Χαρακτηριστικά προστασίας ιδιωτικότητας μέσω των μηχανισμών κατανεμημένων μητρώων

Sotirios Brotsis

Cryptography and Security Lab
Dept. of Informatics and Telecommunications
University of the Peloponnese

1η Ημέρα Διαλόγου
με την Ερευνητική Κοινότητα

Research Day ● Oct. 1, 2025

Περιεχόμενα Παρουσίασης

Κίνητρα

Υπόβαθρο και βασικές έννοιες

Τεχνολογίες κατανεμημένων μητρώων

Μηχανισμοί διατήρησης ιδιωτικότητας (on/off-chain)

Προτεινόμενη αρχιτεκτονική

Συμπεράσματα

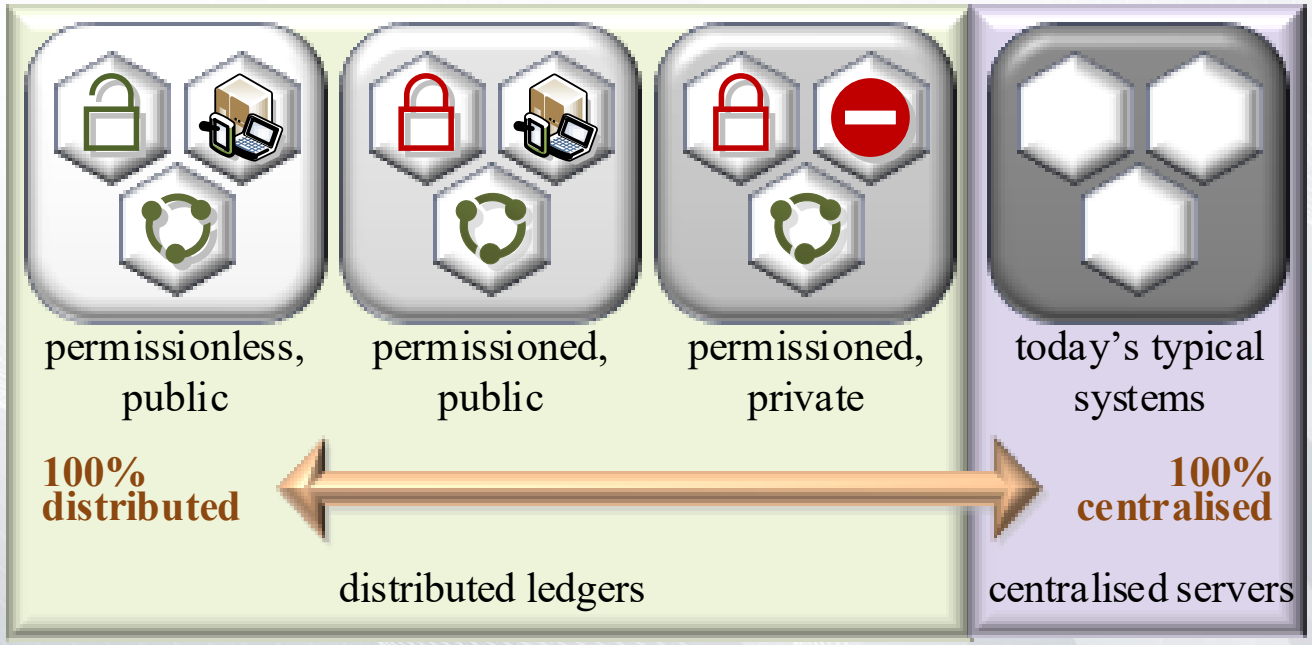
Κίνητρα

- Γιατί η ιδιωτικότητα έχει σημασία σε μηχανισμούς blockchain;
- Ποιες τεχνικές προστασίας της ιδιωτικότητας χρησιμοποιεί η τεχνολογία blockchain;
- Συμμόρφωση των τεχνολογιών blockchain με το δικαίωμα στη λήθη;

Υπόβαθρο: Τεχνολογία Κατανεμημένων Μητρώων

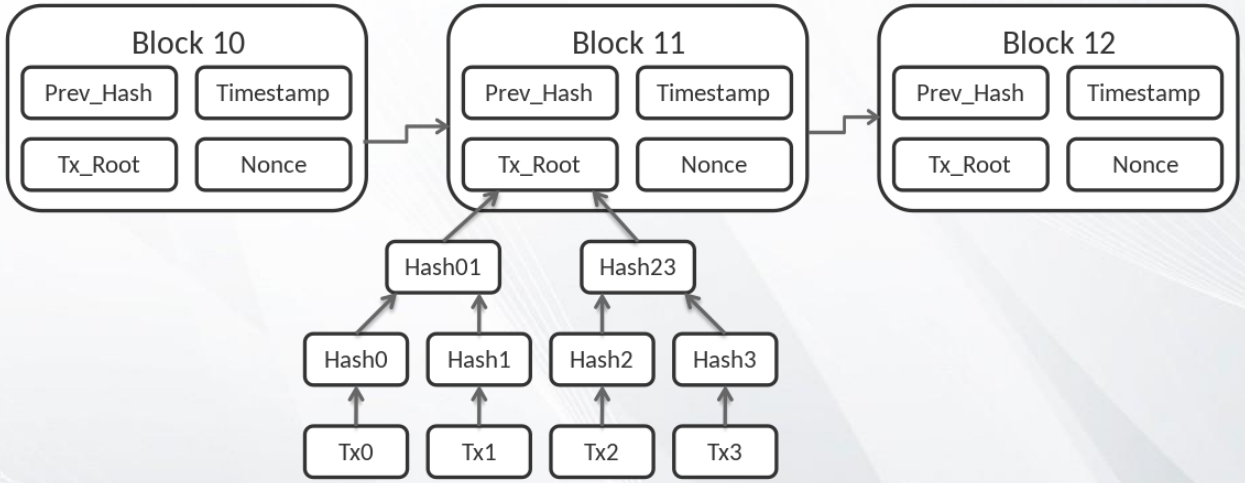
- Κατανεμημένη υπηρεσία/ Χωρίς SPoF
- Χρησιμοποιεί
  - Εκτελέσιμο κώδικα
  - Πρωτόκολλα συναίνεσης
  - Μοντέλα πρόσβασης
    - Χωρίς άδεια

      vs.
    - Με άδεια
      - Δημόσια vs. ιδιωτικά

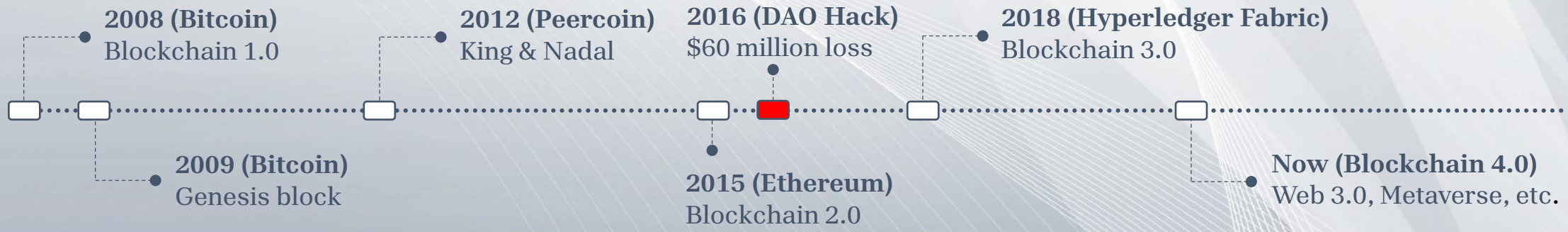


Υπόβαθρο: Τεχνολογία κατανεμημένων μητρώων

Τρόπος Λειτουργίας:



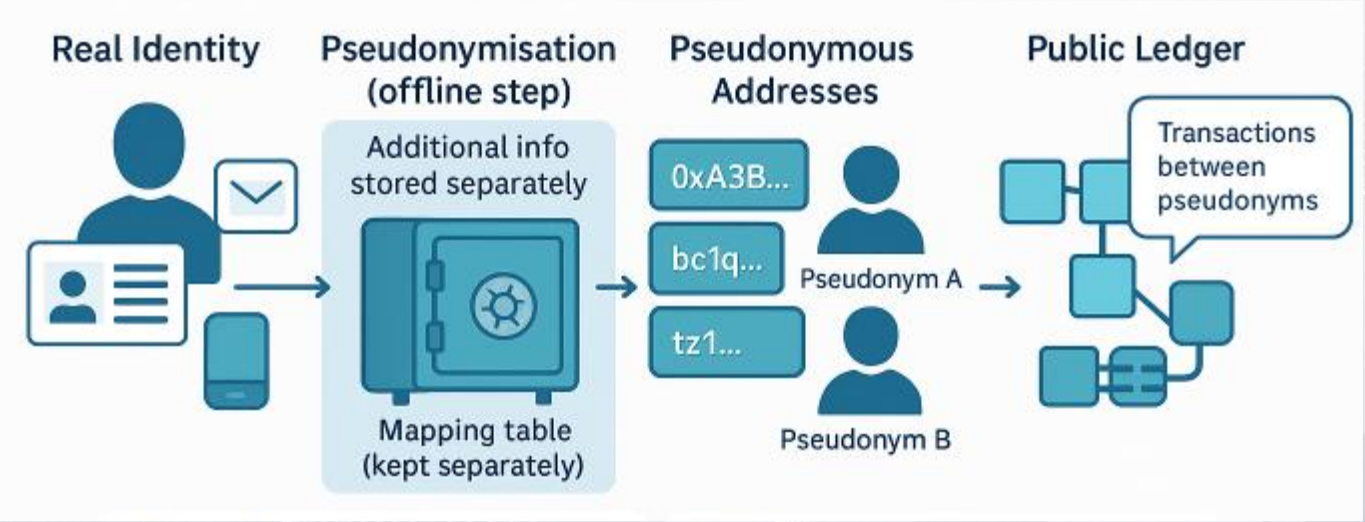
Ιστορική Αναδρομή:



Τεχνικές διατήρησης ιδιωτικότητας: Ψευδονυμοποίηση

Ψευδωνυμοποίηση:

- η επεξεργασία δεδομένων προσωπικού χαρακτήρα
- δεν μπορούν να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων
- χωρίς συμπληρωματική πληροφορία
- διατηρείται χωριστά & υπόκειται σε τεχνικά και οργανωτικά μέτρα
- δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.
- Ψευδωνυμοποιημένα δεδομένα **παραμένουν** δεδομένα προσωπικού χαρακτήρα (και όχι ανώνυμα).

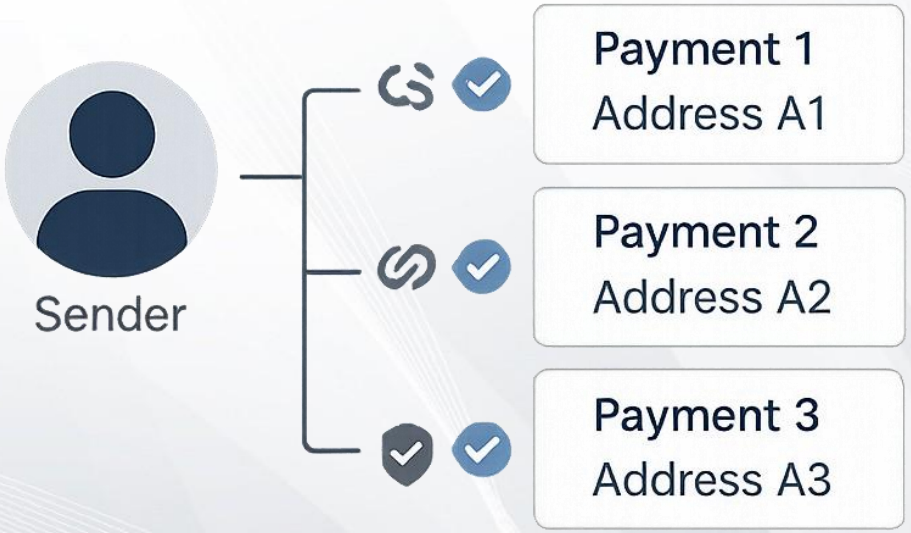


Η δημόσια διεύθυνση κάθε χρήστη είναι πάντοτε η ίδια.
Π.χ. Bitcoin & Silk Road trial
Blockchain platforms: Όλες

Τεχνικές διατήρησης ιδιωτικότητας: Διεύθυνση μίας χρήσης

Διεύθυνση μίας χρήσης:

- μοναδική διεύθυνση που παράγεται για κάθε συναλλαγή
- σπάει η συσχέτιση μεταξύ πληρωμών/χρηστών

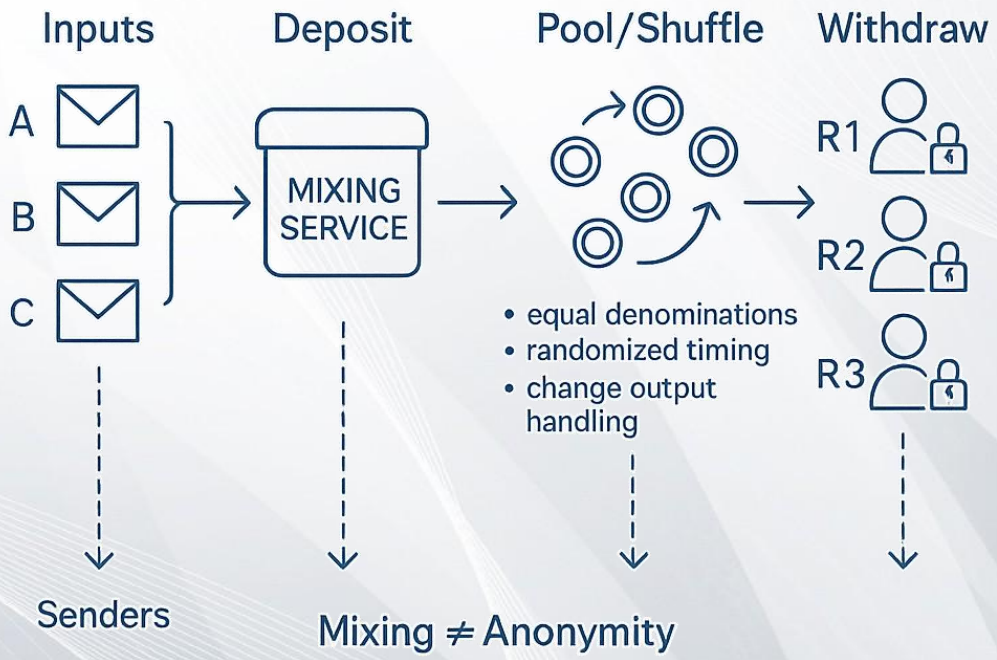


- Blockchain platforms:

Bitcoin, Ethereum, Monero & Ripple.

Τεχνικές διατήρησης ιδιωτικότητας: Τεχνικές ανάμειξης

- Αποστολή κρυπτο-νομίσματα σε “χώρο ανάμειξης”.
- Τα ποσά «σπάνε» και αναμειγνύονται.
- Παραλαβή νομισμάτων σε νέες διευθύνσεις.
- Δυσδιακριτότητα σε είσοδο και σε έξοδο.
- Συν: Απλότητα, μεγάλα pools.
- Πλην: Εμπιστοσύνη σε τρίτα μέρη.

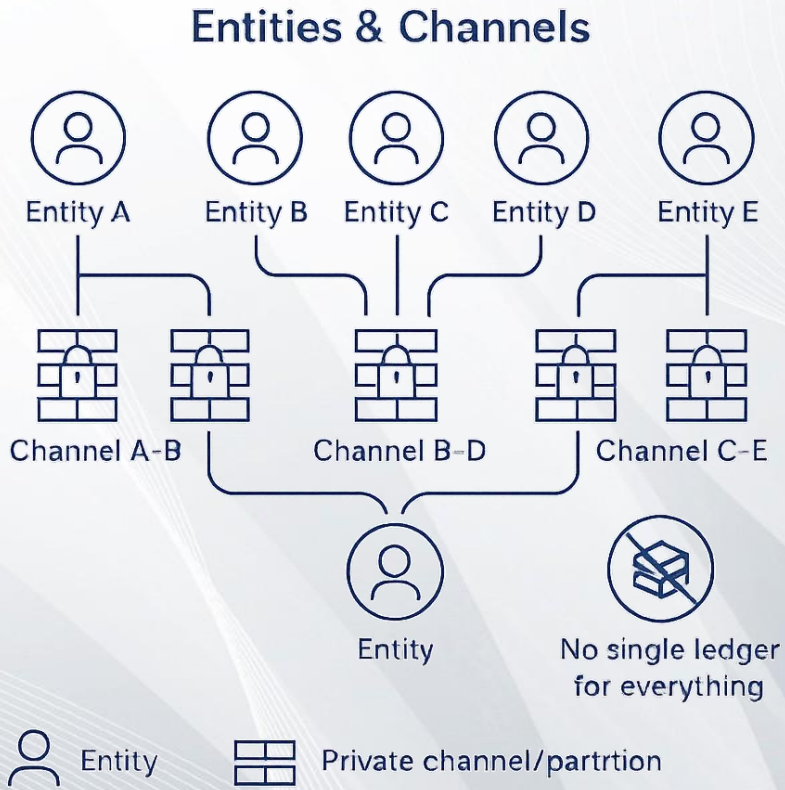


- Blockchain platforms:

Bitcoin, Ethereum & IOTA.

Τεχνικές διατήρησης ιδιωτικότητας: Διαχωρισμός blockchain

- Δεν υπάρχει διαμοιρασμένο μητρώο
- Κανόνες ελέγχου πρόσβασης
- Κάθε συμμετέχων έχει πρόσβαση μόνο σε ένα υποσύνολο των συναλλαγών
- Μη εξουσιοδοτημένοι κόμβοι δεν έχουν πρόσβαση

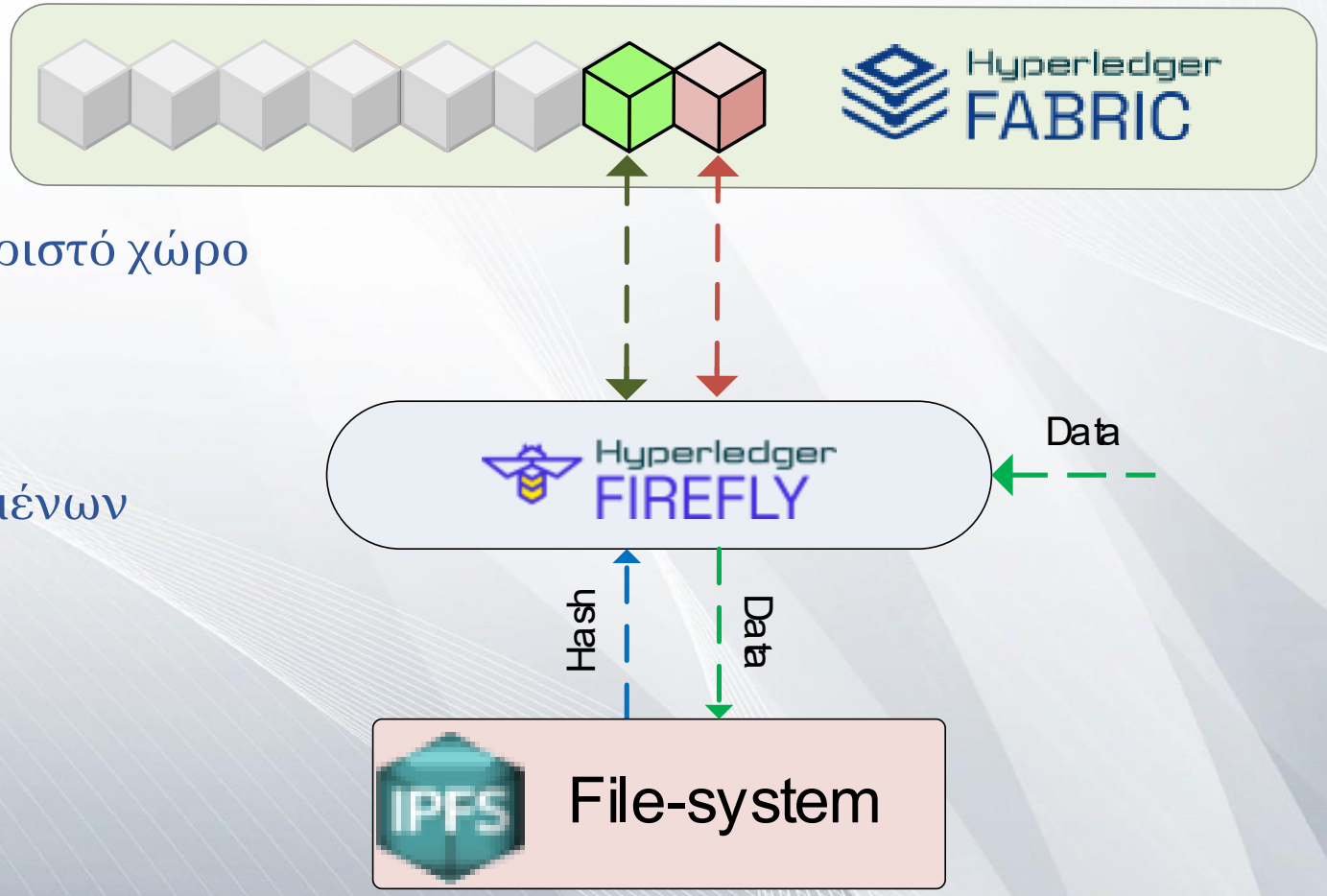


- Blockchain platforms:

Corda, Hyperledger Fabric, Hyperledger Iroha and EOSIO

Τεχνικές διατήρησης ιδιωτικότητας: Αποθήκευση εκτός αλυσίδας

- Τα δεδομένα αποθηκεύονται σε ξεχωριστό χώρο αποθήκευσης
- Π.χ. στην IPFS
- Μια κατακερμάτιση αυτών των δεδομένων
- Blockchain platforms: all



Άλλες Τεχνικές διατήρησης ιδιωτικότητας

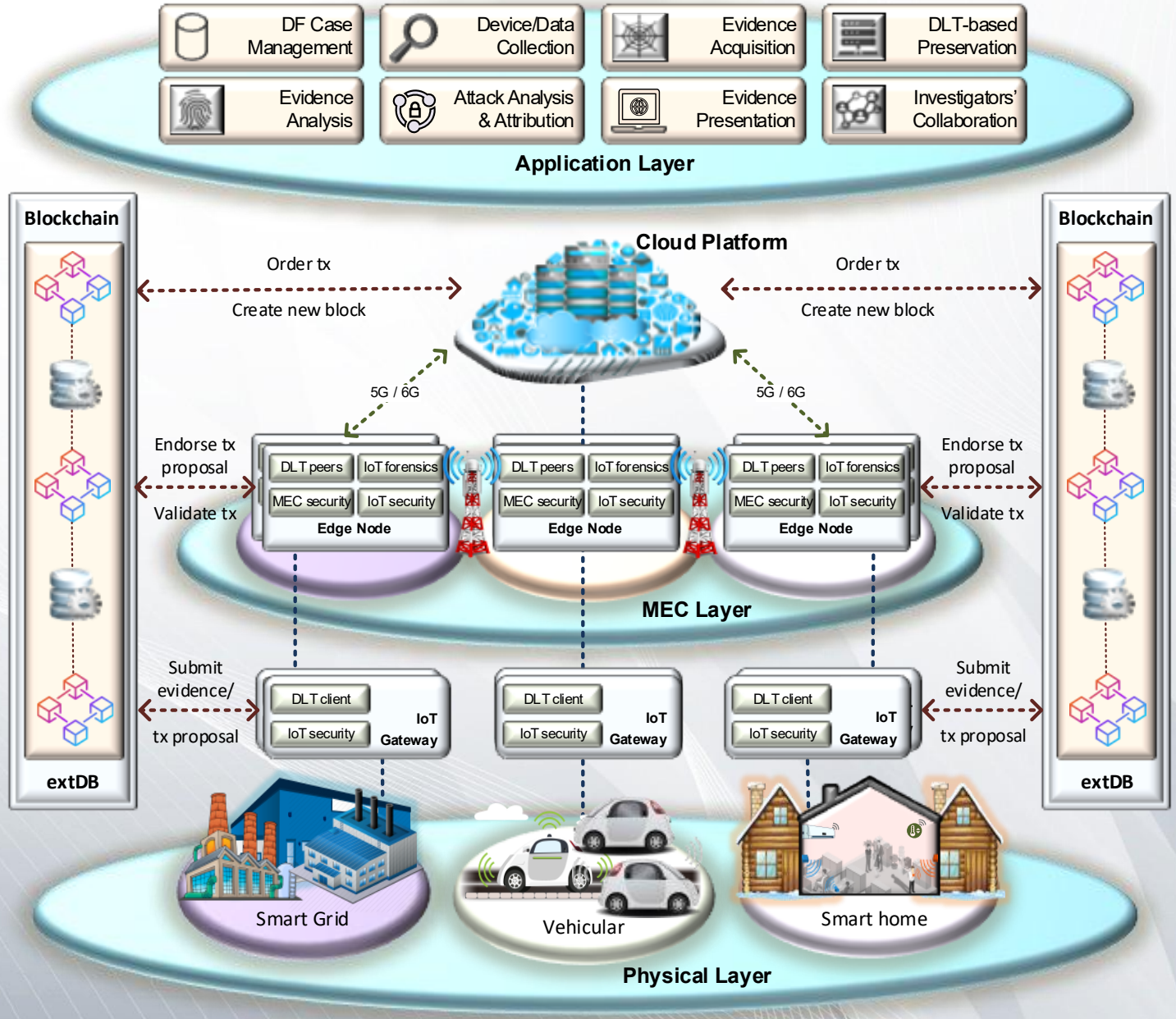
Τεχνικές	Δακτυλιοειδής υπογραφή	ZK-Proofs	Συναλλαγές με απόρρητο
Σκοπός:	Αποκρύπτουν την ταυτότητα του αποστολέα	Αποκρύπτουν τις λεπτομέρειες μιας συναλλαγής	Αποκρύπτουν τα δεδομένα κάθε συναλλαγής
Επίπεδο ιδιωτικότητας:	Δεν αποκρύπτουν την ταυτότητα του παραλήπτη και τα δεδομένα κάθε συναλλαγής	Αποκρύπτουν αποστολέα, παραλήπτη και δεδομένα κάθε συναλλαγής	Δεν αποκρύπτουν αποστολέα, παραλήπτη
Blockchain platforms:	Monero, Ethereum, IOTA, Hyperledger Iroha, Stellar, Tron, Ripple και Algorand	Zcash, Ethereum, Quorum, Ouroboros, Tron, Fabric, Stellar, Tezos, Corda, Zerocoin	Quorum, Hyperledger Besu, Sawtooth και Fabric, Symbiont, Ethereum, Ouroboros και Bitshares,

Τεχνικές διατήρησης ιδιωτικότητας: Επεξεργάσιμα (redactable) blockchains

- Αμεταβλητότητα σε μηχανισμούς blockchains
- Υπάρχει δικαίωμα διαγραφής δεδομένων – Δικαίωμα στη λήθη;
- Τρόποι αντιμετώπισης
  - Ένα νέο transaction που δηλώνει διαγραφή.
  - Αποθήκευση εκτός αλυσίδας
    - Υψηλά προνόμια πρόσβασης
    - π.χ. μια αρμόδια αρχή, να αλλάζει ή να διαγράφει δεδομένα

Προτεινόμενη αρχιτεκτονική

- Εφαρμογές τεχνολογιών κατανεμημένων μητρώων στην ασφάλεια ψηφιακών πειστηρίων του Διαδικτύου των Πραγμάτων (ΔτΠ)



Συμπεράσματα

- Μια δημόσια (permissionless) πλατφόρμα κατανεμημένων μητρώων εγείρει περισσότερες ανησυχίες για την ιδιωτικότητα από μια ιδιωτική (permissioned).
- Ο αριθμός των υιοθετημένων μηχανισμών ιδιωτικότητας δεν οδηγεί σε συμπέρασμα για το αν διατηρείται ή όχι η ιδιωτικότητα
- Ορισμένα χαρακτηριστικά ιδιωτικότητας μπορεί σε κάποιες περιπτώσεις να είναι περιττά, ενώ σε άλλες —αντιθέτως— ανεπαρκή

Αναφορές

- Brotsis, S., Limniotis, K., Bendiab, G., Kolokotronis, N., & Shiaeles, S. (2021). On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance. Computer Networks, 191, 108005.
- Brotsis, S., Grammatikakis, K. P., Kavallieros, D., Mazilu, A. I., Kolokotronis, N., Limniotis, K., & Vassilakis, C. (2023). Blockchain meets Internet of Things (IoT) forensics: A unified framework for IoT ecosystems. Internet of Things, 24, 100968.
- Brotsis, S., Kolokotronis, N., Limniotis, K., Bendiab, G., & Shiaeles, S. (2020, October). On the security and privacy of hyperledger fabric: Challenges and open issues. In *2020 IEEE World Congress on Services (SERVICES)* (pp. 197-204). IEEE.
- Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., & Pavué, C. (2019, June). Blockchain solutions for forensic evidence preservation in IoT environments. In *2019 IEEE conference on network softwarization (NetSoft)* (pp. 110-114). IEEE.

Questions and answers