Demo: A Delay-Tolerant Payment Scheme on the Ethereum Blockchain

Ahsan Manzoor[‡], Yining Hu[*†], Madhusanka Liyanage[‡], Parinya Ekparinya,[§], Kanchana Thilakarathna[§], Guillaume Jourjon[†], Aruna Seneviratne[*†], Salil Kanhere[*] and Mika E Ylianttila,[‡]
[‡]University of Oulu, Finland, [*]University of New South Wales, Australia,
[†]Data61-CSIRO, Australia, [§]University of Sydney, Australia
Email: [†]firstname.lastname@data61.csiro.au, [‡]firstname.lastname@oulu.fi, [§]pekp6601@uni.sydney.edu.au,
[‡]firstname.lastname@unsw.edu.au, [§]kanchana.thilakarathna@sydney.edu.au

***Abstract*—Cash-less payment via a variety of credit, debit or prepaid cards is pervasive in our interconnected society, but not so ubiquitous in remote rural regions where network connectivity is intermittent. We proposed a cash-less payment scheme for remote villages based on blockchains that allow maintaining a record of verifiable transactions in a distributed manner. We overcome the limitations of intermittent network connectivity by solely relying on blockchain mining nodes in the village for transaction processing and verification. The bank joins as a peer and monitors node behaviors, rewards miners and processes currency exchanges whenever the connectivity is available. We take advantage of the Ethereum network to develop our solution and demonstrate the feasibility of the proposed system on off-the-shelf computing devices. We emulate a remote village scenario with intermittent network connectivity and show the robustness and reliability of the proposed system.**

I. Introduction

Mobile operators starting businesses in rural areas often face challenges associated with limited roadway connectivity, high equipment maintenance and protection costs, and high staff salaries. As a consequence, most of the pervasive services that are taken for granted in always-connected regions cannot be provided in real-time in these connectivity-restricted environments. This has led to the development of techniques to support services masking intermittent connectivity [5].

One of the services in high demand is banking. The unreliable connectivity and high cost of transport and infrastructure make it hard and impractical for banks to build branches or set up ATMs in some rural regions. The only possibilities have been to leverage the short message service (SMS) or Unstructured Supplementary Service Data (USSD) of cellular networks. This is exemplified by the BAAC in Thailand [2]. However, a lack of proper encryption on SMS messages makes them insecure and hence require additional verifications that inevitably cause more burden for the customers, while USSD is session-based and does not enable local storage so users can only access their account information within certain sessions. More recently, cryptocurrencies have received massive attention and are regarded by many as a potential revolution of the banking industry [3]. The technology behind, the blockchain, is secured by hard-coded programs and enables peer democracy for transaction verification. Global-level cryptocurrencies such as Bitcoin [4] and Ethereum [6] rely on consistent network connectivity for data exchange are not accessible for rural communities with intermittent connectivity. Nonetheless, if blockchain could be made to work in intermittently connected environments, it will be possible to deliver augmented banking services to remote regions.

Without being always connected to the broader Internet, a reliable local connectivity could be accomplished, for example, with the Nokia Kuha [1] small-cell base stations that are on the one hand connected to the wider Internet intermittently and on the other hand offering 4G coverage within the village. In our system design, a bank, which leads the deployment of the system, utilizes the intermittent connectivity and only periodically accesses the village network to monitor system operation. Instead of building physical infrastructures such as branches or ATMs, the bank distributes the verification and storage tasks to villagers through a self-regulated system that is able to process and record transactions securely. In the case of blockchains, this can be achieved by bank supplying mining equipment and granting permissions to selected (trusted) volunteers[1].

In this demo, we show the viability of realizing the proposed architecture through a prototype implementation with off-the-shelf laptops and mobile devices. Section II describes the system architecture and Section III presents a prototype implementation. Section IV gives an overview of the showcase we intend to present at the Demo Session, followed by Section V which specifies a set of technical requirements.

II. System Architecture

Our system design enables seamless use of cash-less payment within a remote community that is intermittently connected to the bank's central network. Figure 1

[1]A teaser video about this demonstration is published here: https://research.csiro.au/ng/research/network-measurement-modelling/distributed-delay-tolerant-payment-blockchains/

978-1-5386-4725-7/18/$31.00

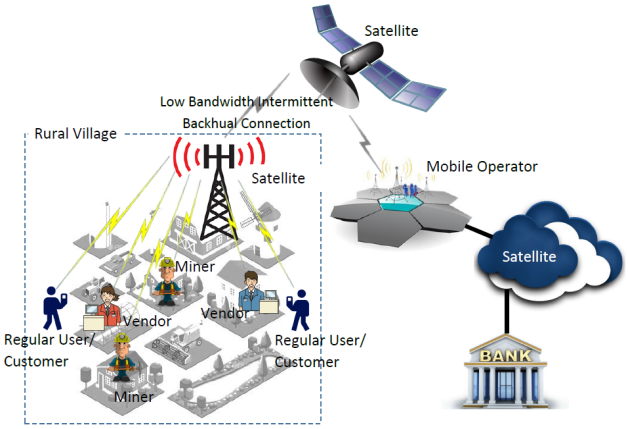

Fig. 1: System architecture.

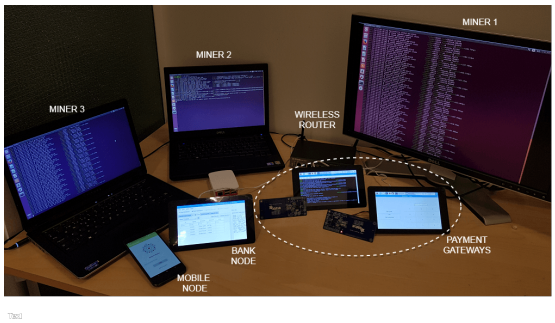

Fig. 2: Prototype implementation

graphically illustrates the scenario where a local operator provides a 4G LTE cellular network coverage to the inhabitants via a base station, similar to Nokia Kuha [1]. The backhaul network can be an unreliable low-bandwidth satellite or a long-range microwave connection. We propose to use a private Ethereum blockchain [6] for transaction processing within the village, restricting mining rights to only a set of qualified (trusted) users. We also create our own Token[2] for money circulation in the local community that behave similarly to Ethers except they are issued via a smart contract by the bank.

The proposed network consists of three types of nodes, i.e. *miners*, *full nodes* and *light nodes* hosted by three different players, i.e. *the bank*, *vendors* and *regular users*. The bank distributes authorized mining equipment to a set of selected villagers and compensates them for the electricity power consumed leveraging the Token-based rewarding scheme of Ethereum through a smart contract. Vendors may choose to implement full nodes as payment gateways and keep a complete transactional record. Regular users with mobile devices can join the system by running light nodes that are deployed in the form of a customized wallet app. Miners and full nodes require dedicated computing resources and are preferred to always be active. In order to monitor the village network and keep track of transactions, the bank operates a passive full node, which does not create any forks even in an intermittently connected, asynchronous setting.

The bank creates one fiat account and one digital account for each user to record the user balance in both currencies. When the connection between the bank and the village is established, it synchronizes with other blockchain nodes, updates user balances and processes requests for money exchange transactions. The bank also takes necessary actions in case of malicious behaviors such as suspicious transactions, network partitioning and misbehaving miners.

[2]https://www.ethereum.org/token

III. Prototype Setup

We demonstrate the feasibility of the system design with a prototype implementation containing a private Ethereum blockchain with an intermittently connected bank node.

Figure 2 illustrates the setup containing a bank full node, 2 shops, and 3 regular users. Each shop runs a mining node and in addition, Shop 1 owns two full nodes and Shop 2 owns one full node. Regular User 3 operates a miner while the other two regular users are light mobile clients. We implemented NFC (Near Field Communication) and QR (Quick Response) code capabilities on full node payment gateways to improve usability.

We used a D-Link DSR-250N Wi-Fi router to represent the community base station and an IEEE 802.11n Wi-Fi network to interconnect the above nodes except the bank node which periodically joins the blockchain via the Wi-Fi router's public network interface. We used the auto-discovery protocol of geth to connect different nodes, and configured the bank node's backhaul bandwidth via the router's WAN port. A summary of devices and their capabilities are presented in Table I.

A. Bank Node

The bank application is developed on python 2.7.12 to update the account information. It is implemented on a Raspberry Pi 3, which also acts as an ethereum

TABLE I: Devices and their capabilities

	Miner	**Full node (incl. bank)**	**Light node**
Device	Dell Latitude 6430u	Raspberry Pi 3	Google Pixel XL
# of nodes	3	4	1
OS	Ubuntu 17.04	Raspbian Jessie	Android v8.1.0
Geth	v1.6.5	v1.6.5	v1.6.7

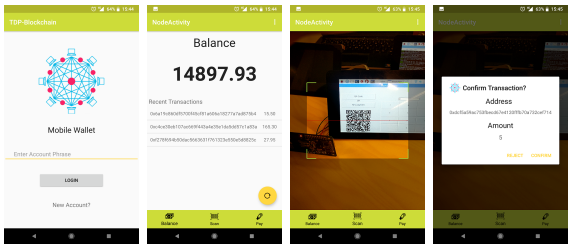

Fig. 3: Mobile Wallet Application

full node. The application is synced with the blockchain using the Python-JSON RPC library [3]. It keeps track of the connectivity and update the account balances in SQLite database.

B. NFC and QR code enabled Payment Gateway

Payment gateway is designed by connecting an Adafruit PN532 NFC module with a Raspberry Pi 3. A customized application is designed as the user interface on python 2.7.12.

C. Mobile Wallet App

We developed the mobile wallet app (Figure 3) in Android Studio 3.0. The wallet app is connected to the blockchain as a light node, which submits and retrieves the transactions directly to/from the blockchain. Both NFC and QR code based payment modes are embedded in the app. The app also shows the account balance and recent transaction history.

IV. Demonstration and Interaction

In our demonstration, we will visualize the process from the initiation of a transaction until it is received by the recipient. We will demonstrate the two scenarios and attendees will be able to interact with both. First, the update on the mobile wallet and vendor's payment gateway after performing a payment (via NFC or QR code). Second, the bank node synchronization after a disconnection period.

[3]https://github.com/ConsenSys/ethjsonrpc

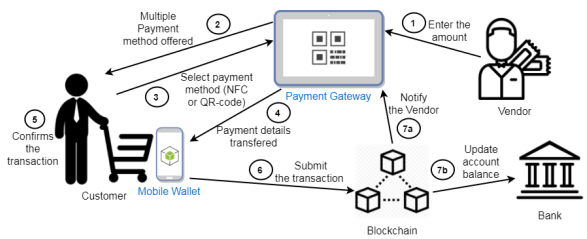

Fig. 4: Demonstration Flowchart

A. Payment at a shop

Initially, the vendor enters the requested payment amount in the payment gateway. Then, a mobile user can select the preferred payment method (i.e. NFC or QR code) based on the capabilities of his phone. Once confirmed, the transaction is submitted to blockchain and the amount will be deducted from the user balance. The payment gateway receives a confirmation of the submitted transaction from the blockchain. The vendor's balance is updated once the transaction is confirmed by miners. In this scenario, the attendee will be able to interact as a customer/user. They can either download the developed mobile wallet application on their mobile phone or use one of the authors mobile, with the pre-installed wallet application.

B. Bank Node Synchronization

First, we disconnect the bank node manually for a certain period of time (e.g. 60 seconds), during which user account balances at the bank node are frozen. Meanwhile, we or the attendees will perform several transactions within the village. Then, we reconnect the bank node to the network and show the synchronization of the bank node as well as the updates in the recorded user balances.

V. Technical Requirements

We will require 3 laptops as miners, 3 Raspberry Pis with displays (for bank node and two payment gateways), one Wi-Fi router with Ethernet cable as the base station and two mobile phones (to demonstrate the mobile wallet). Authors will bring the above equipment. In addition, we need a 24" monitor with VGA cables from the organizers to display the vendor wallets.

Acknowledgement

This work has been performed under the framework of 6Genesis Flagship (grant 318927), SECUREConnect and Towards Digital Paradise Projects.

References

[1] "KUHA Mobile Network," https://www.kuha.io, 2017, [Online; accessed 19-September-2017].

[2] D. Fitchett, "Bank for agriculture and agricultural cooperatives (baac), thailand (case study)," *Washington DC: Consultative Group to Assist the Poorest (CGAP) Working Group on Savings Mobilization*, 1999.

[3] T. J. MacDonald, D. W. Allen, and J. Potts, "Blockchains and the boundaries of self-organized economies: predictions for the future of banking," in *Banking Beyond Banks and Money*. Springer, 2016, pp. 279–296.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] A. S. Pentland, R. Fletcher, and A. Hasson, "Daknet: Rethinking connectivity in developing nations," *Computer*, vol. 37, no. 1, pp. 78–83, Jan. 2004. [Online]. Available: http://dx.doi.org/10.1109/MC.2004.1260729

[6] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, 2014.