Untethered: Deployable Blockchains for IoT Environments

Kolbeinn Karlsson, Danny Adams, Gloire Rubambiza, Zangyueyang Xian,
Robbert van Renesse, Hakim Weatherspoon, and Stephen Wicker
Cornell University

CCS CONCEPTS

• **Computer systems organization** → **Peer-to-peer architectures**; • **Security and privacy** → *Privacy-preserving protocols*; • **Networks** → Peer-to-peer protocols; • **Theory of computation** → Distributed computing models; • **Software and its engineering** → Distributed systems organizing principles;

KEYWORDS

blockchain, tamper-proof logging, accountability, ad hoc networks, Internet of Things, gossip protocols, Edge Clouds

The popularity surrounding blockchains has naturally led to research into its applicability in many areas. However, Nakamoto-style blockchains possess several characteristics that make them inappropriate for many purposes in the Internet of Things (IoT) domain. Notably, they are power-intensive and require high network connectivity. These requirements are fundamentally incompatible with IoT where nodes may have limited power and sporadic network access.

We are designing a blockchain approach for IoT environments called *Vegvisir*. Vegvisir is a partition-tolerant blockchain for use in power-constrained IoT environments with limited network access. Under the hood, it is a membership-based, directed acyclic graph (DAG)-structured blockchain [1]. It is motivated by and ideally suited for paramedics and firefighters in disaster scenarios. For instance, it can be used to aid in many tasks during disaster response where network connectivity is poor or nonexistent; namely, it is a blockchain, so provides the abstraction of an append-only log of transactions that is tamperproof.

Utilizing a distributed trust model, Nakamoto-style blockchains are free from centralized control and single

point-of-failures. As long as a large enough fraction of participants follow the protocol correctly (usually greater than 50%), its security properties will be preserved in a system that is both strongly consistent and highly available. A key to Nakamoto-style blockchains is proof-of-work, a crypto puzzle that has to be solved to create new blocks. While this feature adds to its security, it makes blockchains dependent upon network access and a significant power source [2].

Our research dramatically reduces power consumption by replacing proof-of-work with *proof-of-witness*. A proof-of-witness requires that a block has spread to k neighbors and has been sufficiently propagated within the network to certify the activity has been logged.

In regards to limited network access and partitions, Vegvisir is implemented with CRDTs, conflict-free replicated data types [3]. CRDTs remove the need for constant network access since they are always conflict-free. In particular, CRDTs are associative, commutative and idempotent. Counters and 2P sets are examples of CRDTs. With the properties of CRDTs, a fully distributed set of blocks will resolve to the same overall blockchain; thus, making Vegvisir an ideal platform for deploying in IoT environments.

In summary, Vegvisir is a low-powered, DAG-structured, blockchain that greatly extends the range of applications for which blockchain technology can provide tamper-proof distributed logging. We continue to explore emergency preparedness applications, while extending our work to digital agriculture and the tracking of food products.

Acknowledgements

This work was partially funded NSF (CSR-1422544) and NIST (60NANB15D327 and 70NANB17H181), Cisco, Intel, Facebook, Infosys, and Amazon.

REFERENCES

- [1] Kolbeinn Karlsson, Weitao Jiang, Stephen Wicker, Danny Adams, Edwin Ma, Robbert van Renesse, and Hakim Weatherspoon. 2018. Vegvisir: A Partition-Tolerant Blockchain for the Internet-of-Things. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. IEEE.
- [2] Karl J O'Dwyer and David Malone. 2014. Bitcoin mining and its energy footprint. (2014).
- [3] Marc Shapiro, Nuno Preguiça, Carlos Baquero, and Marek Zawirski. 2011. Conflict-free replicated data types. In *Symposium on Self-Stabilizing Systems*. Springer, 386–400.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

SoCC '18, October 11–13, 2018, Carlsbad, CA, USA

© 2018 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-6011-1/18/10.

<https://doi.org/10.1145/3267809.3275450>