alebo veľkosti, môžu byť uložené off-chain a v blockchaine len ich HASH a tým zabezpečiť nepopierateľnosť



EY

Blockchian – dalšie témy

- Konsenzuálne algoritmy - PoW, ine PoS a

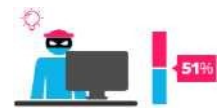
- Kryptomeny a tokenizácia asetov

- SMART contaracts - Ethereum, 2015

- Zero knowledge proof

ProofofWork vs Proof of Stake

proof of work is o requirement to define on expensive Computer calculation. aiso c a U e d mlning



A reward is given to the first miner wha solves each bjocks problém,

NetWork miners compete to be the first to f lnd a solutlon f or the mathematlcal problém

Proof of stoke, the creator of a new block Is chosen In a determlnlstlc way, depending on its wealth. a/so defined os stake.

The PoS systém there is no block reward. so. the miners také the transactlon fees.

Proof of Stake currencies can be several thousand time s more cost effectlve.

Information security in Blockchain

Decentralised vs centralised processing

Are audited data:

- Complete?
- Existing?
- Accurate?

Asymm. encryption

ution

Authentic Non repudiable

Immutable

Permanent

Redundant

Fast

	D	O	C	I
C	✓	x x	n/a	✓
I	✓	✓	✓	✓
A	✓	n/a	x	n/a

I need solution:

- Fast
- Cheap
- No 3rd party

BC inventor

p

My solution leads to:

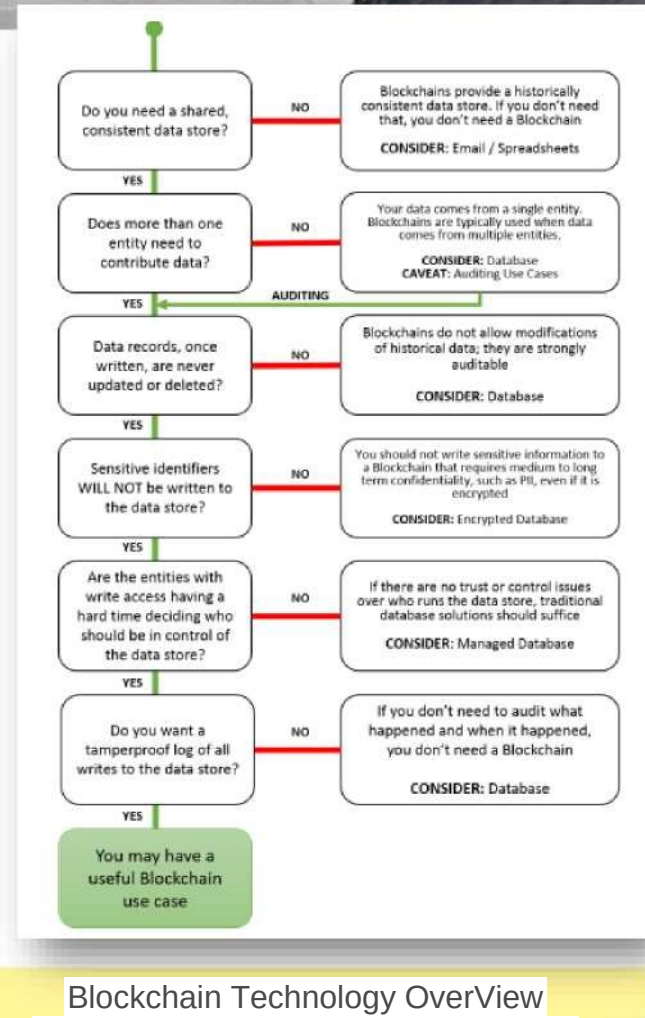
- Distributed • Open
- Consensual
- Immutable

EY

When to use blockchain

Typical "symptoms"

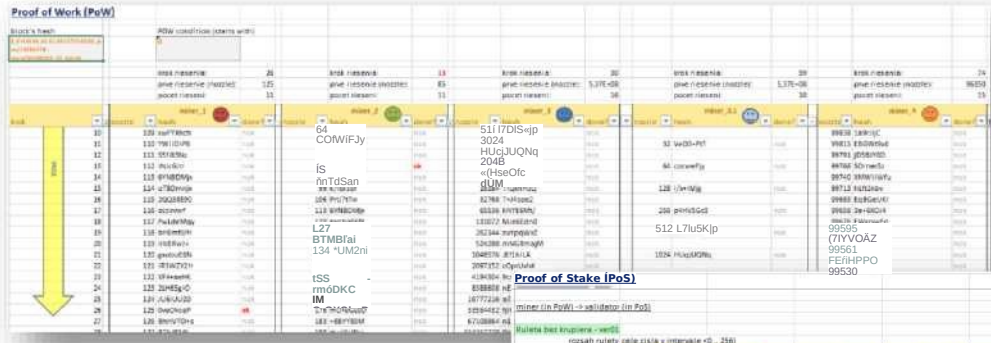
- When it is necessary to maintain and track important transactions or events in a **transparent, reliable, permanent and incontestable manner**
- When a reliable **audit trail** or time stamp are needed with respect to records of these transactions or events
- When the data in question is **generated 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.

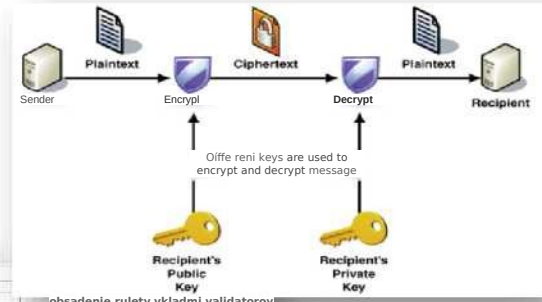


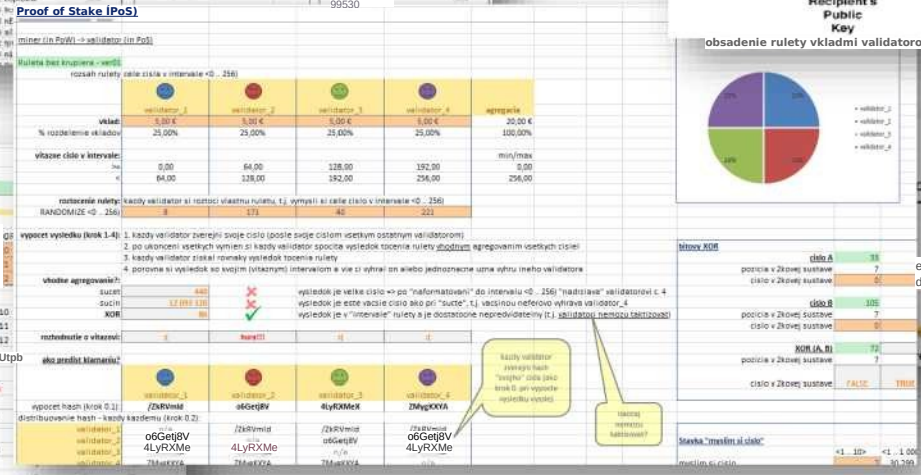
Blockchain Technology OverView
NISTIR 8202: https://nvlpubs.nist.gov

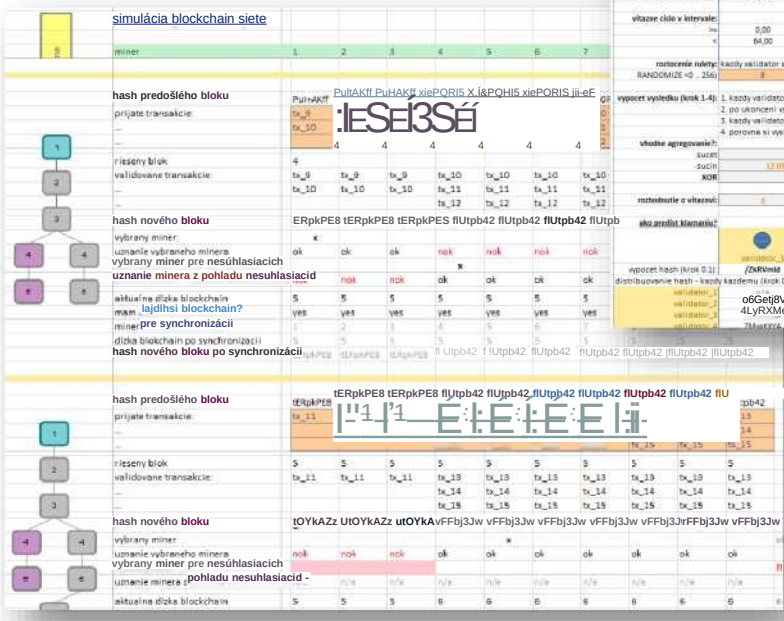
Blockchain fundamentals in XLS

Hash, chain, mining / validating, consensus



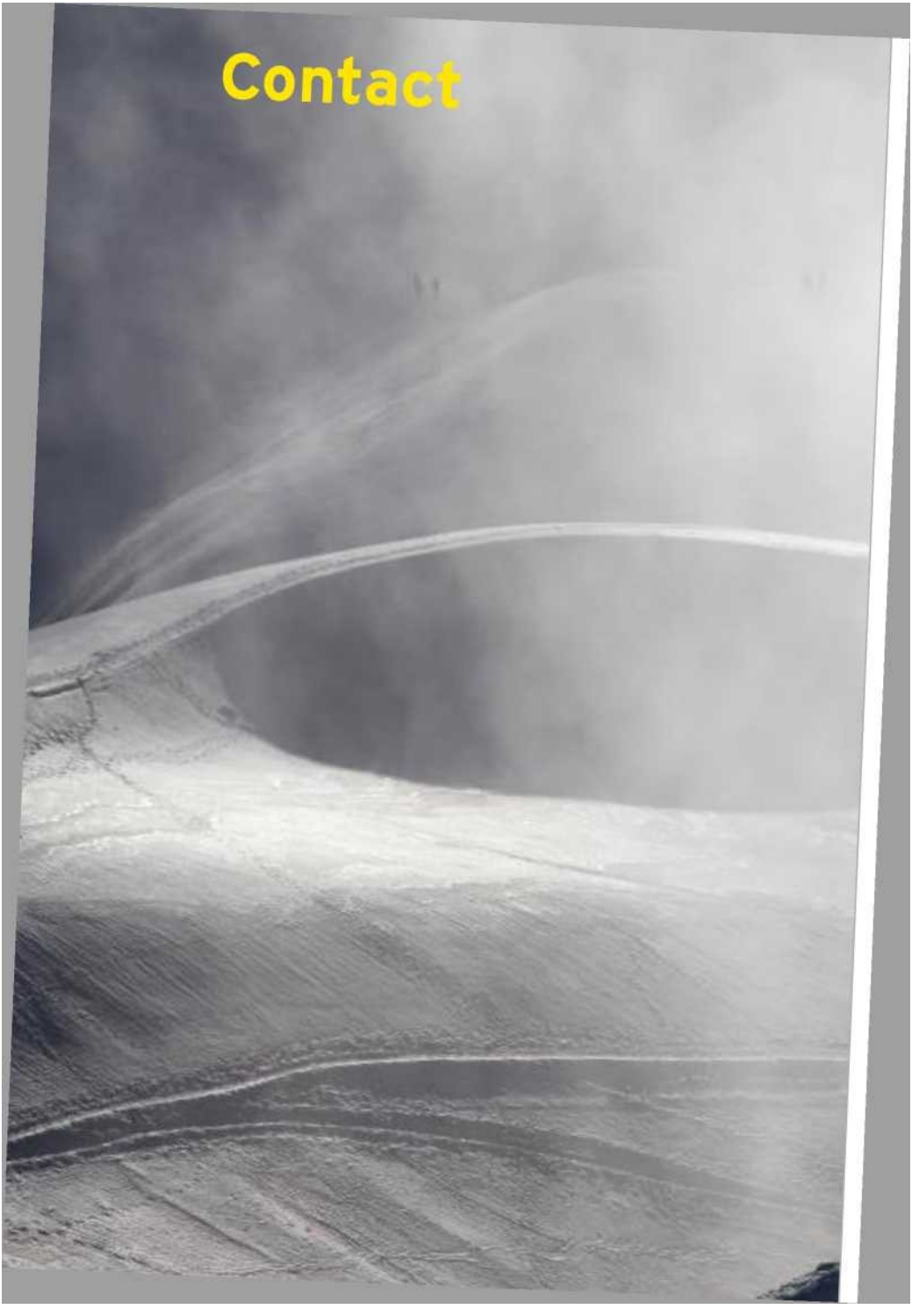






Questions?

Contact



EY
Žižkova 9
811 02 xxxxx

+421 2 3333 9111
ev@sk.ev.com
ey.com/sk

The information contained in this presentation is intended to provide generál 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 guality 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 separáte 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.

ey.com/sk