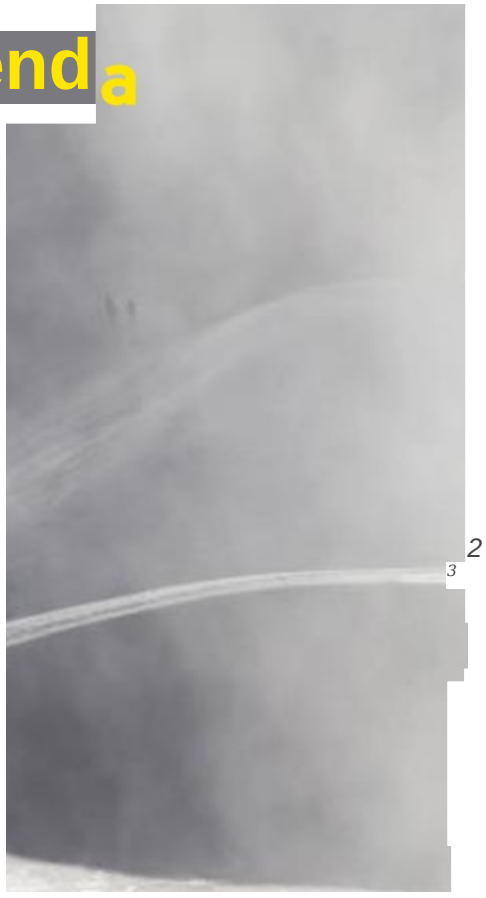
Štúdia možností a potenciálu technológie „blockchain“ pri zlepšovaní eGovernment riešení

Úvodné stretnutie

16.10.2018

Agenda



1

Blockchain in generál

Brief description, advantages, when to use

2

Štúdia

Zadanie, navrhovaný obsah, EU a blockchain

3

Príklad využitia, EY prototypovací nástroj

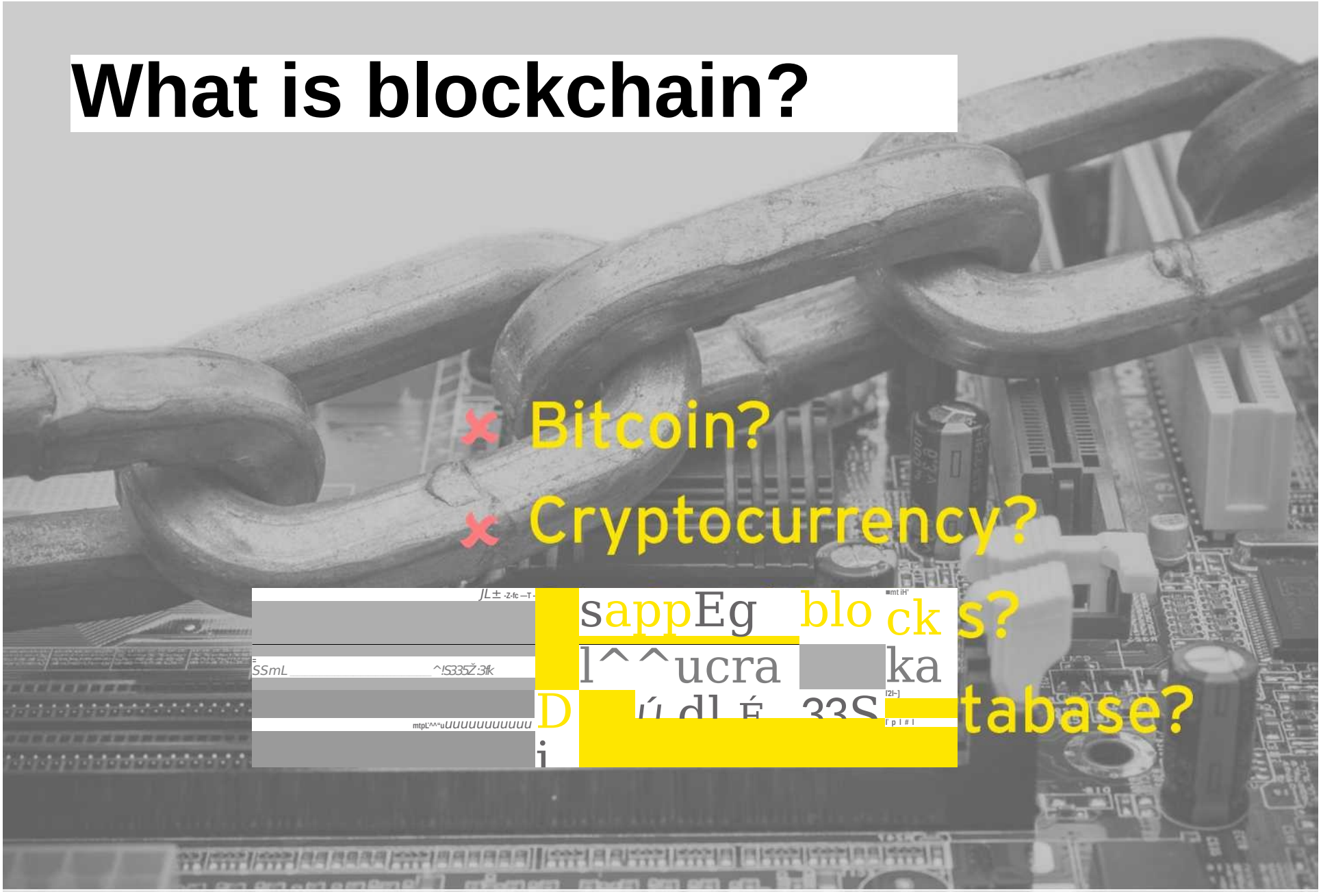
Blockchain proti stáčaniu kilometrov v autách

4

Blockchain fundamentals in XLS

Hash, chain, mining, consensus

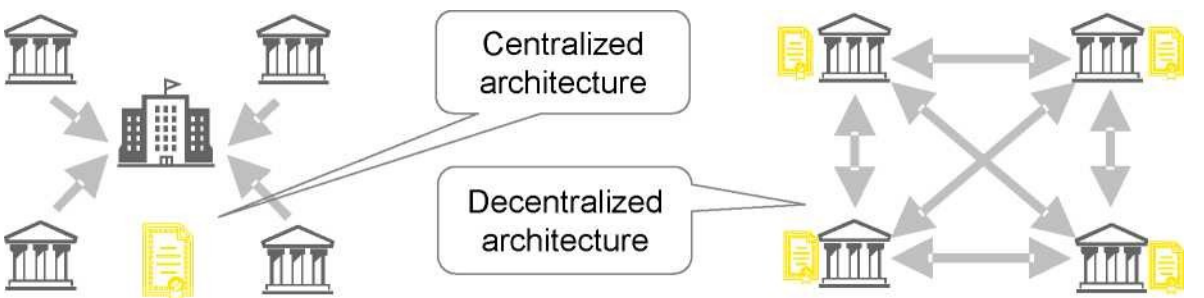
What is blockchain?



EY

What is blockchain
Working definition

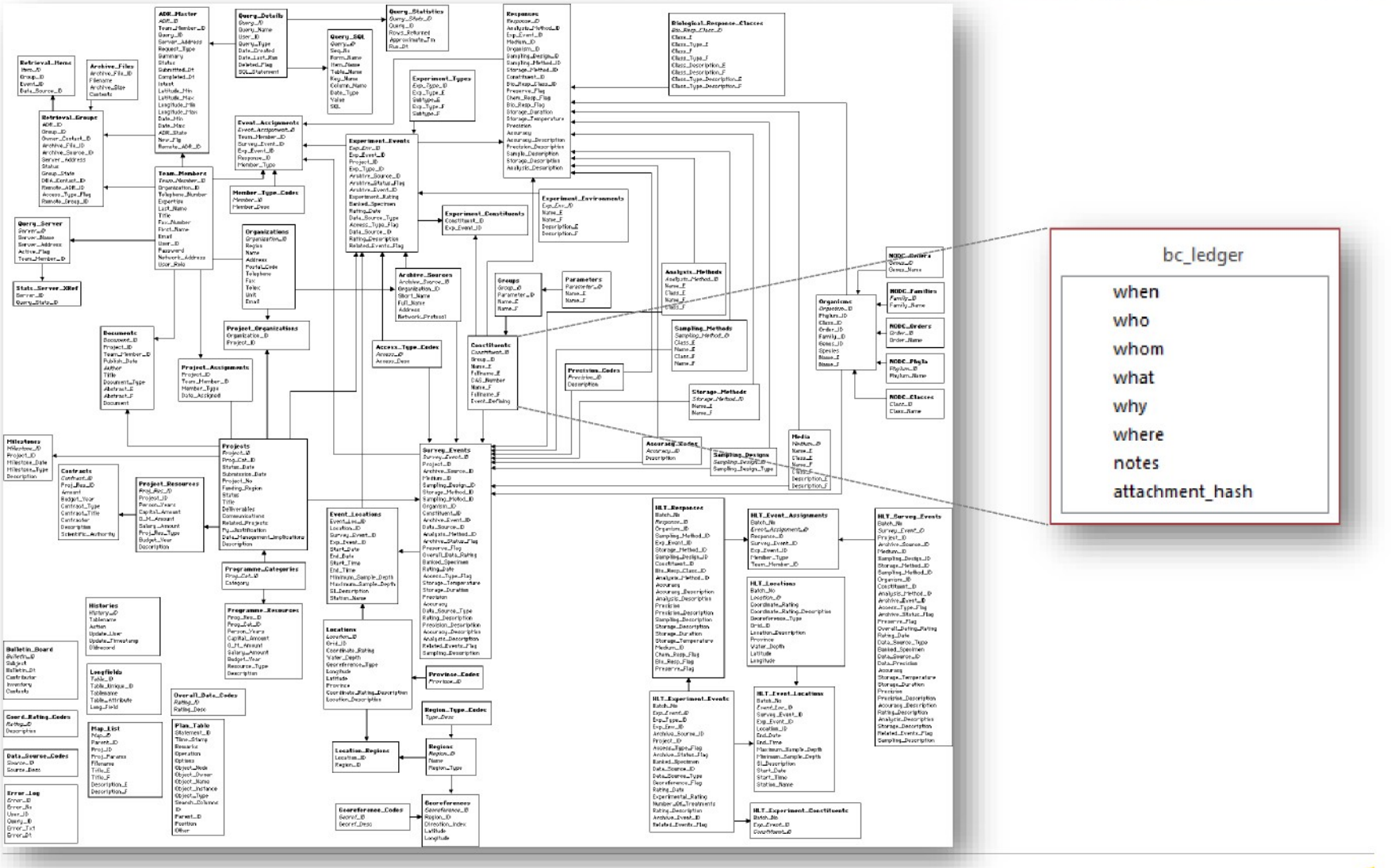
- Blockchain is a distributed ledger of meaningfully-selected smaller data records - so-called transactions, messages or events
- These records are grouped in interconnected blocks which protect them permanently from modification or deletion
- A new block of data is replicated very quickly and automatically onto all nodes in the blockchain network
- Using modern cryptographic algorithms and communication protocols, the blockchain network can ensure availability, authenticity and indisputability of recorded data
- Data is visible for all blockchain network users, except for confidential data which may be protected by encryption
- Users are able to agree unequivocally on the authenticity and reliability of data in blockchain (reaching consensus), even without the need for a trustworthy arbitrator
- Other related data files can be linked with records in blockchain by storing only a file reference and its hash (unique digital "fingerprint") in the blockchain network



EY

Blockchain is a single table database

Traditional vs Blockchain DB



Key building block of bockchain
Hash function

- A hash function creates an encrypted digital output from any digital input
- A good hash function is any **one way function (not possible to restore input data from hash)** that can be used to map data of arbitrary size to data of fixed size, with **slight differences in input data producing very big differences in output data.**
- Not possible to find **other meaningful input data producing same hash**
- Common hashes - MD5, SHA1, SHA256
- Example SHA256 hashes:

Text
(abc)

Function f(x>

Hash
(0bee89b07a248e27c83fc3d5951213c1)

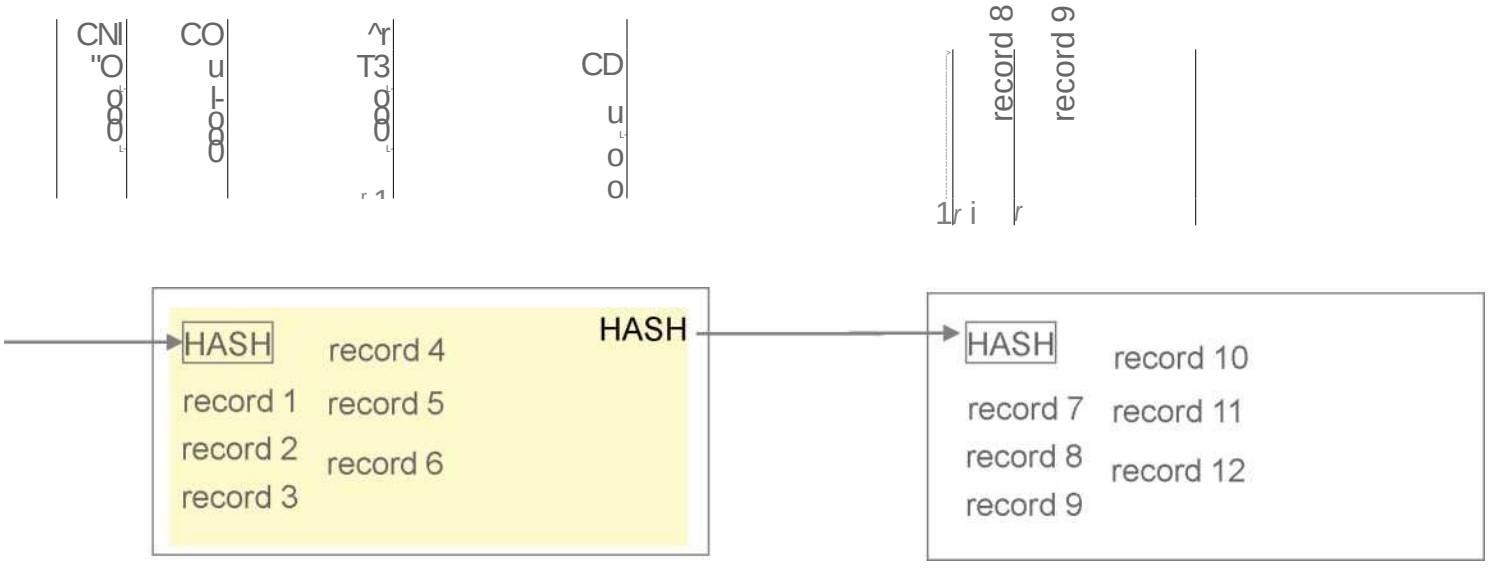
abc^ EDEAAFF3F1774AD2888673770C6D64097E391BC362D7D6FB34982DDF0EFD18CB abC ^

CD655CE2BE7D42A0D7255326DAFDE8F87F17DF5131247819F715D9223FEF2662 ab c ^

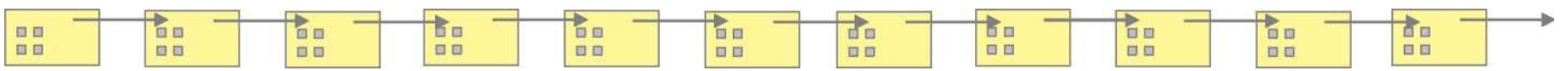
D1BCD337B7A3F564F38AFC5888A638A30343398FD686580628C480EED0354CB9

Hashing gives you confidence that information being received has not been tampered with

Chaining the data
Using hash functions



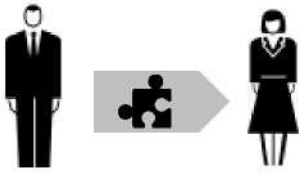
TIME



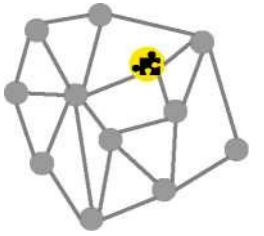
EY

Then "blockcham" process
In a nutshell

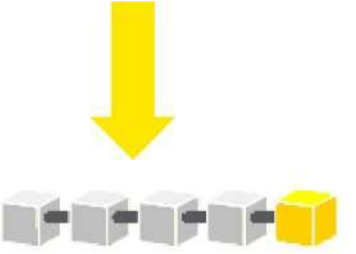
An exchange of information or a transaction between A and B is initiated.



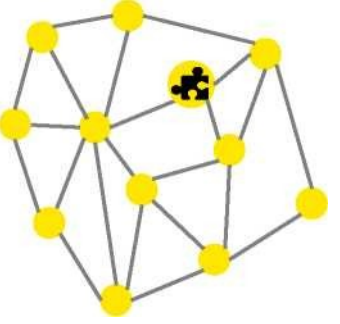
The transaction is submitted to the network and cryptographically secured. Transactions are grouped into a "block" that is "signed off" with a hash.



The network works to validate all transactions in the current block by collectively solving a cryptography problém. Only when the majority of parties on the network validate the transaction does the transaction proceed.

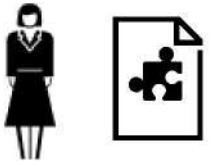


Once validated, the transaction is added to the current block. Each block contains the hash, or signature, of the preceding block linking the new block to the chain via the same cryptographic techniques.



All parties on the network can view the transaction block, with access rights determined by a system of public and private keys.

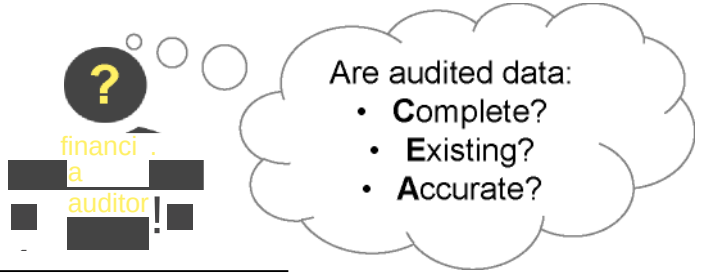
Person B receives the information.



EY

Information security in Blockchain

Decentralised vs centralised processing



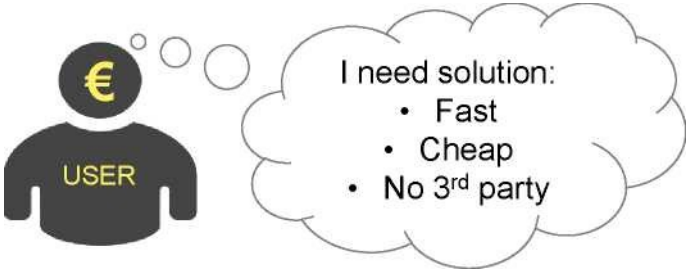
Asymm. encryption

lution

Authentic
Non repudiable
Immutable

- Permanent
- Redundant
- Fast

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



BC
invento
r
| | p

My solution leads to:

- Distributed • Open
- Consensual
- Immutable

EY

When to use blockchain
Typical "symptoms"

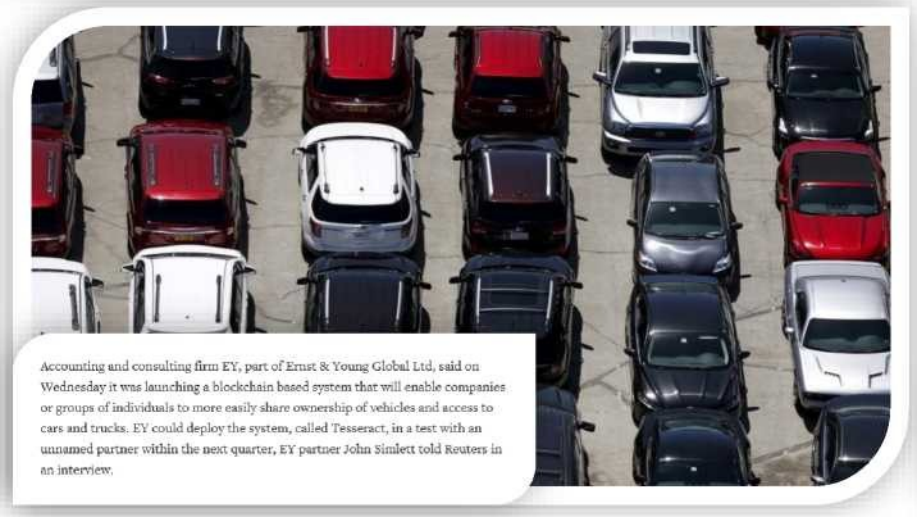
- When it is necessary to maintain and track important transactions or events in a transparent, reliable, permanent and incontestable manner
- When a reliable audit trail or time stamp are needed with respect to records of these transactions or events
- When the data in question is generated and shared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

EY

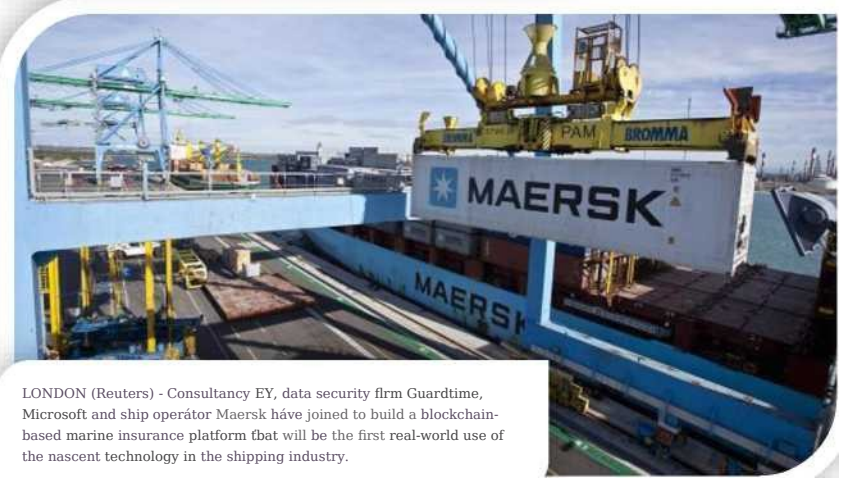
When to use blockchain
Selection of EY BC

EY creates the Wine Blockchain with the goal of certifying and comrnunicating the quality and geographlcal origin of wines made in Italy. Involved in this project also the EzLab startup.

Thanks to a partnership between EY and EzLab, the Wine Blockchain was bom to certily the wholetraceabilityofwine production, allowlngto guarantee quality, provenanceand production.



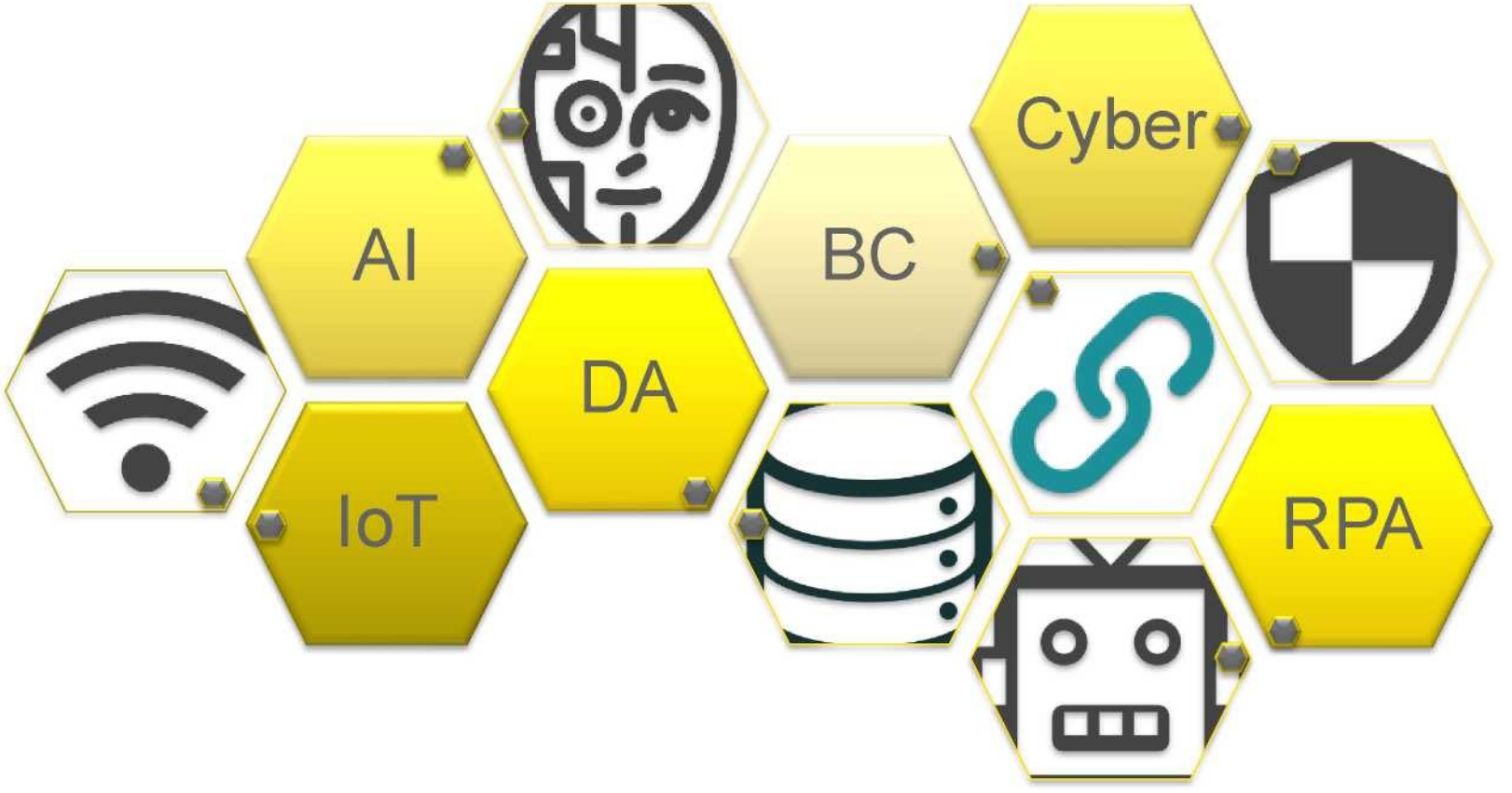
Accounting and consulting firm EY, part of Ernst & Young Global Ltd, said on Wednesday it was launching a blockchain based system that will enable companies or groups of individuals to more easily share ownership of vehicles and access to cars and trucks. EY could deploy the system, called Tesseract, in a test with an unnamed partner within the next quarter, EY partner John Similett told Reuters in an interview.



LONDON (Reuters) - Consultancy EY, data security firm Guardtime, Microsoft and ship operátor Maersk háve joined to build a blockchain-based marine insurance platform tbat will be the first real-world use of the nascent technology in the shipping industry.

When to use blockchain

Key element in the mosaic of"disruptive" technologies



EY

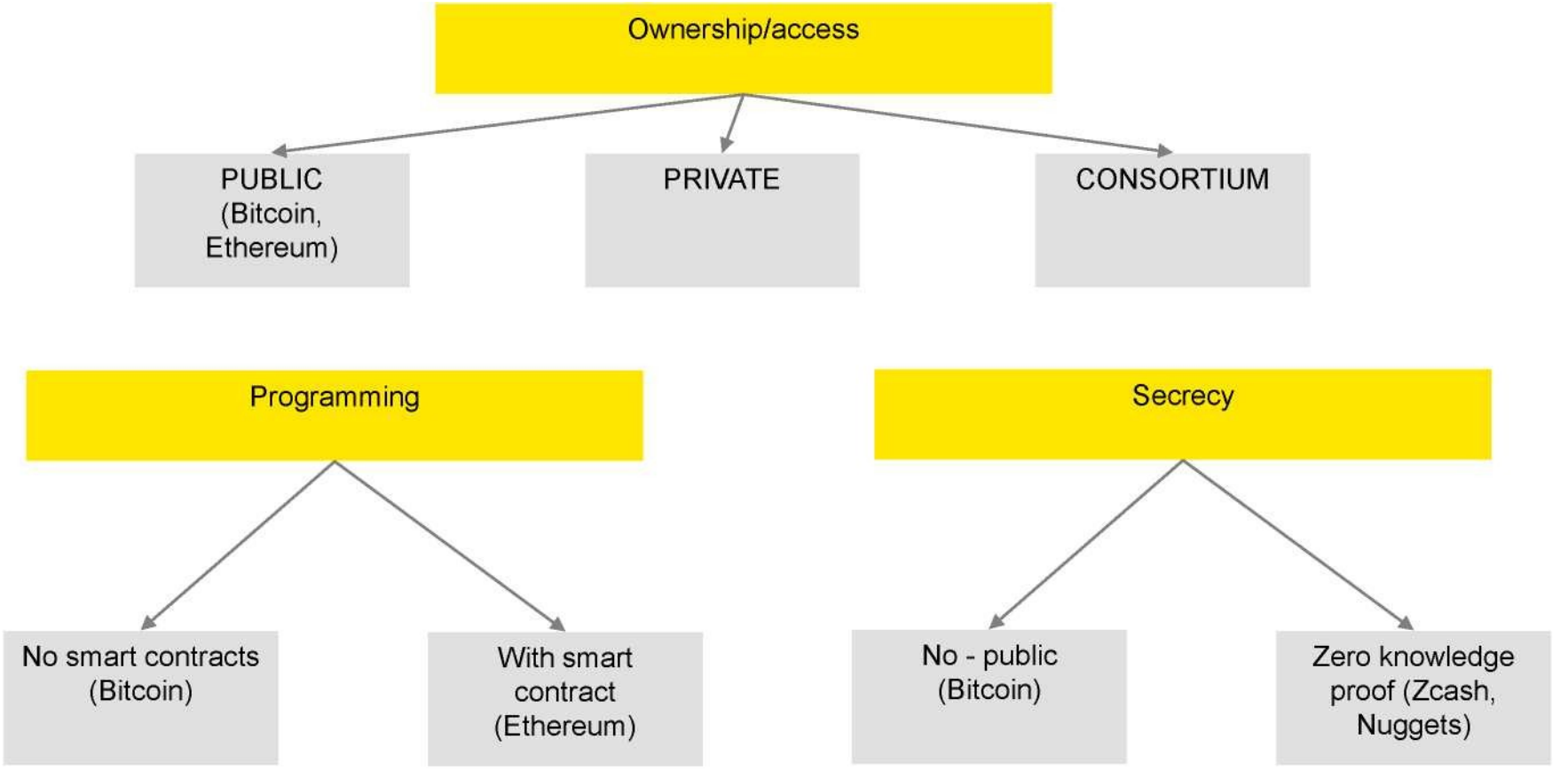
Blockchain taxonomy 1/2

Consensus algorithm

- With mining
  - Proof of work (Bitcoin)
- Without mining
  - Proof of stake
    - Proof of elapsed time - PoET
    - Proof of capacity - Burstcoin
    - Proof of activity – (Decred)
  - Delegated Proof of stake (SpohiaTX)
    - Proof of weight PoB PoW (Filecoin)
  - Practical Byzantine Fault Tolerance PBFT (Hyperledger)
    - Unique Node Lists - UNL
  - Proof of authority
    - Proof of burn- (Slimcoin)

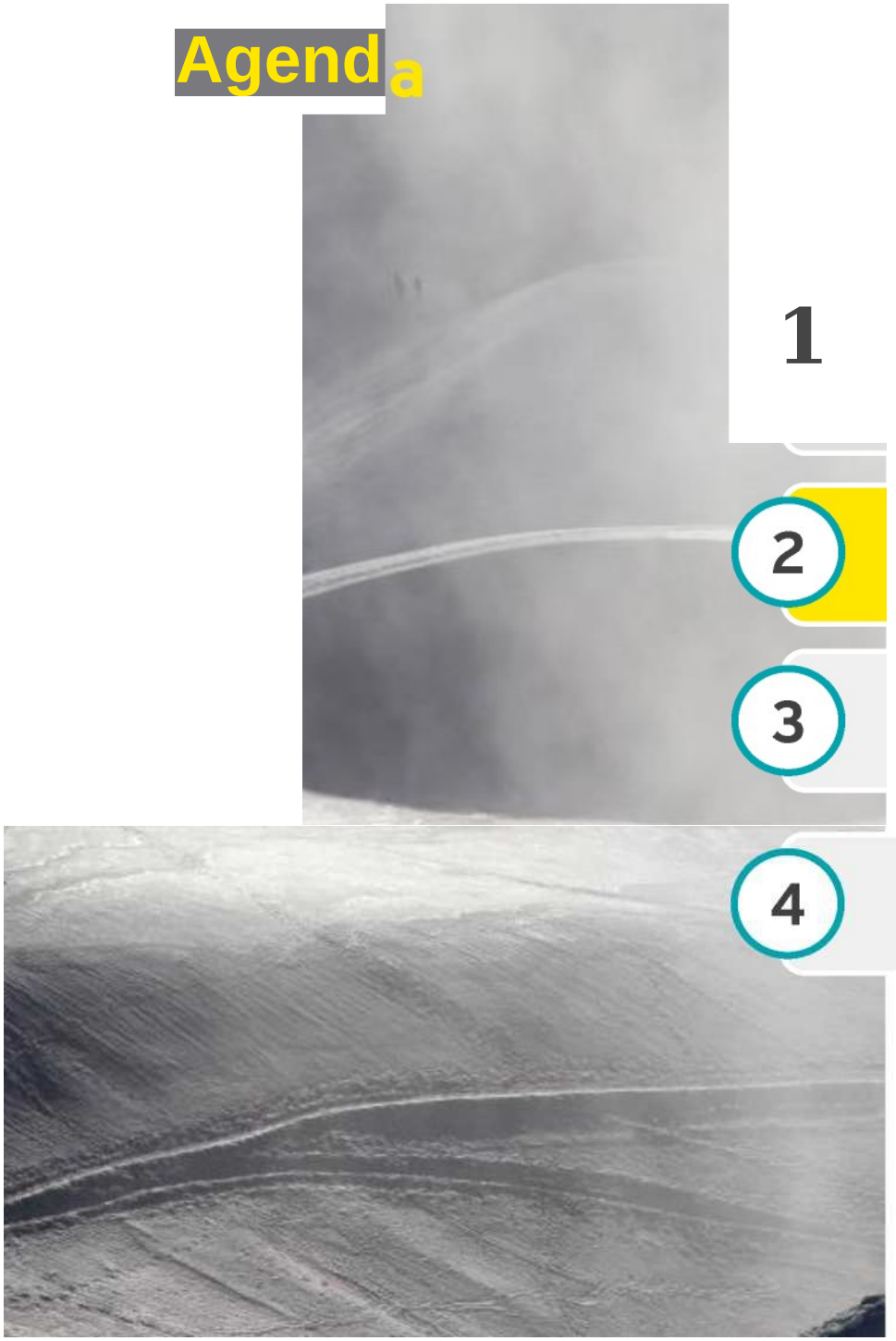
EY

Blockchain taxonomy 2/2



EY

Agenda



1

Blockchain in generál
Brief description, advantages, when to use

2

Štúdia
Zadanie, navrhovaný obsah, EU a blockchain

3

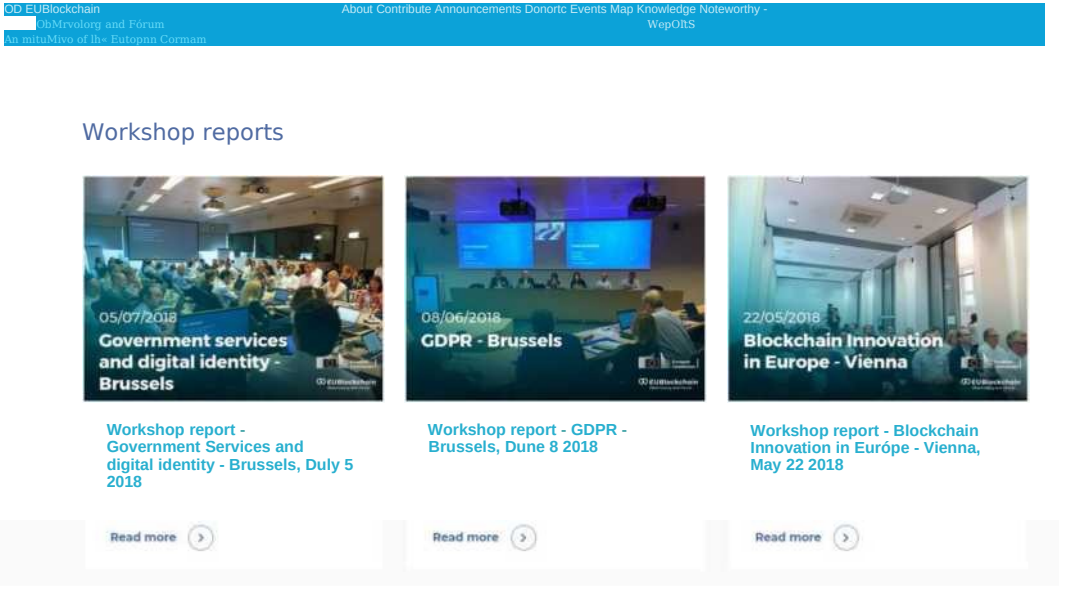
Príklad využitia, EY prototypovací nástroj
Blockchain proti stáčaniu kilometrov v autách

4

Blockchain fundamentals in XLS
Hash, chain, mining, consensus

European Commissior

THE EU BLOCKCHAIN OBSERVATORY & FORUM



Over 1000 stakeholders actively engaged, representing industry, innovative start- ups, public authorities, universities, civil society organisations (...)

Working together to accelerate blockchain innovation and the development of a blockchain ecosystem within the EU. Cementing **Europe's position as a global leader** in this transformative new technology.

#EUBlockchain

EY

European Commission

THE EUROPEAN BLOCKCHAIN PARTNERSHIP

The Blockchain partnership declaration launched at Digital Day 2018, represents a commitment by Member States to work together in the establishment of a secure and resilient **European Blockchain Services Infrastructure (EBSI)** to support cross-border digital public services.

By end of 2018, the Partnership will provide recommendations on:

1. A **set of use-cases** for digital public services that can be deployed through the EBSI

2. A description of the **functional specifications** of the EBSI

3. A **governance model** forthefuture development and operations of the EBSI

#EUBlockchain

Hlavné zainteresované strany (Stakeholders)

1. Vláda SR a ministerstvá
2. Štátne organizácie, úrady a agentúry: UPPVII, UHP, NBU, NASES a iné
3. Centra pre finančné inovácie na MF SR
4. Orgány miestnej štátnej správy
5. Združenia: Blockchain Slovakia, Slovensko Digital a iné
6. Fakulty univerzít zamerané na IT
7. Dodávatelia IT riešení
8. Ďalší podľa jednotlivých projektov

EY

Hlavné plánované stretnutia

1. MV SR
2. MF SR
3. Centra pre finančné inovácie na MF SR
4. MŠVVaŠ
5. MDVR SR
6. Blockchain Slovakia, Slovensko Digital

Zameranie Štúdie 1/2 (podľa článku 3 Zmluvy)

a) zmapovanie súčasného stavu riešení eGovernmentu (stratégií, plánov, ukončených a prebiehajúcich projektov) a ich obmedzení a nedostatkov, ktoré je potenciálne možné adresovať zavedením *„blockchain“* technológie,

b) zmapovanie ďalších požiadaviek a potrieb na dostupnosť, spoľahlivosť a bezpečnosť služieb a údajov poskytovaných občanom verejnou správou, ktoré je potenciálne možné adresovať zavedením *„blockchain“* technológie,

c) identifikovanie rozdielov medzi súčasným a požadovaným stavom (v zmysle dvojice písmen vyššie),

d) identifikovanie triedy problémov, ktoré je možné riešiť implementovaním distribuovaných a decentralizovaných technológií, k akým patrí aj blockchain,

EY

Zameranie Štúdie 2/2 (podľa článku 3 Zmluvy)

e) kvalitatívne (a ak je to možné a relevantné aj kvantitatívne) porovnanie jednotlivých distribuovaných a decentralizovaných technológií (s dôrazom na technológiu „blockchain") voči „tradičným" technológiám pri riešení danej triedy problémov,

f) rámcové definovanie potenciálnych projektov (predmet, ciele, harmonogram, zdroje, predpoklady a súvislosti s inými projektami) pre aplikácie („use cases"), v ktorých sa ukáže ako výhodné riešenie technológia blockchain,

g) návrh mechanizmu podpory spoločností typu a/alebo služieb typu „fintech" (typicky malé a stredné podniky) v SR, aj s využitím financovania z Operačného programu integrovaná infraštruktúra, prioritná os 8.

EY

Hlavné ciele Štúdie 1/3 (podľa článku 4 Zmluvy)

a) poskytnutie prehľadu o základných princípoch a prvkoch *„blockchain"* technológie a jej uplatnení v rámci e-Government aplikácií a služieb občanom,
b) prehľad výhod a nedostatkov aplikácie *„blockchain"* technológie v prostredí e-Governmentu,
c) definícia tém, otázok a výziev v skúmanej oblasti pre najbližšie obdobia (infraštruktúra a architektúra súčasného e-Governmentu v SR, *„blockchain modely",* legislatívny rámec, centralizovaný model vs. decentralizovaný model, bezpečnosť, finančná udržateľnosť, rezistencia voči zmenám, pripravenosť verejnosti a pod.),
d) prehľad potenciálnych kľúčových úloh a rolí štátu pri adopcii *„blockchain"* technológie,

EY

Hlavné ciele Štúdie 2/3 (podľa článku 4 Zmluvy)

e) poskytnutie prehľadu o súčasných významných iniciatívach vedúcich k zavádzaniu *„blockchain"* technológie na úrovni EÚ a v prostrediach verejnej správy členských štátov EÚ,

f) poskytnutie detailného prehľadu o najvýznamnejších aplikáciách *(„use cases")* zavedenia *„blockchain"* technológie v prostredí eGovernmentu v podmienkach SR a ostatných členských krajín EÚ,

g) rámcový prehľad potenciálnych dopadov aplikácie *„blockchain"* technológie na efektivitu a účinnosť aktivít a služieb poskytovaných štátom,

h) rámcový prehľad potenciálnych dopadov na občanov využívajúcich služby, ktorých fungovanie je založené na aplikácii *„blockchain"*

EY

Hlavné ciele Štúdie 3/3 (podľa článku 4 Zmluvy)

i) prehľad tzv. „quick wins" pri aplikácii *„blockchain”* technológie v prostredí e-Governmentu,

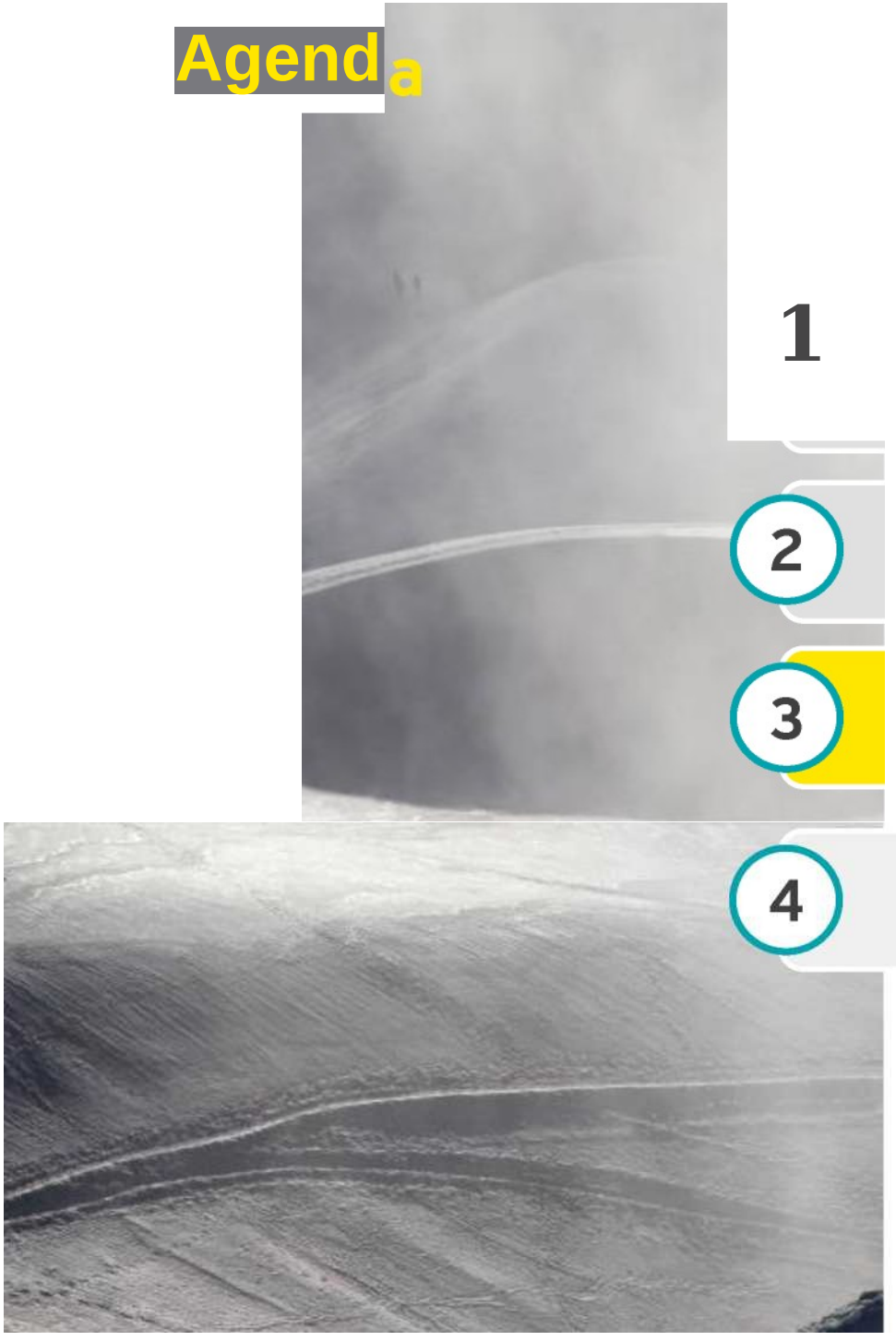
j) rozšírenie povedomia o vlastnostiach a možnostiach technológie *„blockchain"* medzi pracovníkmi zodpovednými za riadenie budovania eGovernment riešení,

k) podpora malých a stredných podnikov typu *„fintech"* v oblasti rozvoja ich služieb v SR,

l) vypracovanie odporúčaní na realizáciu aktivít zo strany ÚPPVII, vychádzajúcich z hore uvedených výstupov Štúdie, vrátane indikácie časovej postupnosti týchto aktivít.

EY

Agenda



1

Blockchain in generál

Brief description, advantages, when to use

2

Štúdia

Zadanie, navrhovaný obsah, EU a blockchain

3

Príklad využitia, EY prototypovací nástroj

Blockchain proti stáčaniu kilometrov v autách

4

Blockchain fundamentals in XLS

Hash, chain, mining, consensus

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_control_station	02.1_emission_control
	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 the "what_vin" and "how_meny" data)

entity identification and authentification via assymetric crypto

encrypted with public key of the "01_police" user

id_vehicle_categ	id_district
01_L	BA_SK
02_M	BB_SK
03_N	BE_DE
04_O	KE_SK
05_T	MI_IT

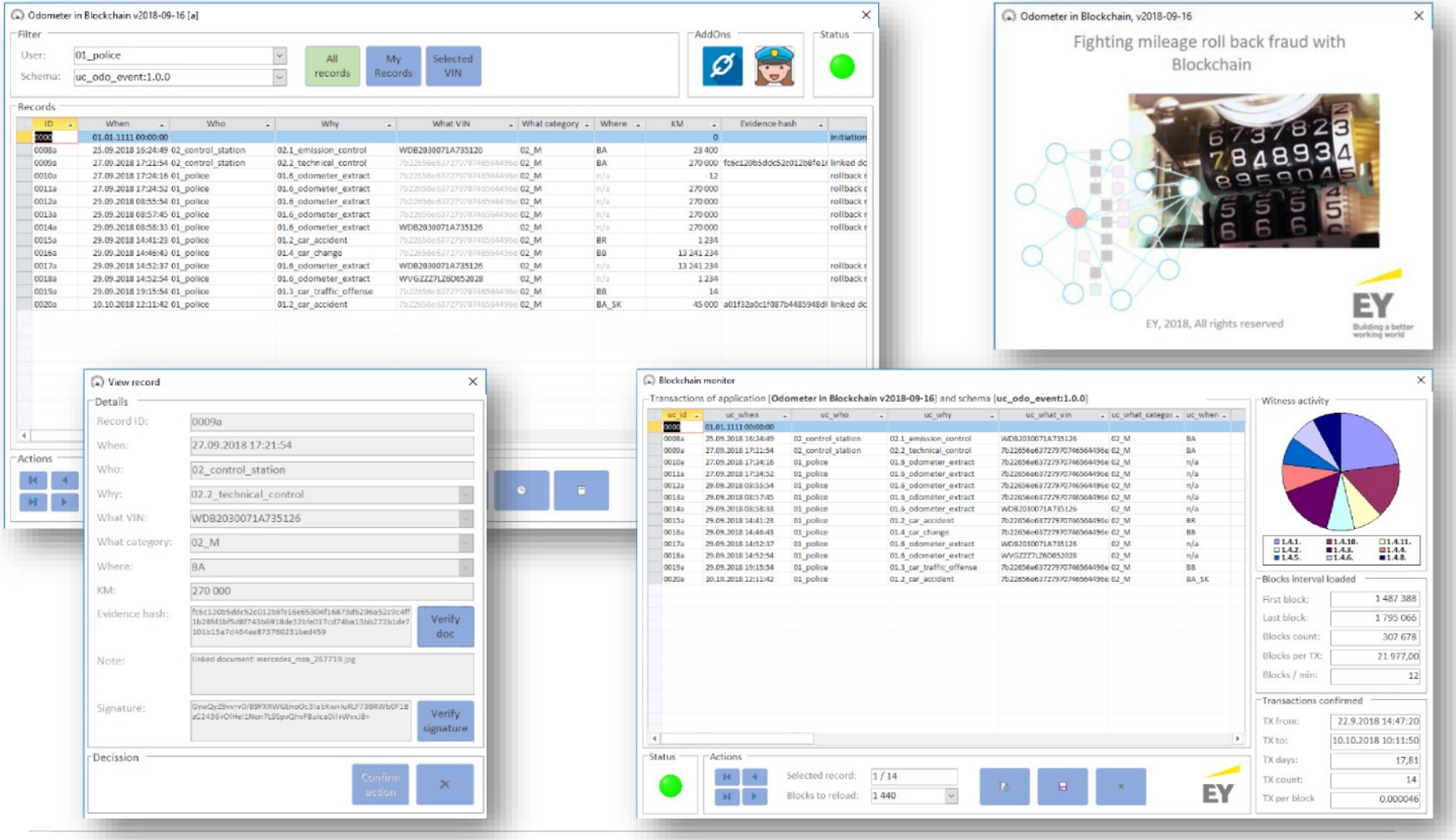
evidence document (e g. photo of vehicle's dashboard with odometer) remains off-chain; only hash of the photo is stored on blockchain

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	WDB2030071735126	02_M	MI IT	3 500	[hash of dashboard.jpg]	sa i e of a demonstration vehicle
0002a	23.09.2018 11:10:05	04 car service	04.1_regular_inspection	WDB203007735126	02_M	BA_SK	15 000	[hash of dashboard.jpg]	oil and oil filter replacement
...	...	...	...	...	...	...	...	...	...

EY prototyping tool

Fighting mileage roll back fraud with Blockchain



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

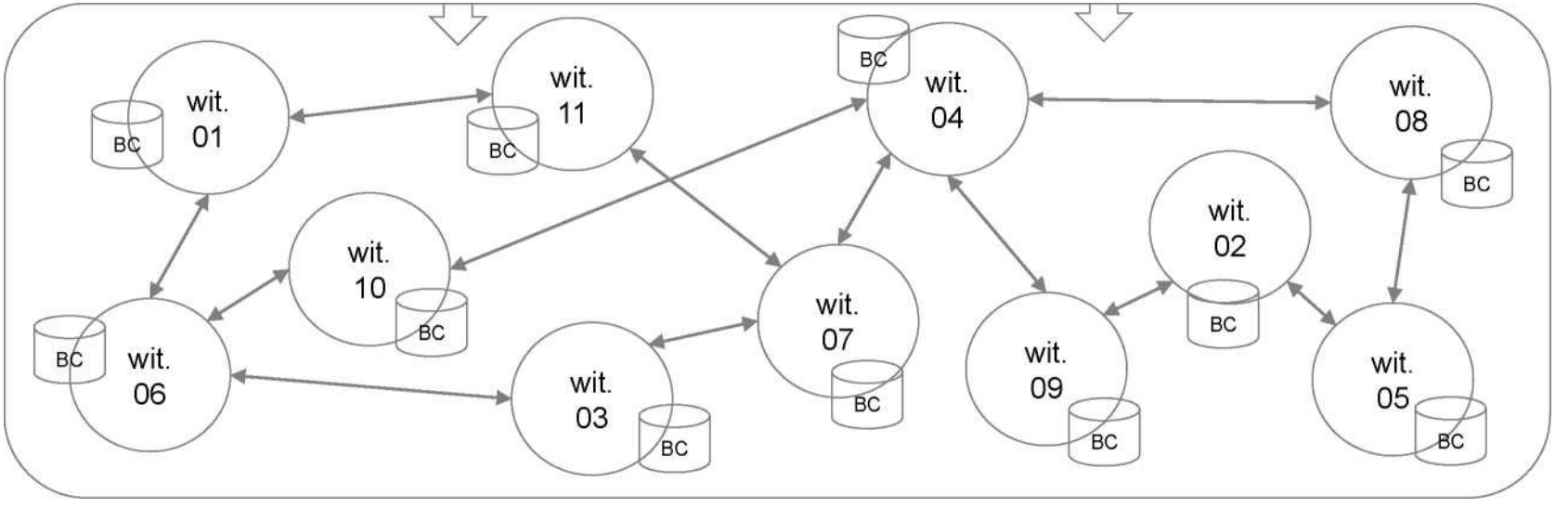
PC 02

MS Access Forms + VBA

MS Access VBA BC library

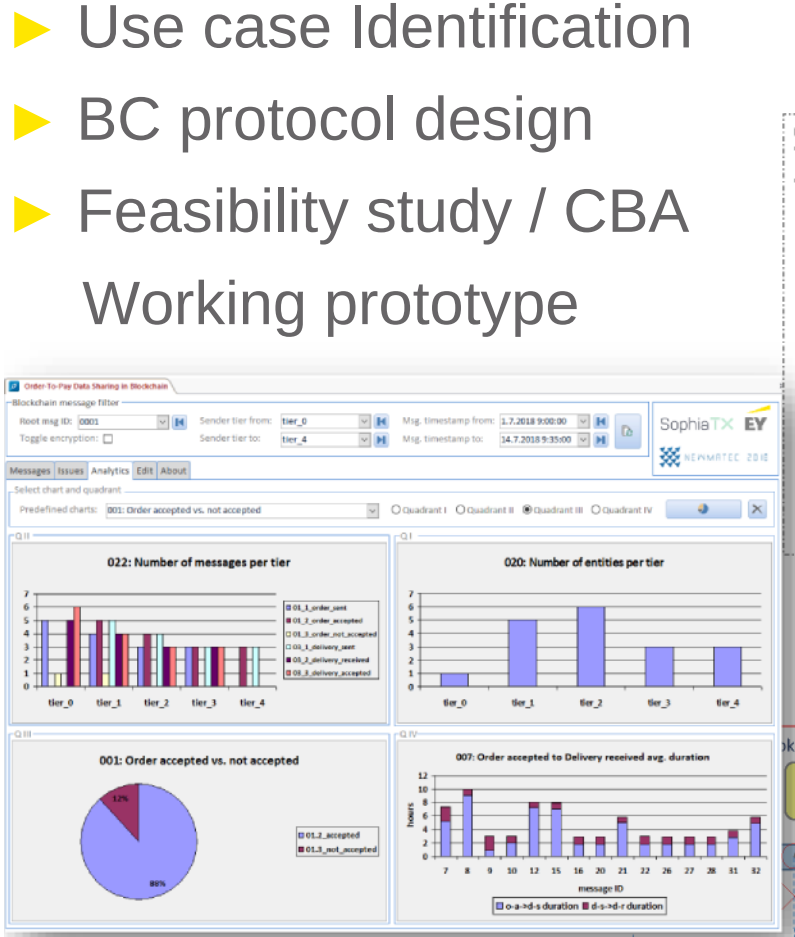
BC gateway (wallet)

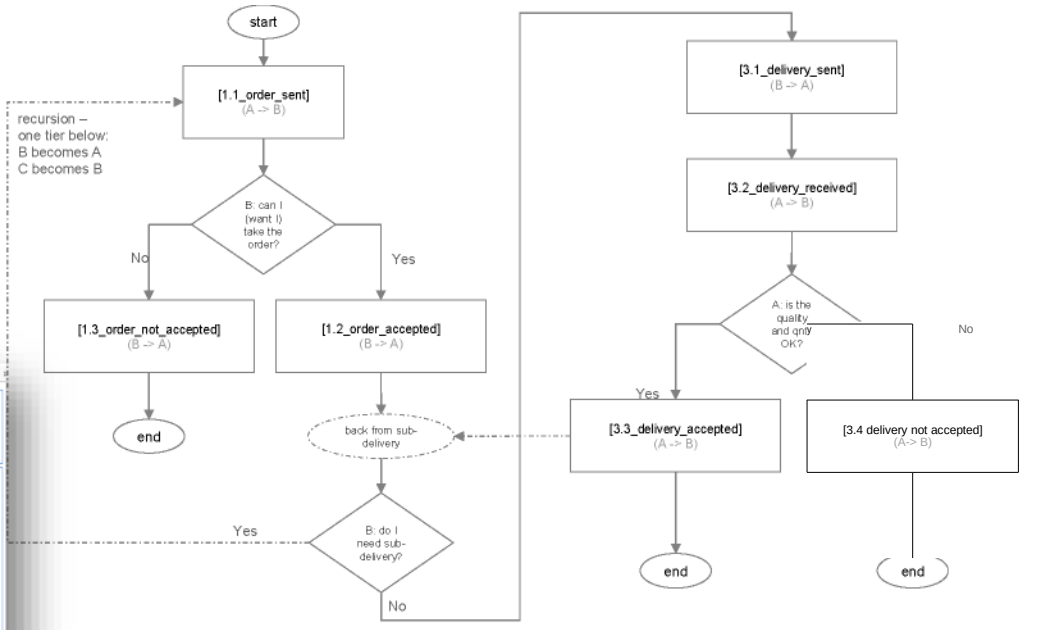
local DB

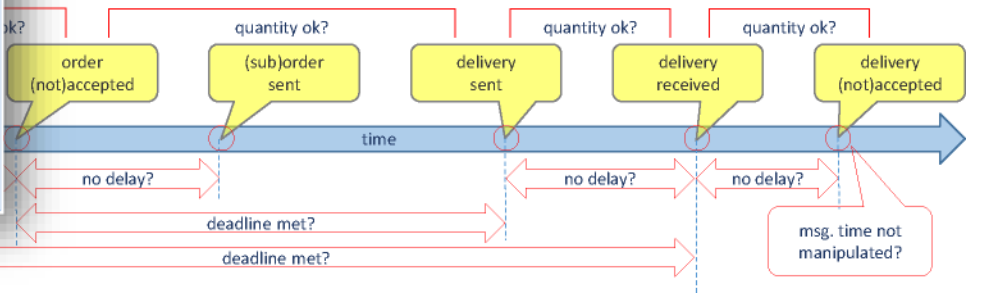


EY prototyping tool
Service proposal

- Use case Identification
- BC protocol design
- Feasibility study / CBA
- Working prototype







EY

Agenda

1

Blockchain in generál

Brief description, advantages, when to use

2

Štúdia

Zadanie, navrhovaný obsah, EU a blockchain

3

Príklad využitia, EY prototypovací nástroj

Blockchain proti stáčaniu kilometrov v autách

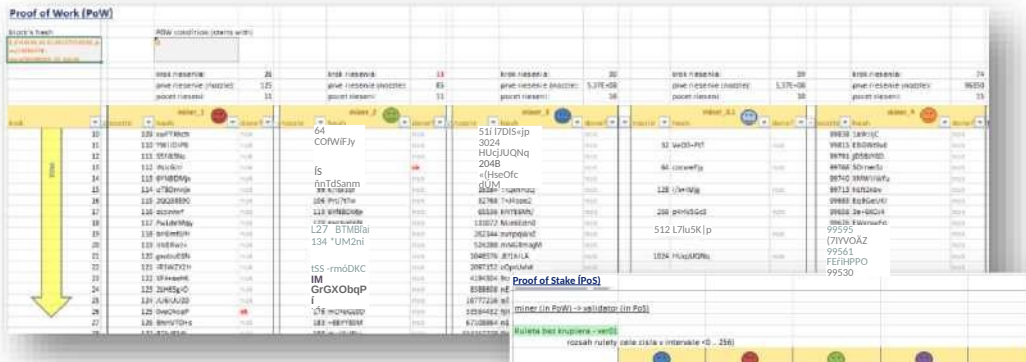
4

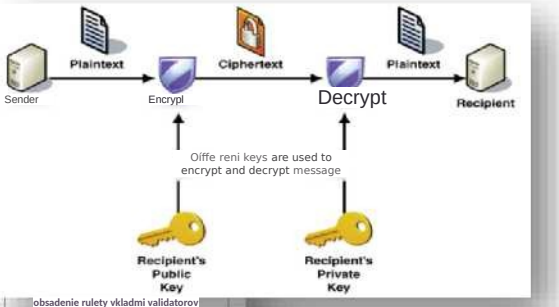
Blockchain fundamentals in XLS

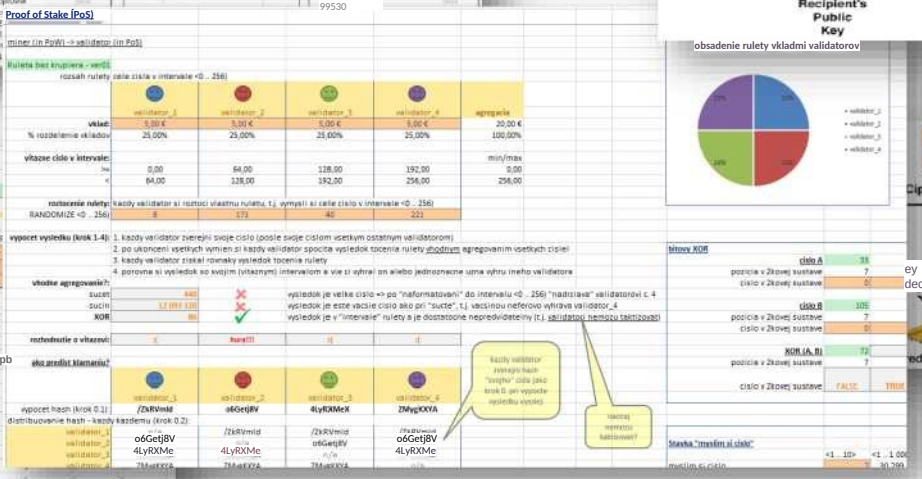
Hash, chain, mining, consensus

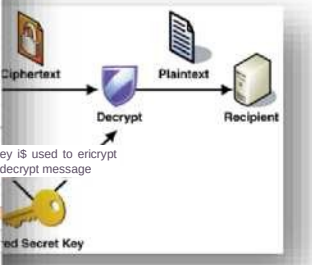
Blockchain fundamentals in XLS

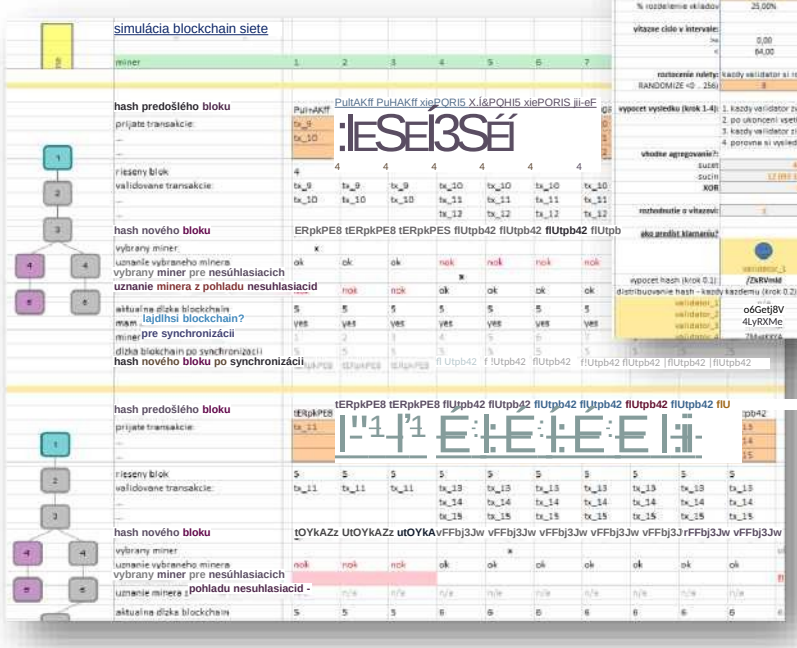
Hash, chain, mining / validating, consensus, ...





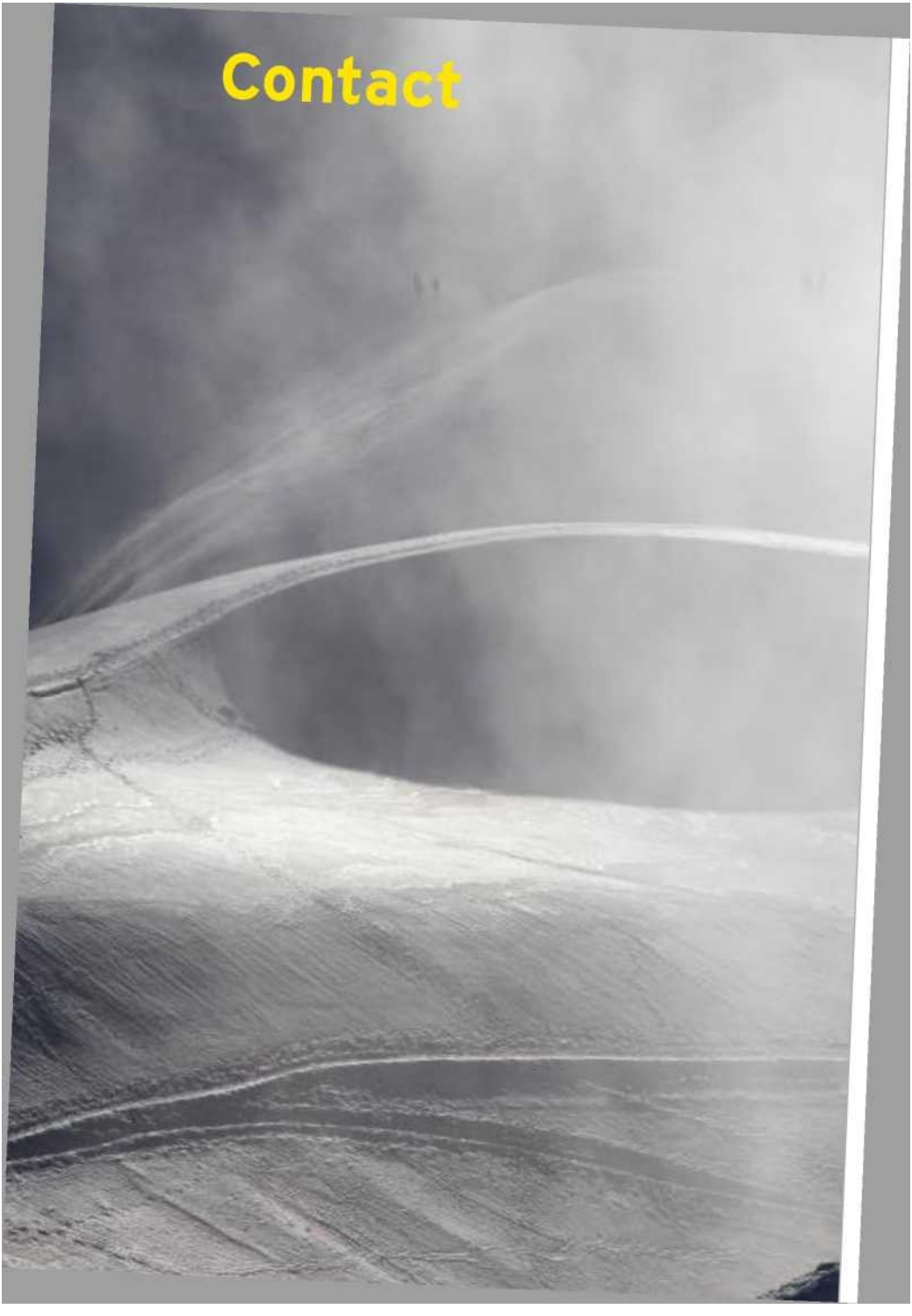






Questions?

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