Blockchain + CONIKS
Publiczna weryfikacja prywatnych danych i inne zastosowania

Sebastian Smyczyński

Simplito Computer Science Lab

Blockchain

- Rozproszony rejestr transakcji / stanów
- Globalny konsensus w sieci „wzajemnego niezaufania” (PoW / PoS / PoET / …)
- Publiczna weryfikowalność / transparentność
- Bezpieczeństwo i prywatność

HYPERLEDGER PROJECT

Some of the most innovative companies in the world are actively engaged -- It is a global collaboration of the best and brightest in Finance, Banking, Internet of Things, Supply Chains, Manufacturing and Technology.

PREMIER

accenture
High performance. Delivered.

CME Group

DEUTSCHE BÖRSE GROUP

Digital Asset

DTCC

FUJITSU

HITACHI
Inspire the Next

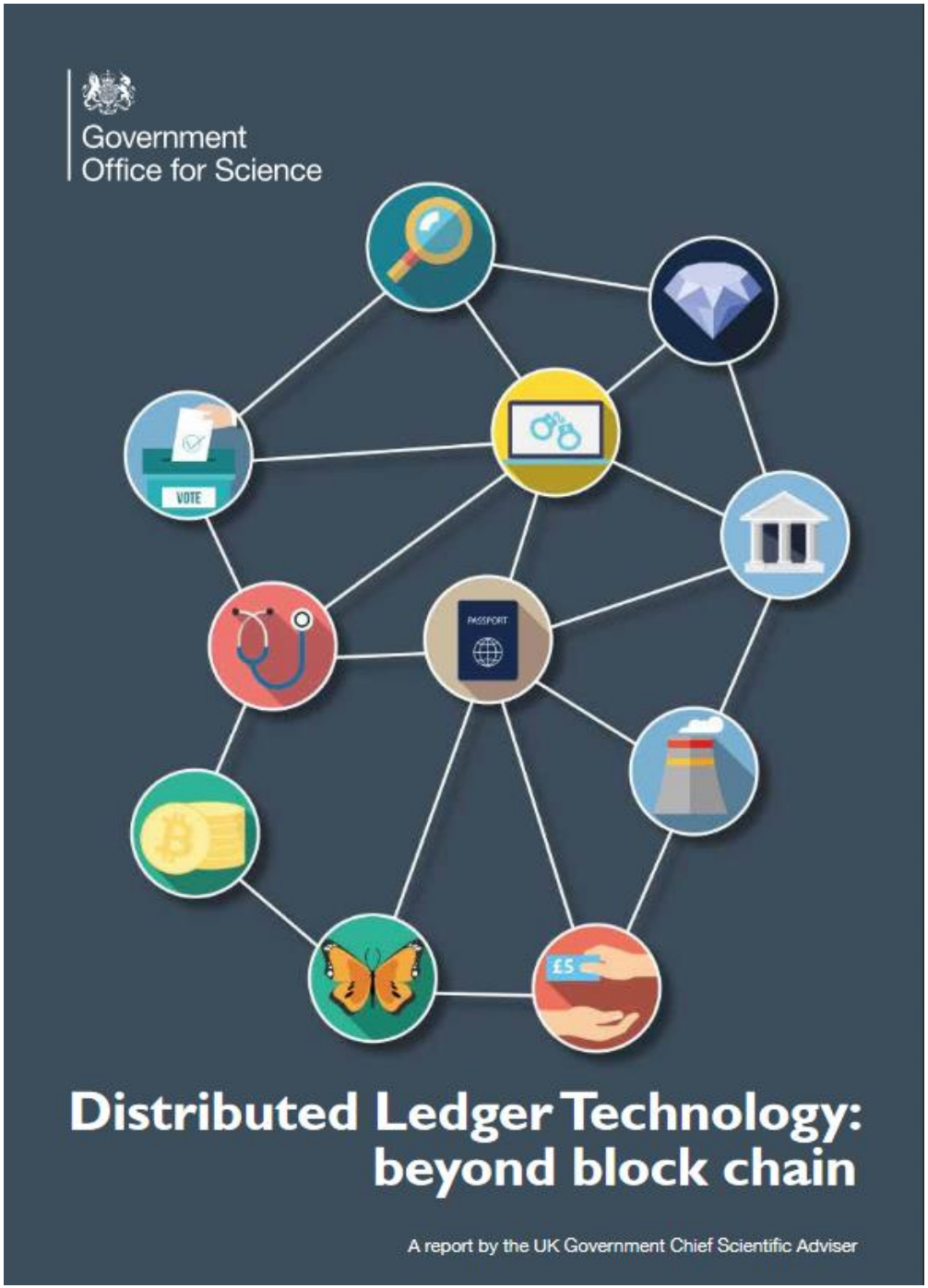
IBM

intel

J.P.Morgan

R

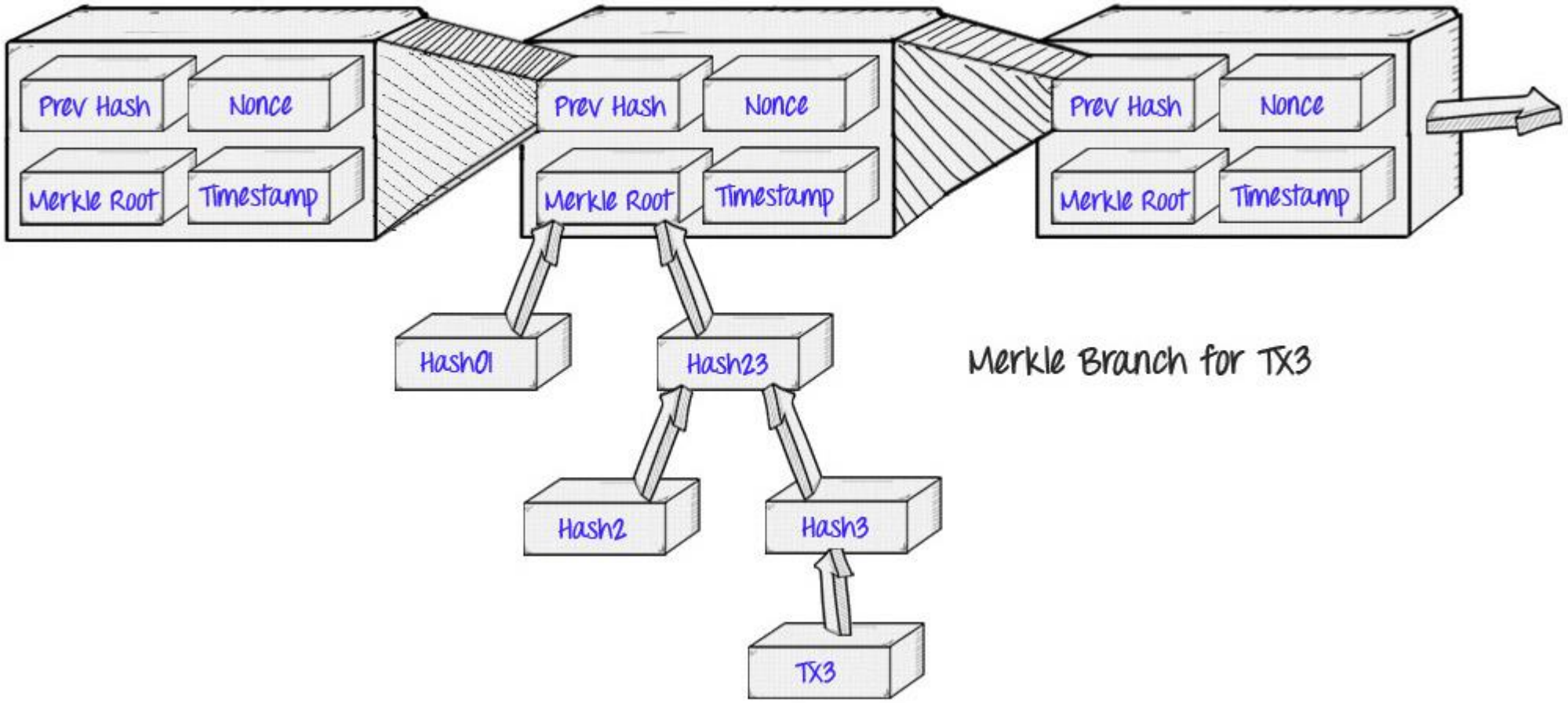
R3CEV konsorcjum ponad 40 instytucji finansowych z całego świata skupione wokół badania zastosowań technologii blockchain w systemach finansowych.


Government
Office for Science
VOTE
PASSPORT
£5
Distributed Ledger Technology:
beyond block chain
A report by the UK Government Chief Scientific Adviser

Publiczna weryfikowalność

- „Dowód istnienia” – dla każdego obiektu, któremu można przypisać unikalny identyfikator
- Zaufane znakowanie czasowe
- Publiczna weryfikowalność prywatnych danych (?)

Simplified Payment Verification



CONIKS: Bringing Key Transparency to End Users

Marcela S. Melara, Aaron Blankstein, Joseph Bonneau[†], Edward W. Felten, Michael J. Freedman

Princeton University, [†]Stanford University/Electronic Frontier Foundation

- Prywatna baza danych z publicznym „skrótem” zawartości
- Historia „skrótów” utrzymywana w strukturze typu blockchain (transparentny log)
- Tylko znając klucz można dostać się do zawartości (opcjonalnie zaszyfrowanej)
- Klucz → index (256 bitów) → ścieżka w merkle tree
- Dla każdegu klucza dostarczany dowód istnienia lub dowód nieistnienia(!) w bazie

privmx

Dziękuję za uwagę

Sebastian Smyczyński

Simplito Computer Science Lab