MS CS thesis proposal: Towards decentralized digital banking for the unbanked

December 13, 2020

1 Background

Blockchain and distributed ledger technology. Blockchain and distributed ledger (BC/DL) technology facilitates managing ownership of digital resources by pseudonymous users under decentralized governance, that is without a single authority or party controlling or having privileged access to processes or data compared to other parties.

A BC/DL system is commonly realized as a dynamic, partially synchronous peer-to-peer computer network that maintains consensus on a single tamper-proof append-only log of digitally signed events. These events include transfers of ownership of digital resources such as electronic money and tokenized (that is, digitally represented) assets, rights and objects. An event is considered *validated* once an honest peer in the BC/DL system reports that it is appended to the log with 100% or at least very high probability.

In this fashion, a BC/DL system provides a decentralized platform for implementing a bank account system: Accounts containing *digital money* (cryptocurrency) can be controlled by pseudonymous users using standard public-key cryptography; they can confidentially authorize *payments*, that is money transfers to other accounts, which are settled and thus irrevocably performed, once they are validated by the BC/DL system. Being decentralized means that the bank account system is not run or controlled by a single party such as a government, a regulatory body, a bank, a banking system (an association of banks), or a cloud/data center provider hosting the accounts and monitoring authorization and/or validation of events.

Banking the unbanked. Basic banking is the efficient, secure and trusted of ownership, storage and transfer of money. Basic digital banking is basic banking that provides these services simultaneously quickly and over long distances by using computers, ranging from mainframe and laptops to cell phones and embedded devices, attached to computer networks. Basic digital banking is a necessary foundation for secure and effective trading (commercial contracts, that

is money for goods-and-services) and core banking services (financial contracts, that is money-now for money-later).

Basic digital banking is unfortunately still inaccessible, unaffordable, manual/inefficient or untrusted in some regions around the world, such as those with substantial poverty, corruption, no or weak rule of law, untrusted government, or dominant private actors. It is noteworthy that many such regions *do* have a rather reliable and commonly trusted digital networking infrastructure, with even the poorest users owning a mobile, fully-programmable computer that would be considered *very powerful* in the richest of countries only 20 years ago: a smartphone.

2 Goals

The overall goal of this project is to explore, develop and evaluate (eventually) decentralized technology for *banking the unbanked*; that is trustworthy basic digital banking that is scalable, sustainable, affordable, fair, and effectively available, usable and acceptable by people that are presently unbanked.

Specific objectives are:

- The design, implementation and demonstration of a modular, configurable software architecture suitable for basic smartphone-based digital banking supporting payments and atomic exchanges of digital assets (payment versus payment, payment versus delivery), and suitable for both centralized and (eventually) decentralized implementation.
- Optionally, discuss, design and prototype decentralized implementations that
  - employ a trusted backbone network for availability for crash fault tolerance;
  - employ a scalable and (energy-)efficient blockchain or distributed ledger system, permissioned or nonpermissioned, for Byzantine fault tolerance;
  - support safe (finally settled) transactions in off-line mode;
  - take into account theoretical and practical trade-offs between desirable properties such as availability, consistency, partition tolerance, fault tolerance, privacy, scalability, implementation complexity and cost.

The fundamental research hypothesis is that these objectives are effectively achievable by following a staged approach of designing a modular software architecture; rapid prototyping using proven (centralized) database technology; evaluating its adequacy for smartphone-based basic digital banking for the hitherto unbanked; subsequently gradually replacing centralized components by distributed and decentralized services; supporting effectively settled transaction in

off-line mode; and eventually using the users' smartphones themselves, without a separate backbone network, as the network implementing a decentralized basic digital banking system. (The latter parts of the hypothesis are not expected to be reached in this project.)

3 Tasks

- Baseline:
  - Identify and investigate a relevant context (target group) where basic digital banking is lacking and is to be facilitated in the present project; see e.g. [Hen18].
  - Identify, read and analyze available literature, artifacts and software repositories on the state of the art in basic digital banking, paying attention to the interplay of technology, socio-political context and practical experiences relevant in the identified context.
  - Analyze (partially based on above, partially based on functionality of basic digital banking system requirements) and specify *modular* system requirements (functionality) of a basic digital banking system for one (crypto)currency, including authentication and authorization, account-to-account transfers, activity monitoring/reporting. The modules should facilitate rapid adaptation to multiple or changing requirements (e.g. support for a range of authentications, from fully anonymous numbered ("Swiss") accounts (no authentication) to proof of identity of a designated certificate authority) rather than have baked-in/hardwired protocols that are hard or impractical to change.
    - Discuss account-based and token-based representation of resource ownership, how they relate to each other and how they facilitate transfers.
  - Design, code and test a centralized (server-hosted) system that implements the specification, using standard technology such as an RDBMS.
  - Identify simple, but practically relevant (in the identified context) authentication/authorization, transfer and monitoring/reporting protocols and implement them.
  - Provide a simple (web) app that exercises and illustrates basic digital banking by using the implemented server-based system on a simple smartphone.
- Multiple resource types: Extend the account system and resource transfer functionality with support for multiple resources; in particular, support atomic resource exchanges, e.g. payment versus [token] delivery. See e.g. [TG20].

- Decentralization:
  - (Re)implement the system specification using a small P2P network of trusted nodes (no Byzantine nodes) with crash-fault tolerance and acceptable energy consumption, latency and throughput such as Hyperledger Fabric [ABB+18].
  - Investigate other BC/DL systems and analyze their appropriateness as a (partially) synchronous decentralized *backbone network* for basic digital banking, taking the identified context requirements and fundamentals of distributed systems [Asp18] into account.
- Disconnected mode:
  - Analyze the requirements for disconnected mode (offline) operation in the given context, in particular finalized (de facto settled) smartphone-based payments and exchanges amongst participants while disconnected from the backbone network.
  - Research, design and prototype disconnected mode transactions; see e.g. [ILK19].
- Discuss hosting the peers of the backbone network on the users' smartphones instead of a separate backbone network, that is providing basic digital banking hosted by a BC/DL system running exclusively on users' smartphones.

All tasks and associated objectives past the baseline are *optional*. The references are only indicative seed entries into the literature.

4 Learning objectives

- Describe and explain the basic characteristics, designs, properties and trade-offs in blockchain and distributed ledger technology.
- Analyze, design, implement, test and evaluate a modular software architecture that is adequate for identified basic digital banking requirements.
- Investigate and discuss how existing BC/DL technology can be employed to provide a decentralized backbone network for affordable and available smartphone-based basic digital banking in regions with basic wireless networking.
- Research and discuss how payments and atomic exchanges can be finalized (settled) by smartphone users while being offline (from the backbone network) for extended periods of time.

References

[ABB+18] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. Hyperledger Fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, page 30. ACM, 2018.

[Asp18] James Aspnes. Notes on theory of distributed systems. Lecture Notes for CPSC 465/565, Fall 2017, February 2018.

[Hen18] Fritz Henglein. Virtual savings and loan associations: Peer-to-peer banking and trading based on low-power smartphones. Project proposal to CARE Denmark, June 2018.

[ILK19] Ikechi Saviour Igboanusi, Jae-Min Lee, and Dong-Seong Kim. NFC Pure Wallet (PW): An offline and real-time blockchain transaction architecture. Preprint, December 2019.

[TG20] Juan-Manuel Torres Garcia. Algebraic resource accounting for transfers and transformations. Master's thesis in computer science, Department of Computer Science, University of Copenhagen (DIKU), September 2020.