An IoT-friendly Blockchain for Coordination and Accountability

Danny Adams, Gloire Rubambiza, Xinwen Wang,
Robbert van Renesse, Hakim Weatherspoon, and Stephen B. Wicker

Real world problems

Our Solution

Emergency Responders work in challenging environments

Emergency Responders & Network Access

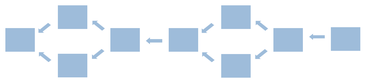
- Infrastructure can be damaged during a disaster
- Some locations may have intermittent or no network access

Medical Records

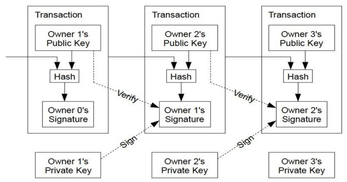
- Access to health records is essential to victim care
- However:
  - Providing secure and quick access to privacy-sensitive records is difficult
  - Need a way to secure and audit all accesses

Vegvisir

- Means “Roadmap” in Icelandic
- Runs on IoT devices, such as smartphone, tablets.
- Works with intermittently connected network
- Properties:
  - Consistency:
    - CRDT State Machine
    - State Reconciliation Protocol
  - Tamperproof:
    - “Proof-of-Witnesses”

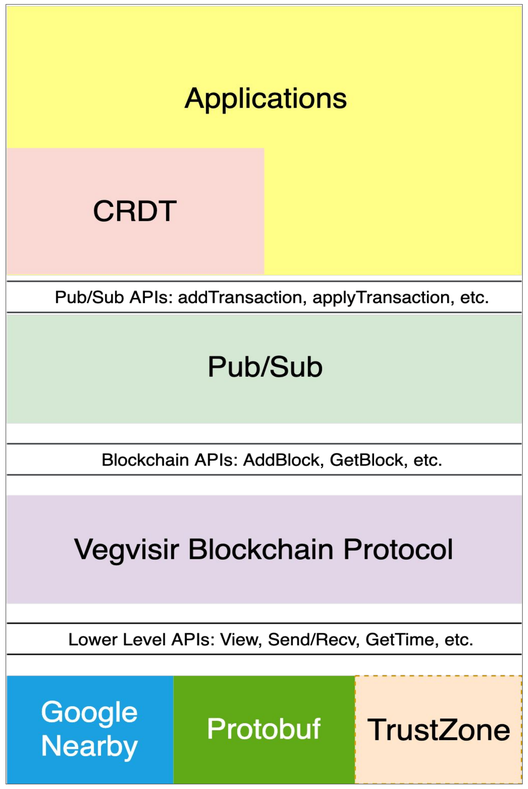


Blockchain & Tamperproof Log



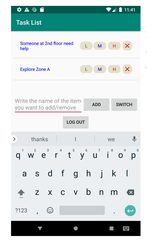
- A growing list of records (“blocks”) that are linked and secured cryptographically
- Individual blocks cannot be altered once committed (Tamperproof)
- Decentralized and Distributed
- Can be used for virtually any data, not just cryptocurrency

Vegvisir Structure



Sample Applications

Task List



Collaborating and sharing tasks with other teams.

Annotated Map

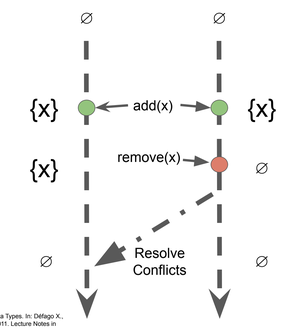
Sharing locations and knowing what is happening directly on map.

Working without Internet connection
Syncing up with other devices opportunistically

CRDT

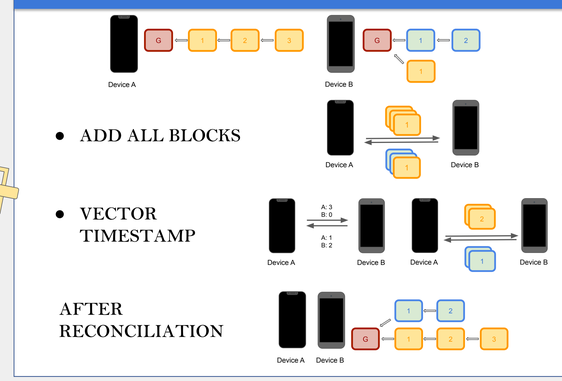
Conflict-free Replicated Data Type[1]

- A replicated data structure
- Concurrent updates must commute
- Replicas can be updated independently
- Basic CRDTs form registers, counters, sets



[1] Shapiro M., Preguiça N., Baquero C., Zawirski M. (2011) Conflict-Free Replicated Data Types. In: Défago X., Petit F., Villain V. (eds) Stabilization, Safety, and Security of Distributed Systems. SSS 2011. Lecture Notes in Computer Science, vol 6976. Springer, Berlin, Heidelberg

Reconciliation Protocols



Current & Future Projects

Acknowledgements:

- This work was partially funded and supported by NIST Information Technology Laboratory (60NANB15D327 & 70NANB17H181).
- **Special Contributions**: Aniroodh Ravikumar, Karan Newatia, Runde Yang, Zhengxun Wu, Zitao Zheng, Zangyueyang Xian, Edwin Ma, Weitao Jiang, Sherbin Abraham, Ning Ning Sun, Andreas Unterweger, Yi Jiang, Kolbeinn Karlsson