BankChain - Product Vision

Chainable Technologies

H.G. van de Kuilen

rvandekuilen, 4226151

J.C. Kuijpers

jckuijpers, 4209915

E.J. Sennema

esennema, 4496582

M.R. Kok

mrkok, 4437659

I. Dijcks

idijcks, 4371151

May 2017

Contents

1 Abstract

The title and names of the author are given at the front page. This product vision explains the target customer and the need for this product. First o short introduction is given, which introduces the project, the purpose of the product and some technical terms.

The product has a customer that has a basic understanding of the technology he uses. The product delivers a web of trust of costumers. Their are other comparable products, but these product don't use the IBAN infrastructure, which adds a trustful way of adding a costumer to the web of trust. The crucial product attributes of the product are therefore the Blockchain, that holds the web of trust and the IBAN infrastructure. There are 8 weeks available to create this product.

2   Introduction

The Distributed Software (DS) group at the Delft University of Technology has been developing a peer-to-peer application for many years (Delft University of Technology, 2017). Part of their project is a blockchain for trust. As a research project and proof of concept for the DS division, our product creates trust between two peers.

This document describes the product we are creating, BankChain, and the vision we have on the product. The product vision gives a view of the customer and its needs. A view of the current market, together with a budget and time frame of the project.

In this document the terms Blockchain, encryption and IBAN are used. Before reading the product vision, explanation is needed. "Blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way." (Iansiti, 2017) For Blockchain and public private key pairs, encryption is needed. "Public-key cryptography requires each user to have two keys: a public key, used by the entire world for encrypting messages to be sent to that user, and a private key, which the user needs for decrypting messages."(Tanebaum & Wetherall, 2011). And at last our product uses IBAN. "The IBAN facilitates the communication and processing of cross-border transactions. It allows exchanging account identification details in a machine-readable form."(SWIFT, 2016)

3   Target customer

The customer are the stateholders and other with the need for public keys of others and distributing his own. These customer have troubles to distribute their public key. The product helps to solve this. The customer has a basic understanding of Public-key cryptography. The kind of customer the product has is involved in the information technology and has the need of using Public-key cryptography. The web of trust helps to solve the public key distribution and identifying persons on the Internet. The customer uses the product to make sure that communication is done with the right person.

4   Customer needs

The product will address mainly the need for digital security from the customer. The product will deliver a way to create a trust relation between customers. The customer has the need of being sure of a identities of someone else. When communicating the customer can, because of the trusted relation, be sure he is communicating with the right one. Distributing public keys it imported for achieving this. The product is a way for doing this. That is way the product addresses this problem of the customer.

5   Crucial product attributes

There are a few elements of our application that we cannot do without. In order for the Customer to successfully use the app it will have to be able to both validate IBAN accounts from other users and send proof of access for its own account. Which means that the user needs a GUI to input this data into the app (preferably in an intuitive and easy manner). Then the application has to be able to send bank transfers and read incoming one. This validated data then must be stored securely so the validator needs to have access to one which in our case would be a blockchain.

6   Existing Comparable Products

A comparable product would be signing a message containing your IBAN with your private key that has been verified in a web of trust.

Using private keys holding Bitcoin would also be a comparable product. This private key would of course not have any trust attached to it, but it would be a PoS (proof of stake). The Bitcoin ledged against the message are easily traceable by nature. Therefore this would make it possible to verify that the coins are unique and not used in thousands of other message signings recently, thus protecting against spammers or Sybil attacks.

Our product is unique however, in that it requires an IBAN account, which is very hard to obtain illegitimately. This does give the responsibility to protect against bots partially out of our hands and into the banking world, but since this sector has a lot of experience with this and strict laws to follow, we trust this sector to handle this problem with great care.

Using an additional proof of life is something that we have recently seen in the gaming community as well. The free online game "Dota 2" has implemented such a method (Orland, 2017). The players now need a verified phone number to enable in game trading with other players. This prevents Sybil attacks and automated attacks against the in game economy.

7   Time frame and budget

The application has to be presented on the 30th of June So there are 8 weeks to create the final product. In these weeks we should have our first version by may 12th. We should finish our Product by June 9th in order to integrate our features with those from other projects. Finally the codebase will have to be completely finished on June 23rd for review purposes which means that no changes can be made to that codebase after the 23rd.

There is no real budget to create this app we do however have resources. These contain developers at approximately 24 hours a week each to work on the application. There is space available for meetings and hardware has been made

available to test the application. Also there is some money available for small costs (e.g. transaction fees).

References

Delft University of Technology. (2017). *About tribler.* Retrieved May 4th, 2017, from `https://www.tribler.org/about.html`

Iansiti, K. R., Marco; Lakhani. (2017, January 17). *The truth about blockchain.* Harvard Business Review. Harvard University. Retrieved January 17th, 2017, from `https://hbr.org/2017/01/the-truth-about-blockchain`

Orland, K. (2017, April 21). *Valve asks for phone numbers to confirm dota 2 player identities.* Ars Technica. Retrieved May 4th, 2017, from `https://arstechnica.com/gaming/2017/04/valve-asks -for-phone-numbers-to-confirm-dota-2-player-identities/`

SWIFT. (2016, May). *Iban registry.* Retrieved May, 2016, from `https://www.swift.com/sites/default/files/resources/ swift_standards_ibanregistry.pdf`

Tanebaum, A. S., & Wetherall, D. J. (2011). *Computer networks.*