UMEÅ UNIVERSITY
Department of Computing Science
Master thesis report

Examensarbete för civilingenjörsexamen i teknisk datavetenskap
30HP, 5DV143, VT19

Cross-chain Settlement and Exchange in Cryptocurrency

Name	Carl-Johan Andersson
CAS	caan0156@umu.se
CS	c14can@cs.umu.se
Date	2019-02-07

University Supervisor
Jan-Erik Moström (jem@cs.umu.se)
Company Supervisor
Oskar Janssson (oskar.jansson@cinnober.com)

Contents

Abstract

wafawf

1 Introduction

Although blockchain and other types of distributed ledgers are still in their infancy a growing number of people and companies are starting to see that they hold great promise, especially when it comes to financial technology, where things like trust and security is held to be very important.

1.1 The origins of bitcoin

The most well known, developed and researched blockchain technology is know as Bitcoin. The mysterious nature of bitcoins creator makes hard to pinpoint how and when the idea was first thought up and when the development started, the most exact way and most well known would be to pinpoint at: `2009-01-03 18:15:05`, which is the timestamp on the very first block in the bitcoin blockchain, however the white paper (**Bitcoin: A Peer-to-Peer Electronic Cash System**) specifying the technical details circulated on cryptographic mailing lists as early as 31 October 2008, and the domain name `bitcoin.org` was registered 18 August 2008.

Satoshi Nakamoto

The author name given in the white paper is `Satoshi Nakamoto`, this name is believed to be a pseudonym. Satoshi remained in the bitcoin community for a couple of years. Regularly posting on the forum `bitcointalk.org` and keeping up with conversations in the mailing list. Those who have been interested in finding out Satoshi's real identity have analyzed his active time and language used. The findings were that Satoshi was most active during Western European day time, and he also used a lot of Anglo-colloquialisms such as "bloody hard", and "flat" instead of apartment, so a popular theory is that Satoshi lived in Britain at least during this time.

`April 23, 2011` was the last time anyone ever heard from Satoshi Nakamoto, in a mail to a fellow developer Mike Hearn he said "I've moved on to other things. It's in good hands with Gavin and everyone.". Speculations on who Satoshi really is still going strong even to this day, but Nakamoto's true identity is so far unknown.

1.2 Basics on Bitcoin

Most people, even the layman with no blockchain experience, have at least heard of bitcoin. But the exact details of how it works is not common knowledge. Described in a single sentence: bitcoin is a currency where a communal ledger that is shared between the whole world. The ledger holds the information on who owns what in terms of money or other assets. The regular monetary system we are used to has a centralized authority, for example a central bank, who decides how much money is in circulation, who can transact with who etc. The monetary system presented by bitcoin has no centralized authority, instead it relies on decentralized, trust-less verification.

These usually are the main concerns people have with distributed ledgers:

- How is spending someone else's money prevented?
- How is spending the same money in different places in the world prevented?
- How is the consensus on the order of transactions reached?
- How do I interact with it?
- What type of transactions can you make?

These questions will be given ansers in the sections below.

Digital signatures

Bitcoin would not be possible at all without the underlying cryptographic mathematics. When it comes to proving ownership in bitcoin ECDSA (Elliptic curve digital signature algorithm) is used. Elliptic curve cryptography will not be covered in depth here but the basic idea is that you have a private and public key. The public key can be shared with anyone without danger, the public key can be derived from the private key, but not the other way around, this is something called trap-door mathematics. This means that it is easy to go one way via equations. But going back is nearly impossible. The reason for it not being completely impossible is because any potential attacker could always just keep guessing private keys until the right one is found. However with a sufficiently large private key it should take several million years to find the correct private key even with unrealistically strong and fast computers.

The most common transaction made on the blockchain is one where you "pay to" a public key. Who ever holds the private key paired with that public key can then via a mathematical equation prove that they hold the private key without actually revealing the private key.

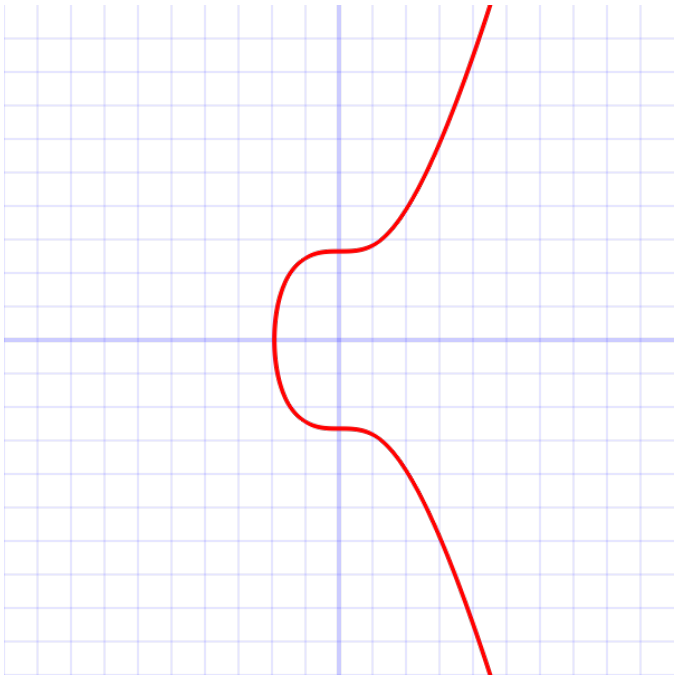

Figure 1: The `Secp256k1` plotted over real numbers. Note that the real curve is over a field, and thus looks more like a scattering of random points

The elliptic curve used can hold different parameters that defines it, certain elliptic curves are standardized and have their own names. The curve used in bitcoin is named `Secp256k1`.

Blocks and the blockchain

A block is fairly simple to understand, it is simply a datatype or structure that holds information about it self, all the transactions that can fit and the previous block in the chain (more on that in a bit). Because every block holds information about the previous block you can follow all blocks backwards in time all the way back to the original, alos called the genesis block. This is what is referred to as the blockchain.

A block could be added to the chain by anyone in the world. However it will only be accepted if it has sufficient proof of work, and this is the key to how consensus is reached in the network

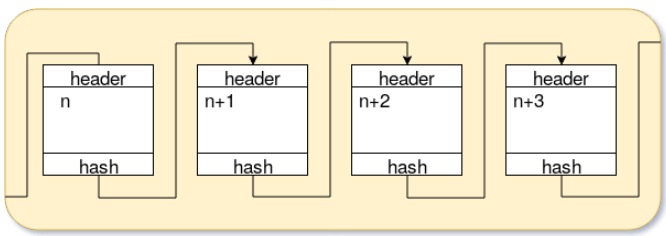

Figure 2: A basic overview of a blockchain

Proof of work

Proof of work is, just like the digital signatures, based in cryptographic mathematics. Before we go on you first need to understand what a hashing algorithm does, the hashing algorithm used in bitcoin is called `SHA256`. `SHA256` takes in data of any size and produces a sort of finger print of 256 bits.

For example the `SHA256` of the text "cool":

```
echo "cool" | openssl sha256
```

Produces:

```
27c16ce7e3861da034af1bb356d6a4f38cb84fa
65d51fa62f69727143b4c6b60
```

The text produced is actually bytes represented in a hexadecimal number system, in fact the entire string can be considered to be a very large number. Just like with the digital signature there is no known viable way that can take a hash and find what the original data that produced it was.

There is a term in bitcoin called mining difficulty, or just difficulty. This is a large number, 256 bits to be exact. When you want to add a new block to the chain you have to do something called mining, this is a process where you change certain variables in the block until the hash of the block header (Think of this a number) is less than the target difficulty. The term hashpower refers to how many times the machine you are using to mine blocks can test a certain combination of variables per second, or H/s.

The difficulty of mining a block is adjusted about every 2 weeks. The difficulty is so that the combined hashpower of the entire world is enough to mine one block every 10 minutes on average.

Software

Programmable transactions

1.3 Lightning network

1.4 Atomic swaps

1.5 The goal of the project

2 Background

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec arcu felis, efficitur nec lorem sed, dapibus elementum ipsum. Sed semper nunc at odio pellentesque congue. Mauris lectus magna, dapibus scelerisque lobortis nec, gravida et odio. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nunc diam lacus, tristique ut ultricies a, tempor sit amet urna. Nulla blandit massa nulla, at fringilla elit vestibulum quis. Praesent in rhoncus lacus. Vestibulum ante ipsum primis in fau-

cibus orci luctus et ultrices posuere cubilia Curae; Mauris vulputate diam sed dapibus maximus. Pellentesque rutrum nisi in facilisis efficitur. Proin at nunc facilisis, rhoncus justo ac, feugiat augue. Fusce vel molestie ligula, sed mattis magna. Nam ac nisl suscipit elit suscipit gravida. Duis tincidunt libero magna, sed placerat libero interdum eget. Cras molestie lacinia elementum.

Donec egestas ac orci vel tincidunt. Vestibulum metus ante, lobortis quis faucibus a, interdum id libero. Maecenas tincidunt turpis ac urna vehicula, in ornare enim sodales. Phasellus ultricies nec elit vel aliquam. Mauris commodo massa ut leo eleifend varius. Integer nec augue sollicitudin, finibus dui sit amet, accumsan nunc. Quisque sollicitudin vulputate justo eu vulputate.

Nam lacinia, risus ac consequat viverra, ligula ligula aliquet nisl, et efficitur odio dolor vel ipsum. Nulla placerat fermentum dui, vel bibendum tortor viverra sed. Praesent mollis turpis ac neque varius, id vulputate nisi bibendum. Integer nec purus ac ante sollicitudin vehicula ac vel nunc. Curabitur at efficitur urna, ut interdum justo. Donec id magna quis mi gravida venenatis. Integer nec nulla ligula. Praesent felis purus, semper eget ipsum et, tincidunt dapibus libero. Mauris varius cursus nunc, id pretium libero ultricies non. Donec elementum sapien eu porta accumsan. Pellentesque tristique massa purus, vitae congue ex ornare at. Quisque quis viverra nunc, condimentum pretium ex. Cras nec augue non eros faucibus consequat. Sed venenatis luctus libero, sit amet fermentum risus pharetra accumsan.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Praesent gravida diam mauris, eget egestas diam interdum in. Cras tempor, ante euismod vehicula commodo, nulla dui pharetra leo, ut malesuada arcu sem vitae ipsum. Nullam et est malesuada, condimentum mi ultrices, gravida massa. Fusce scelerisque vitae purus sed imperdiet. Nullam et ipsum rutrum, lobortis orci eget, blandit urna. Curabitur elementum finibus euismod. Integer efficitur interdum nulla, at varius lectus ultricies eget.

In laoreet tincidunt libero, tempus pharetra turpis rhoncus sed. Nunc convallis ligula non blandit auctor. Fusce maximus nulla odio, eu blandit sem lacinia in. Vivamus sed tristique metus. Curabitur et ultrices lacus. Integer dictum ante a mi ullamcorper vehicula. Fusce ut feugiat sapien. Maecenas sagittis commodo nibh in accumsan. Nulla at iaculis erat. Aenean nec elementum ligula. Duis finibus aliquam lacus, nec rhoncus ex dignissim ac. Nunc nisi velit, elementum vitae elit in, rutrum pulvinar justo. Maecenas bibendum accumsan orci ac feugiat. Morbi quis lectus eget justo bibendum sodales.

Interdum et malesuada fames ac ante ipsum primis in faucibus. Mauris eros lacus, gravida in nulla vitae, interdum finibus leo. Maecenas egestas libero volutpat enim malesuada porta. Aliquam consectetur, mauris nec venenatis dapibus, ipsum metus placerat urna, eget imperdiet dui leo sed orci. Maecenas quis ultricies nisi. Suspendisse tristique fermentum lorem vel consequat. Proin vel commodo neque. Donec risus metus, tempus ut sodales quis, finibus sed neque. Cras pretium porttitor ante nec bibendum. Phasellus ultricies, ex vel rhoncus tincidunt, tellus enim imperdiet enim, eget tincidunt massa risus nec erat. Curabitur venenatis mi sed metus tempus, et sollicitudin massa vehicula. Nam lectus ex, pretium malesuada elementum ac, convallis eu tortor. Integer ullamcorper elit at diam dignissim, nec iaculis felis eleifend. Nunc in ligula venenatis, dapibus erat eu, tristique magna. Phasellus pretium sapien vitae laoreet efficitur. Maecenas vehicula condimentum fringilla.

Mauris enim ligula, viverra feugiat neque ut, tempus vestibulum nisi. Phasellus et turpis mi. In hac habitasse platea dictumst. Nam fringilla mauris orci, eget facilisis ex gravida non. Maecenas id maximus lectus. Integer ac dictum ipsum. Praesent dictum eleifend dolor, et faucibus lectus sagittis sit amet. Curabitur sollicitudin nisi luctus convallis mattis. Curabitur sem mauris, ullamcorper non ex vel, pulvinar elementum dui. Cras quis condimentum leo. Integer rutrum magna eu dictum luctus. Praesent et eleifend elit. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Nullam ac lacus posuere, elementum nisi eu, vulputate dui.

Nulla at pretium quam. Donec cursus mauris in purus sagittis finibus. Nam tincidunt venenatis quam ac auctor. Nulla sodales mattis facilisis. Sed ac arcu porttitor, porttitor nulla a, maximus lorem. Sed in efficitur nisi, vel facilisis arcu. Integer facilisis sit amet tellus quis mattis. Integer a lacus urna. Ut sed aliquet purus. Morbi ornare felis eu metus imperdiet, vel bibendum magna mollis. Fusce lacinia quis justo dictum aliquam. Morbi sit amet turpis aliquet, maximus mi quis, consequat metus. Duis elementum neque non tortor ornare porttitor. Curabitur posuere vulputate odio, ut pulvinar justo volutpat at.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec arcu felis, efficitur nec lorem sed,

dapibus elementum ipsum. Sed semper nunc at odio pellentesque congue. Mauris lectus magna, dapibus scelerisque lobortis nec, gravida et odio. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nunc diam lacus, tristique ut ultricies a, tempor sit amet urna. Nulla blandit massa nulla, at fringilla elit vestibulum quis. Praesent in rhoncus lacus. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Mauris vulputate diam sed dapibus maximus. Pellentesque rutrum nisi in facilisis efficitur. Proin at nunc facilisis, rhoncus justo ac, feugiat augue. Fusce vel molestie ligula, sed mattis magna. Nam ac nisl suscipit elit suscipit gravida. Duis tincidunt libero magna, sed placerat libero interdum eget. Cras molestie lacinia elementum.

Donec egestas ac orci vel tincidunt. Vestibulum metus ante, lobortis quis faucibus a, interdum id libero. Maecenas tincidunt turpis ac urna vehicula, in ornare enim sodales. Phasellus ultricies nec elit vel aliquam. Mauris commodo massa ut leo eleifend varius. Integer nec augue sollicitudin, finibus dui sit amet, accumsan nunc. Quisque sollicitudin vulputate justo eu vulputate.

Nam lacinia, risus ac consequat viverra, ligula ligula aliquet nisl, et efficitur odio dolor vel ipsum. Nulla placerat fermentum dui, vel bibendum tortor viverra sed. Praesent mollis turpis ac neque varius, id vulputate nisi bibendum. Integer nec purus ac ante sollicitudin vehicula ac vel nunc. Curabitur at efficitur urna, ut interdum justo. Donec id magna quis mi gravida venenatis. Integer nec nulla ligula. Praesent felis purus, semper eget ipsum et, tincidunt dapibus libero. Mauris varius cursus nunc, id pretium libero ultricies non. Donec elementum sapien eu porta accumsan. Pellentesque tristique massa purus, vitae congue ex ornare at. Quisque quis viverra nunc, condimentum pretium ex. Cras nec augue non eros faucibus consequat. Sed venenatis luctus libero, sit amet fermentum risus pharetra accumsan.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Praesent gravida diam mauris, eget egestas diam interdum in. Cras tempor, ante euismod vehicula commodo, nulla dui pharetra leo, ut malesuada arcu sem vitae ipsum. Nullam et est malesuada, condimentum mi ultrices, gravida massa. Fusce scelerisque vitae purus sed imperdiet. Nullam et ipsum rutrum, lobortis orci eget, blandit urna. Curabitur elementum finibus euismod. Integer efficitur interdum nulla, at varius lectus ultricies eget.

In laoreet tincidunt libero, tempus pharetra turpis rhoncus sed. Nunc convallis ligula non blandit auctor. Fusce maximus nulla odio, eu blandit sem lacinia in. Vivamus sed tristique metus. Curabitur et ultrices lacus. Integer dictum ante a mi ullamcorper vehicula. Fusce ut feugiat sapien. Maecenas sagittis commodo nibh in accumsan. Nulla at iaculis erat. Aenean nec elementum ligula. Duis finibus aliquam lacus, nec rhoncus ex dignissim ac. Nunc nisi velit, elementum vitae elit in, rutrum pulvinar justo. Maecenas bibendum accumsan orci ac feugiat. Morbi quis lectus eget justo bibendum sodales.

Interdum et malesuada fames ac ante ipsum primis in faucibus. Mauris eros lacus, gravida in nulla vitae, interdum finibus leo. Maecenas egestas libero volutpat enim malesuada porta. Aliquam consectetur, mauris nec venenatis dapibus, ipsum metus placerat urna, eget imperdiet dui leo sed orci. Maecenas quis ultricies nisi. Suspendisse tristique fermentum lorem vel consequat. Proin vel commodo neque. Donec risus metus, tempus ut sodales quis, finibus sed neque. Cras pretium porttitor ante nec bibendum. Phasellus ultricies, ex vel rhoncus tincidunt, tellus enim imperdiet enim, eget tincidunt massa risus nec erat. Curabitur venenatis mi sed metus tempus, et sollicitudin massa vehicula. Nam lectus ex, pretium malesuada elementum ac, convallis eu tortor. Integer ullamcorper elit at diam dignissim, nec iaculis felis eleifend. Nunc in ligula venenatis, dapibus erat eu, tristique magna. Phasellus pretium sapien vitae laoreet efficitur. Maecenas vehicula condimentum fringilla.

Mauris enim ligula, viverra feugiat neque ut, tempus vestibulum nisi. Phasellus et turpis mi. In hac habitasse platea dictumst. Nam fringilla mauris orci, eget facilisis ex gravida non. Maecenas id maximus lectus. Integer ac dictum ipsum. Praesent dictum eleifend dolor, et faucibus lectus sagittis sit amet. Curabitur sollicitudin nisi luctus convallis mattis. Curabitur sem mauris, ullamcorper non ex vel, pulvinar elementum dui. Cras quis condimentum leo. Integer rutrum magna eu dictum luctus. Praesent et eleifend elit. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Nullam ac lacus posuere, elementum nisi eu, vulputate dui.

Nulla at pretium quam. Donec cursus mauris in purus sagittis finibus. Nam tincidunt venenatis quam ac auctor. Nulla sodales mattis facilisis. Sed ac arcu porttitor, porttitor nulla a, maximus lorem. Sed in efficitur nisi, vel facilisis arcu. Integer facilisis sit amet tellus quis mattis. Integer a lacus urna. Ut sed aliquet purus. Morbi ornare felis eu metus im-

perdiet, vel bibendum magna mollis. Fusce lacinia quis justo dictum aliquam. Morbi sit amet turpis aliquet, maximus mi quis, consequat metus. Duis elementum neque non tortor ornare porttitor. Curabitur posuere vulputate odio, ut pulvinar justo volutpat at.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec arcu felis, efficitur nec lorem sed, dapibus elementum ipsum. Sed semper nunc at odio pellentesque congue. Mauris lectus magna, dapibus scelerisque lobortis nec, gravida et odio. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nunc diam lacus, tristique ut ultricies a, tempor sit amet urna. Nulla blandit massa nulla, at fringilla elit vestibulum quis. Praesent in rhoncus lacus. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Mauris vulputate diam sed dapibus maximus. Pellentesque rutrum nisi in facilisis efficitur. Proin at nunc facilisis, rhoncus justo ac, feugiat augue. Fusce vel molestie ligula, sed mattis magna. Nam ac nisl suscipit elit suscipit gravida. Duis tincidunt libero magna, sed placerat libero interdum eget. Cras molestie lacinia elementum.

Donec egestas ac orci vel tincidunt. Vestibulum metus ante, lobortis quis faucibus a, interdum id libero. Maecenas tincidunt turpis ac urna vehicula, in ornare enim sodales. Phasellus ultricies nec elit vel aliquam. Mauris commodo massa ut leo eleifend varius. Integer nec augue sollicitudin, finibus dui sit amet, accumsan nunc. Quisque sollicitudin vulputate justo eu vulputate.

Nam lacinia, risus ac consequat viverra, ligula ligula aliquet nisl, et efficitur odio dolor vel ipsum. Nulla placerat fermentum dui, vel bibendum tortor viverra sed. Praesent mollis turpis ac neque varius, id vulputate nisi bibendum. Integer nec purus ac ante sollicitudin vehicula ac vel nunc. Curabitur at efficitur urna, ut interdum justo. Donec id magna quis mi gravida venenatis. Integer nec nulla ligula. Praesent felis purus, semper eget ipsum et, tincidunt dapibus libero. Mauris varius cursus nunc, id pretium libero ultricies non. Donec elementum sapien eu porta accumsan. Pellentesque tristique massa purus, vitae congue ex ornare at. Quisque quis viverra nunc, condimentum pretium ex. Cras nec augue non eros faucibus consequat. Sed venenatis luctus libero, sit amet fermentum risus pharetra accumsan.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Praesent gravida diam mauris, eget egestas diam interdum in. Cras tempor, ante euismod vehicula commodo, nulla dui pharetra leo, ut malesuada arcu sem vitae ipsum. Nullam et est malesuada, condimentum mi ultrices, gravida massa. Fusce scelerisque vitae purus sed imperdiet. Nullam et ipsum rutrum, lobortis orci eget, blandit urna. Curabitur elementum finibus euismod. Integer efficitur interdum nulla, at varius lectus ultricies eget.

In laoreet tincidunt libero, tempus pharetra turpis rhoncus sed. Nunc convallis ligula non blandit auctor. Fusce maximus nulla odio, eu blandit sem lacinia in. Vivamus sed tristique metus. Curabitur et ultrices lacus. Integer dictum ante a mi ullamcorper vehicula. Fusce ut feugiat sapien. Maecenas sagittis commodo nibh in accumsan. Nulla at iaculis erat. Aenean nec elementum ligula. Duis finibus aliquam lacus, nec rhoncus ex dignissim ac. Nunc nisi velit, elementum vitae elit in, rutrum pulvinar justo. Maecenas bibendum accumsan orci ac feugiat. Morbi quis lectus eget justo bibendum sodales.

Interdum et malesuada fames ac ante ipsum primis in faucibus. Mauris eros lacus, gravida in nulla vitae, interdum finibus leo. Maecenas egestas libero volutpat enim malesuada porta. Aliquam consectetur, mauris nec venenatis dapibus, ipsum metus placerat urna, eget imperdiet dui leo sed orci. Maecenas quis ultricies nisi. Suspendisse tristique fermentum lorem vel consequat. Proin vel commodo neque. Donec risus metus, tempus ut sodales quis, finibus sed neque. Cras pretium porttitor ante nec bibendum. Phasellus ultricies, ex vel rhoncus tincidunt, tellus enim imperdiet enim, eget tincidunt massa risus nec erat. Curabitur venenatis mi sed metus tempus, et sollicitudin massa vehicula. Nam lectus ex, pretium malesuada elementum ac, convallis eu tortor. Integer ullamcorper elit at diam dignissim, nec iaculis felis eleifend. Nunc in ligula venenatis, dapibus erat eu, tristique magna. Phasellus pretium sapien vitae laoreet efficitur. Maecenas vehicula condimentum fringilla.

Mauris enim ligula, viverra feugiat neque ut, tempus vestibulum nisi. Phasellus et turpis mi. In hac habitasse platea dictumst. Nam fringilla mauris orci, eget facilisis ex gravida non. Maecenas id maximus lectus. Integer ac dictum ipsum. Praesent dictum eleifend dolor, et faucibus lectus sagittis sit amet. Curabitur sollicitudin nisi luctus convallis mattis. Curabitur sem mauris, ullamcorper non ex vel, pulvinar elementum dui. Cras quis condimentum leo. Integer rutrum magna eu dictum luctus. Praesent et eleifend elit. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Nullam ac lacus posuere, elementum

nisi eu, vulputate dui.

Nulla at pretium quam. Donec cursus mauris in purus sagittis finibus. Nam tincidunt venenatis quam ac auctor. Nulla sodales mattis facilisis. Sed ac arcu porttitor, porttitor nulla a, maximus lorem. Sed in efficitur nisi, vel facilisis arcu. Integer facilisis sit amet tellus quis mattis. Integer a lacus urna. Ut sed aliquet purus. Morbi ornare felis eu metus imperdiet, vel bibendum magna mollis. Fusce lacinia quis justo dictum aliquam. Morbi sit amet turpis aliquet, maximus mi quis, consequat metus. Duis elementum neque non tortor ornare porttitor. Curabitur posuere vulputate odio, ut pulvinar justo volutpat at.

3 Implementation

4 Comparison

5 Conclusion & Discussion

6 Future research