CS 09 805 (P) : Seminar

Bitcoin: A Cryptocurrency

Savitha K J
Reg. No. VEAKECS049
S8 CSE (2010 Admissions)

Department of Computer Science and Engineering
Vidya Academy of Science & Technology
Thalakkottukara, Thrissur - 680 501
(http://www.vidyaacdemy.ac.in)

CS 09 805 (P) : Seminar

Bitcoin: A Cryptocurrency

Savitha K J
Reg. No. VEAKECS049
S8 CSE (2010 Admissions)

Department of Computer Science and Engineering
Vidya Academy of Science & Technology
Thalakkottukara, Thrissur - 680 501
(http://www.vidyaacademy.ac.in)

Department of Computer Science and Technology

Vidya Academy of Science & Technology
Thalakkottukara, Thrissur - 680 501
(http://www.vidyaacademy.ac.in)

CERTIFICATE

This is to certify that the report titled **Bitcoin: A Cryptocurrency** is a bona-fide record of the Seminar presented by **Savitha K J (Reg. No. VEAKECS049)** of the Eighth Semester B.Tech CSE (2010 admissions) of Vidya Academy of Science & Technology, Thrissur - 680 501 in partial fulfilment of the requirement for the award of the Bachelor of Technology in Computer Science and Engineering from the University of Calicut.

Seminar Guide		**Head of Department**	
Name:	Ms. Geethu P C	Name:	Col MP Induchudan,
M.E., FITE, FIE, MCSI			
Signature:	....	Signature:	....
Date:	March 25, 2014	Date:	March 25, 2014

(Seal of Department of Computer Science and Engineering)

Acknowledgement

I wish to record my indebtedness and thankfulness to all who helped me prepare this Seminar Report titled Bitcoin: A Cryptocurrency and present it in a satisfactory way.

My sincere thanks to Dr.Sudha Balagopalan, our Principal, for providing us all the necessary facilities. I am also thankful to Col MP Induchudan, M.E., FITE, FIE, MCSI, the Head of Department of Computer Science and Engineering for encouragement and for giving valuable support. I am especially thankful to my seminar guide Ms. Geethu P C for giving me valuable suggestions and critical inputs in the preparation of this paper.

My classmates have always been helpful and I am grateful to them for patiently listening to my presentation of the seminar and interacting with me through their valuable questions.

Abstract

Bitcoin is the world's first decentralized digital currency, allowing the easy storage and transfer of cryptographic tokens, using a peer-to-peer network to carry information, hashing as a synchronization signal to prevent double-spending, and a powerful scripting system to determine ownership of the tokens. There is a growing technology and business infrastructure supporting it.

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

To send money, you broadcast to the network that the amount on your account should go down, and the amount on a receivers account up. Nodes, or computers, in the Bitcoin network apply that transaction to their copy of the ledger, and then pass on the transaction to other nodes. This, with some math-based security, is really all there is–a system that lets a group of computers maintain a ledger.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Until Bitcoins invention in 2008 by the unidentified programmer known as Satoshi Nakamoto, online transactions always required a trusted third-party intermediary. For example, if Alice wanted to send $100 to Bob over the Internet, she would have had to rely on a third-party service like PayPal or MasterCard. Intermediaries like PayPal keep a ledger of account holders balances. When Alice sends Bob $100, PayPal deducts the amount from her account and adds it to Bobs account. Without such intermediaries, digital money could be spent twice. Imagine there are no intermediaries with ledgers, and digital cash is simply a computer file, just as digital documents are computer files. Alice could send $100 to Bob by attaching a money file to a message. But just as with email, sending an attachment does not remove it from ones computer. Alice would retain a copy of the money file after she had sent it. She could then easily send the same $100 to Charlie. In computer science, this is known as the double-spending problem and until Bitcoin it could only be solved by employing a ledger-keeping trusted third party. Bit coins invention is revolutionary because for the first time the double-spending problem can be solved without the need for a third party. Bitcoin does this by distributing the necessary ledger among all the users of the system via a peer-to-peer network. Every transaction that occurs in the Bitcoin economy is registered in a public, distributed ledger, which is called the block chain. New transactions are checked against the block chain to ensure that the same bit coins havent been previously spent, thus eliminating the double-spending problem. The global peer-to-peer network, composed of thousands of users, takes the place of an intermediary; Alice and Bob can transact without PayPal. One thing to note right away is that transactions on the Bitcoin network are not denominated in dollars or Euros or yens they are on PayPal, but are instead denominated in Bitcoin. This makes it a virtual currency in addition to a decentralized payments network. The value of the currency is not derived from gold or government fiat, but from the value that people assign to it. The dollar value of a Bitcoin is determined on an open market, just as is the exchange rate between different world currencies.

Chapter 2

Related Works

Electronic funds transfer (EFT) is the electronic exchange, transfer of money from one account to another, either within a single financial institution or across multiple institutions, through computer-based systems. It consists of different concepts;

2.1 Fghi Jklm

2.1.1 yo mayo

Sed ut perspiciatis, unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam eaque ipsa, quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt, explicabo. Nemo enim ipsam voluptatem, quia voluptas sit, aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos, qui ratione voluptatem sequi nesciunt, neque porro quisquam est, qui dolorem ipsum, quia dolor sit amet, consectetur, adipisci[ng] velit, sed quia non numquam [do] eius modi tempora inci[di]dunt, ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit, qui in ea voluptate velit esse, quam nihil molestiae consequatur, vel illum, qui dolorem eum fugiat, quo voluptas nulla pariatur?

2.2 Opqrs Tuvw

At vero eos et accusamus et iusto odio dignissimos ducimus, qui blanditiis praesentium voluptatum deleniti atque corrupti, quos dolores et quas molestias excepturi sint, obcaecati cupiditate non provident, similique sunt in culpa, qui officia deserunt mollitia animi, id est laborum et dolorum fuga. Et harum quidem rerum facilis est et expedita distinctio. Nam libero tempore, cum soluta nobis est eligendi optio, cumque nihil impedit, quo minus id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et oluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum hic tenetur a sapiente delectus, ut aut reiciendis voluptatibus maiores alias consequatur aut perferendis doloribus asperiores repellat...

Bibliography

[1] *First Lessons in LaTeX*, by Dr. V N Krishnachandran, Vidya Academy of Science & Technology, Thrissur - 680 501, 2011.

Department of Computer Science and Engineering
Vidya Academy of Science & Technology
Thalakkottukara, Thrissur - 680 501
(http://www.vidyaacademy.ac.in)