TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Information Technology
Department of Computer Engineering

ITC70LT

Christopher David Raastad

THESIS TITLE

Master thesis

Write thesis title

Alex Norta
PhD
Associated Professor

Tallinn 2017

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Arvutitehnika instituut

ITC70LT

Christopher David Raastad

LÕPUTÖÖ PEALKIRI

Magister

Kirjuta pealkirja eesti keeles

Alex Norta
PhD
Associated Professor

Tõlgi PhD eesti keelde

Tõlgi Associated Professor eesti keelde

Tallinn 2015

Todo list

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Christopher David Raastad

May 8th 2017

Abstract

Write English abstract ...

If the thesis is written in English, the abstract is $\frac{1}{2}$ A4 long and the abstract in Estonian (*Annotatsioon*) is of length 1 A4.

The last paragraph of abstract is obligatory and must be written accordingly:

Fill in English abstract thesis details ...

The thesis is in English and contains [pages] pages of text, [chapters] chapters, [figures] figures, [tables] tables.

Annotatsioon

Kirjuta annotatsiooni eesti keeles ...

Kui töö põhikeel on inglise keel, siis esitatakse annotatsioon (Abstract) inglise keeles mahuga $\frac{1}{2}$ A4 lehekülge ja annotatsioon eesti keeles mahuga vähemalt 1 A4 lehekülg.

Annotatsiooni viimane lõik on kohustuslik ja omab järgmist sõnastust:

Täitke eesti keele annotatsiooni lõputöö detailid ...

Lõputöö on kirjutatud [mis keeles] keeles ning sisaldab teksti [lehekülgede arv] leheküljel, [peatükkide arv] peatükki, [jooniste arv] joonist, [tabelite arv] tabelit.

Table of abbreviations and terms

TTÜ	*Tallinna Tehnikal Üllikool*, Tallinn University of Technology
ATI	TTÜ *Arvutitehnika instituut*, Department of Computer Science
DPI	Dots per inch

Continue adding to table of abbreviations and delete old ones...

Table of contents

List of figures

List of tables

1. Introduction

Write the Introduction (Chapter 1) ...

1.1. Setting the Stage

Payments today are the laggard of the information age. While emails can be sent instantly money is either slow and/or expensive to move digitally. Bank transfers can take days, only work during business hours, and have high fees across borders. Card payments are instant but enslave merchants with 3% fees and risk of chargebacks. Paypal brought payments to the internet, but still brings a layer of cost and inconvenience when withdrawing funds. Fintech companies like Venmo and Square can make the illusion of fast payments, but still take days to settle in the background. All of this inconvenience comes from legacy Financial system of banking that has little profitable motivation to innovate and adds an estimated 1% of GDP cost to the economy . citation needed

Bitcoin was the first mover in digital currency, introducing a clever mechanism of digital value transfer completely sidestepping the Financial system. Its distributed consensus protocol, clever economical incentives to maintaining the network, irreversible transactions, and pseudo anonymous users sent shockwaves of interest and skepticism in the financial and regulator community. By great surprise, in 8 years the world's first cryptocurrency increased massively in value and interest. Altcoins forked the Bitcoin blockchain technology to tackle other use cases and attempt to overcome shortcomings of original bitcoin. Exchanges sprung up to bring institutional trust into the ecosystem, making it easier to buy and sell bitcoins, bridging the gap between the traditional world of finance and digital currency. Eventually Bitcoin could be used to buy Domino's pizza and airline tickets.

But still payments are a niche use case in Bitcoin and other cryptocurrencies, the main use case being long term value storage investment and short term "get-rich-quick" speculation. Bitcoin is complicated to use and missing key factors of trust and user identity making it unfavorable for mainstream commerce. In addition converting the digital currency to and from the banking financial world comes at a cost. Providers of goods and services can accept Bitcoin at a 1% fee but directly converting it to Fiat currency. The real world is not priced in

BTC.

The solution is to bring fiat currency and the traditional financial system into the realm into digital currency. This manuscript explores Euro 2.0 digital currency system, with trust, regulation, and usability built in with Estonian ID and the Ethereum blockchain smart contract technology. The system removes the need of financial institution intermediaries to hold balances and execute payments. The usability for payments arises from ease of sending to personal ID codes, identification of users on the system, and use of fiat currency. We explore how to derive the need of this system for stakeholders, the technical requirements, and the security and privacy of its implementation. The system can be initially managed by a foundation and completely run later by central banks saving the economy a majority of it's 1% GDP lost to payment friction.

1.2. History of Currency and Payments

Citations needed ...

Money and payments haven been part of human society since the dawn of civilization. Currency grew out of the need to transport value of goods without transferring the goods themselves. First came gold, silver, and other precious metals to trade in exchange for goods and services. Later in the 1600s came notes issued by the central bank of England backed by silver and shortly after every country in the Western world. Over this time Banks grew into the institutions housing the value created by society. By the 1950s the USA was the first government to eliminate a backing by silver to create the first Fiat currency only backed by the trust of the US Government and Federal Reserve. Again shortly after every other country followed. Finally with the dawn of the information age came digital bank accounts and debit credit cards to to access our money.

Bank transfers can take days to settle and only work during working hours of weekdays. International bank transfers can take even longer and with a heavy 3-5% fee. Card payments transact instantly, but enslave merchants for 1-3% transaction fees and carry the risk of costly chargebacks at the benefit of consumer convenience. Many transactions in financial systems can happen "instantly" (i.e. stock trades) but in fact take days to settle on the backend due to legacy paper based processes. The financial industry and has only in this time created pretty

facades to their inefficient processes. Paypal did the best they could, succeeding to bring payments to the internet, but is still slowed down and brings the inconvenience of the legacy system and regulation. The economic cost of payments is an estimated 1% of GDP . citation needed

In a hopeless quagmire of legacy and greed, following the 2008 Financial meltdown, Satoshi Nakamoto introduced Bitcoin: A Peer-to-Peer Electronic Cash System . The clever decentralized, proof of work, consensus system of value transfer solving the business problem "how do I create a system where nobody can stop me spending my own money?". A by product of the the Bitcoin system is the Blockchain distributed ledger technology. This consensus mechanism inspired developers to create hundreds of different altcoins to overcome some shortcomings of the Bitcoin and tackle a variety of uses cases with similar technology. citation needed

Despite this promising rise of the value transfer protocol, payments for goods and services are still a very niche use case for Bitcoin and other cryptocurrencies. Bitcoin and altcoins have until now had more traction for long term investment and get-rich-quick speculation then becoming the next generation payment method. Websites and stores accepting Bitcoin do so more for marketing then actual economic incentive. Accepting Bitcoin with a payment provider is in fact just charging a 1% fee to receive payment directly to a fiat currency bank account with development costs of integrating a new payment method. cite Bitcoin HCI study citation needed

What's preventing cryptocurrencies from widespread adoption for payments? Ironically the defining features of Bitcoin, pseudo anonymity, irreversibility of transactions, and lack of central regulations, make for an unattractive payments system. Exchanges arose to be a more trustworthy source to buy and sell Bitcoins and create a regulated gateway to the traditional financial system. Transacting with individuals outside of exchanges poses great risk with off chain components of transactions. Users end up doing KYC on their counter-party or rely on other community verification to gain trust in completing transactions. citation needed cite Bitcoin HCI study

2. Bridge of Knowledge

Write the Bridge of Knowledge (Chapter 2) ...

3. Chapter 3

Write Chapter 3 ...

4. Chapter 4

Write Chapter 4 ...

5. Chapter 5

Write Chapter 5 ...

6. Evaluation

Write Evaluation (Chapter 6) ...

7. Summary

Write Summary (Chapter 7) ...

Move these references to Biblio.bib

References

[1] Arvutitehnika instituut. Lõpetajale. [WWW] http://ati.ttu.ee/index.php?page=470 (13.05.2013)

Kasutatud kirjanduse loetelu koostamise näidet vaata TTÜ Raamatukogu juhendmaterjalist „Viitekirjete koostamine“ aadressil: `http://www.ttu.ee/public/r/raamatukogu/juhendid/viitekirjetekoostamine.pdf`.

Appendix 1 - [Heading]

Add Appendix 1 or delete it