Distributed ledger alapú megoldások az új eIDAS rendelet fényében

HTE Infokom 2022
Kecskemét

Benedek Péter
Rockwood Group

Miért „DLT”

Az új eIDAS rendeletről

A DLT lehetséges szerepe azonosítási feladatokban

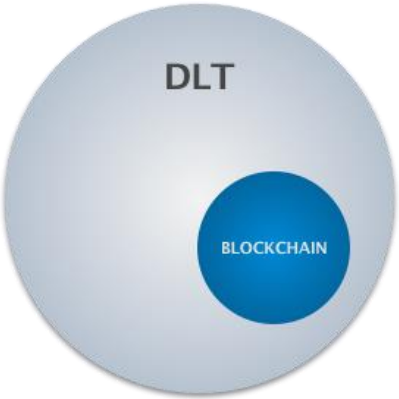
Előnyök – hátrányok

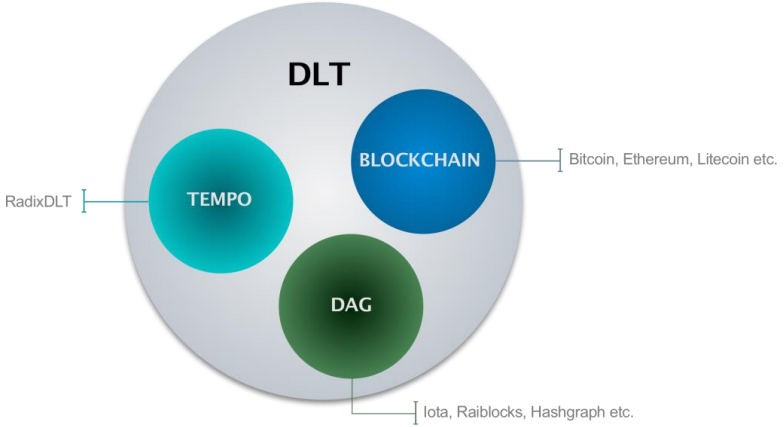
Technológiai szempontok

További lehetőségek

Miért „DLT”

Minden blockchain DLT, de nem minden DLT blockchain





DLT az EU gyakorlatában

Adatvédelem: az EU szigorú adatvédelmi szabályozásának támogatása

Digitális identitás: eIDAS-szal való kompatibilitás, decentralizált és önszuverén identitáskeret támogatása

Kiberbiztonság: magas szintű kiberbiztonság biztosítása

Interoperabilitás: egymás között és a külvilág örökölt rendszereivel is

DLT az EU gyakorlatában

EU szintű stratégia, szervezetek és társulások

Digital Europe Program finanszírozásban pilot projektek

EU szabályozási környezet változása

Az eIDAS 2.0 szabályozásban megjelenő technológiai aspektusok

Az új eIDAS rendelet

Az elektronikus azonosítási, hitelesítési és bizalmi szolgáltatások szabályozási kerete.

- Minden eID jogosult személynek joga van az EU-ban bárhol elismert digitális személyazonossághoz
- SSI - mennyi személyes adatot kíván megosztani az azt igénylő szolgáltatásokkal

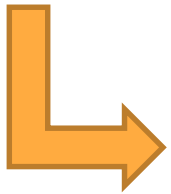
Az új eIDAS rendelet - ewallet

Digitális tárca (ewallet) létrehozásának kötelezettsége

- online és offline azonosítás
- a kormányok által biztosított személyes adatok tárolása és cseréje
- a megbízható magánforrásokból származó információk tárolása és cseréje
- bármely EU tagállamban való tartózkodáshoz, munkavállaláshoz vagy tanuláshoz való jog igazolása

Az új eIDAS rendelet - SSI

Egy kötött attribútum azonosító, amely nyíltan felfed minden személyes adatot az egyénről



Rugalmas self sovereign alkalmazás, amely az összes attribútum feletti irányítást teljes mértékben az egyén kezébe adja.

Az új eIDAS rendelet – DLT elfogadása

Rendeleti úton biztosítja minősített bizalmi szolgáltatók DLT főkönyvi szolgáltatásának elfogadását.

Előírja a biztonság és interoperabilitás minimális szintjét.

A DLT szerepe hiteles azonosítási folyamatokban

Az SSI identitás tulajdonosának biztosítja a lehetőséget, hogy teljes ellenőrzést gyakoroljon identitása és attribútumai felett.

- minden azonosítási attribútumot decentralizáltan tárol
- csak a birtokos döntheti el, hogy kinek ad hozzáférést vagy továbbít azonosító információkat

Az SSI-n alapuló DLT-ben már nincs szükség megbízható harmadik félre

- a DLT-t decentralizált PKI-ként használja: DID megoldások
- tervezésüknél fogva megváltoztathatatlanok

Technológiai aspektusok

A kriptográfiai bizonyítékok használatának kihasználásával a decentralizált attribútum nyilvántartással párosítva nagyon erős fogyasztói adatvédelem és biztonság érhető el.

Az információk csak hozzáférési kulcsként működnek, közvetlenül nem olvashatók.

A zero-knowledge-proof igazolások lehetővé teszik az információk független ellenőrzését anélkül, hogy felfednék, mi maga az információ.

Technológiai aspektusok

A kormányzati eID biztonságos hardverkomponensen kerül tárolásra, és csak az attribútumok tárolása történik az adattárcában szoftverkomponensként.

Megvalósul a biometrikus adatokkal való azonosítás az adott fiókhoz való biztonságos, meghamisíthatatlan hozzáférés biztosítására.

Az ujjlenyomatok, az írisz szkennelés és az egyedi fizikai azonosítók egyéb formái eszközként szolgálnak a hozzáférés megerősítésére.

Köszönöm a figyelmet!