INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1675 - 1680
RECEIVED : 29.02.2017 PUBLISHED : 15.03.2017
March 15, 2017

HANDLING AND VISUALIZING DATA BY BITCOIN CRYPTOGRAPHY IN PEER TO PEER NETWORK USING BITTORRENT TECHNOLOGY

[1]D.Ramya, [2]B.Salai Nalvetham ,[3]Mr.S.Kumarasamy,
[1,2]UG Scholar, Dept of IT, SKP Engineering College,
[3]Asst prof, Dept of IT, SKP Engineering College.

ABSTRACT:

The philosophy of decentralization to adopt to the situation of hosting domains including websites and web apps. In this the data has been run in a decentralized server which is connected to several peers in bittorent network. This paper involves in creating a website to display the open government data in various field from the website data.gov.in. The data can be visualized in different format for understanding purpose. The motivation of BitTorrent network is a distribute files in peer-to-peer system that has the potential for file distribution. Bitcoin cryptography is used for security and authentication purpose and make the transaction to be highly confidential.The additional advantage of the scenario is about using bitcoin is utilizing both proof-of-stake and proof-of-work systems. The aim of P2P network in Peercoin's transactions is balances through SHA-256,the proof-of-work scheme. This paper evaluates that the open government data can be reached to all the people who even not understand the programming language. It also provide high security on data transaction and to share the content dynamically among peers so that the centralized network architecture completely removed.

Keywords: Decentralized architecture,visualization ,web hosting, bitcoin cryptography.

1. SCOPE OF THE PROJECT:

The Scope of the project is implementation of a decentralized network that makes of the existing data handling mechanism to portray sensitive data to be hosted along the network. Main aim of this work is to portray decentralized architecture enabled with data handling. The confidential data can be handled in a architecture that is formed by connecting several peers in a network. The additional advantage of the scenario is about bitcoin cryptography which serves as the alternate method for buying domains under web hosting.

2. INTRODUCTION:

In this paper, we deals with webhosting on decentralized architecture. Building a decentralized architecture with high security using bitcoin cryptography. Handling data in single node becomes difficult. We have to buy a domain for data sharing in centralized architecture. Hence in this a single administrator can contribute in a network. In proposed system, we use decentralized architecture for web hosting. No single point of failure can occur in this network. Every user connected in this network can contribute. Highly confidential data can be shared through this network,hence it use secure network called bittorent network.

3. EXISTING SYSTEM:

Open Government Data (OGD) is a platform for supporting Open Data initiative of Government of India. The portal is intended to be used to publish datasets, documents, services, tools and applications collected by them for public use. It intends to increase transparency in the functioning of Government.It involves centralized accessing of data from government and needs a admin to maintain

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1675 - 1680
RECEIVED : 29.02.2017 PUBLISHED : 15.03.2017
March 15, 2017

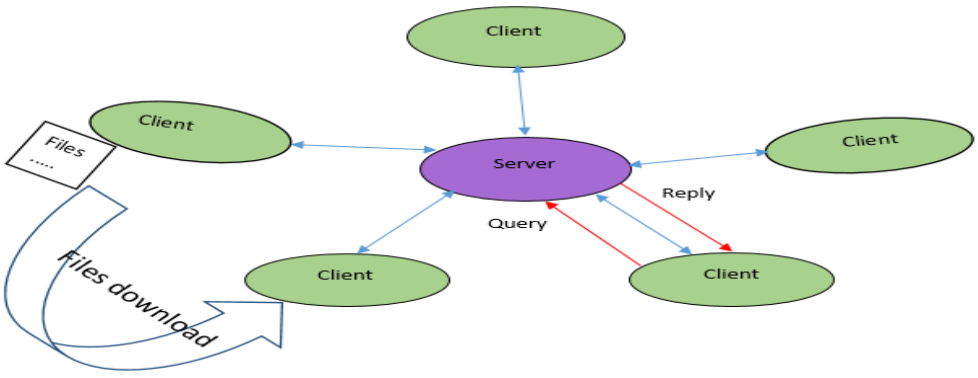
the centralized server.OGD Platform is not responsible for the contents, usability, accessibility, reliability including cyber security related issues.The centralized architecture tries to eave the weakness of a single point of failure.This causes loss of data and also causes traffic during data transmissionThe system under centralized architecture can be quite complex to maintain the architecture and also leads to high cost for buying.The data in this website can be represented only in the format such as XML,JSON,JSONP,XLS,ODS.

4. PROPOSED SYSTEM:

Bitcoin is a peer-to-peer decentralized digital currency. It differs from government backed currencies in that there is no central issuer and there is no middleman involved for various transactions. The supply of Bitcoin is by software.The original behind bitcoin was the create a type of electronic currency that was anonymous, secure and independent.For generating bitcoin hash cash cost function is used. It is quite difficult for generating bitcoin so this method is used. It is highly secured and efficient verifiable cost-function or also called as proof-of work function. RSS (Rich Site Summary; originally RDF Site Summary it is often called Really Simple Syndication) uses a group of standard web feed formats to publish frequently updated information: blog entries, news headlines, audio, video.RSS feeds enable the publishers to syndicate data automatically.A standard XML file format controls compatibility with many different machines. We have created a website that is web page which is running under decentralized server where bitcoin cryptography and bittorrent network is used. Whenever the updating is made in that RSS page here in our webpage it is updated.

5. ARCHITECTURE:

DECENTRALIZED ARCHITECTURE:



A decentralized server is the allocation of resources effectively , both hardware and software to each individual user working in the workstation. A decentralized computer has more benefits over a centralized network. Decentralized servers still enable file sharing and all computers can share the data such as via printers, scanners etc. The systems are capable of running independently of each other. By using Bitcoin cryptography higher level of security is provided for transaction purpose via decentralized server. Every one in the workstation can upload and download the files. The resources available in that network can be shared by everyone in that network.

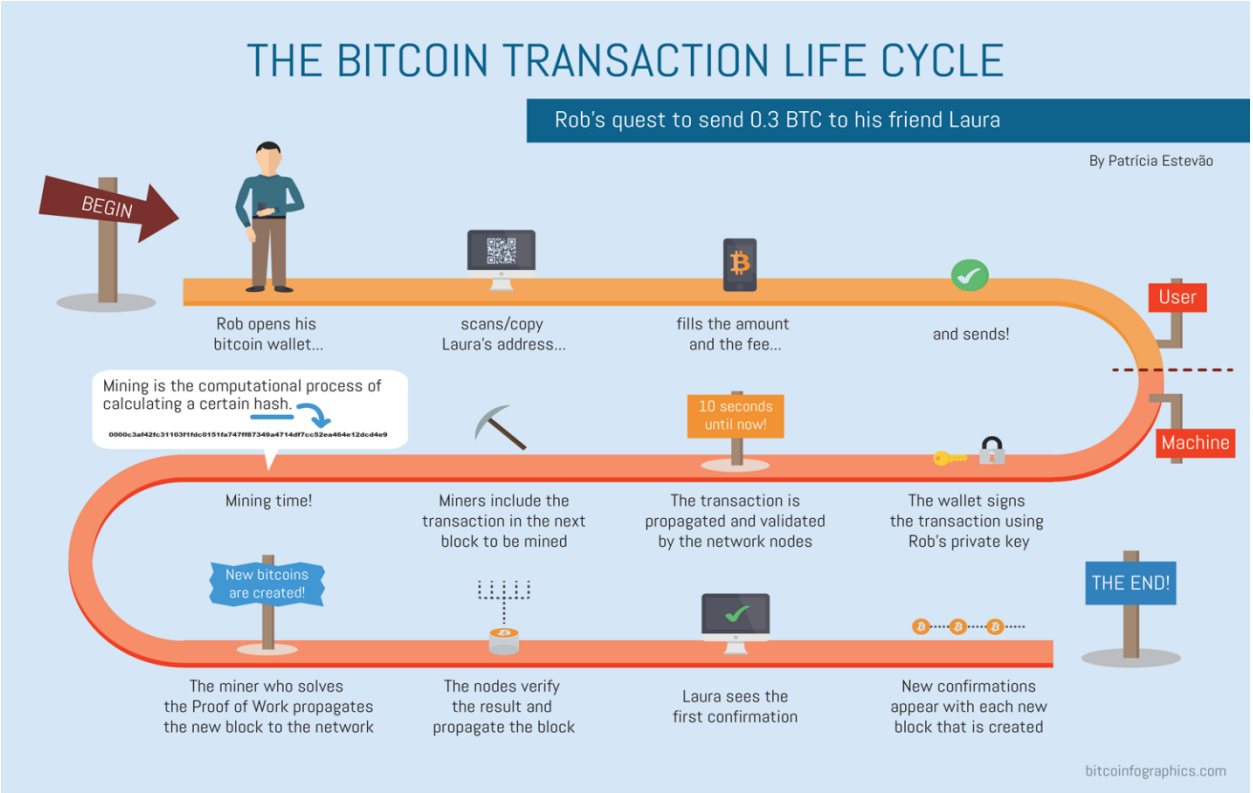
INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1675 - 1680
RECEIVED : 29.02.2017 PUBLISHED : 15.03.2017
March 15, 2017

BITCOIN CRYPTOGAPHY:

Bitcoin is a decentralized digital currency, introduced in 2008, that has recently gained noticeable popularity. It has features such as it lacks a central authority that controls the transactions, the list of transactions is publicly available and its syntax allows more advanced transactions than simply transferring the money. Bitcoin is the payment gateway (Here payment gateway is (e-commerce service provider)) with digital wallet. It is open source software this source can be reviewed by anyone since it is open source. Bitcoin is a decentralized electronic cash system. Bitcoin foundation standardizes, protects and promotes the Bitcoin cryptographic currency worldwide.

Workflow of Bitcoin:

Bitcoin is a peer-to-peer decentralized digital currency. It differs from government-backed currencies in that there is no central issuer and there is no middleman involved for various transactions.



The supply of Bitcoin is by software. The original behind bitcoin was the create a type of electronic currency that was anonymous, secure and independent from other central authorities. Coins are generated using process called mining. Here mining is assumed to be a lottery. Computers are connected with network and they are termed to be miners. They solve the problems and build new blocks. When some bitcoins are send to someone there a message is created and it attach a new owner's public key to this amount of coins and sign in with your private key. The transaction will be send to bitcoin network for broadcasting, this lets everyone to know that new owner of these coins is the owner of new key. Messages verify the signature for everyone so that it is said that message is authentic. The full transactions is kept by everyone, so any one can verify who is the current owner of

any coins which is belong to particular groups. The transactions are kept in the block chain, where a sequence of records is followed known as blocks. All computers in the network have a copy of block chain if anyone is updating in that blocks then the message is passed to all blocks. Each block contains a group of transactions of bitcoins that have been sent till the previous blocks. Record insertion is highly costly because each block must meet certain requirements that make to generate the each block is valid is difficult. This way, no party can overwrite previous records by just branching the chain.

HASH FUNCTION:

Hash cash is a fully distributed and infinitely scalable. Hash cash use symmetric key cryptography namely SHA1 or SHA 256 is used. A cryptographic hash function essentially takes input data which can be of any size, and transforms it, in an effectively manner to reverse or to predict way, into a relatively close packed string (in SHA-256 the hash is of 32 bytes) from other central authorities.

It is quite difficult for generating bitcoin so this method is used. It is highly secured and efficient verifiable cost-function or also called as proof-of work function. It is non-interactive and has no secret keys that can be managed by central server. Hash cash is a fully distributed and infinitely scalable. Hashcash use symmetric key cryptography namely SHA1 or SHA 256 is used.

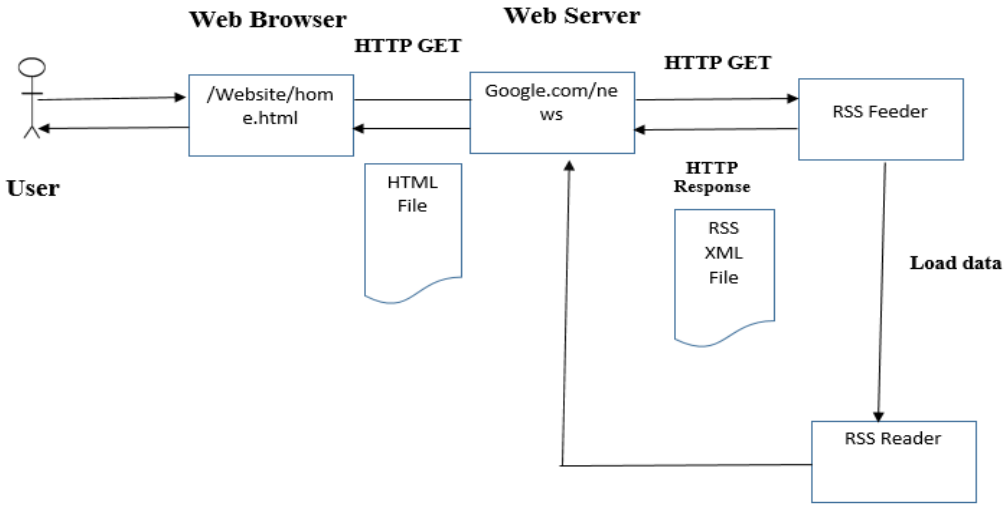
The hash cash difficulty factor is achieved by requiring that the hash output has a number of leading zeros. The hash cash cost-function iterates by perturbing data in the block by a nonce value, until the data in the block hashes to produce a serial number below the threshold which takes a lot of processing power. This low hash value for the each block serves as an easily-verifiable proof of work-every node on the network can instantly verify that the block meets the required criteria.

CREATING WEBPAGE AND VISUALIZE DATA IN DECENTRALISED SERVER:

RSS (Rich Site Summary; originally RDF Site Summary it is often called Really Simple Syndication) uses a group of standard web feed formats to publish frequently updated information: blog entries, news headlines, audio, video. An RSS document are known as "feed" or "web feed" or "channel" which includes full or summarized text, metadata such as publishing date and author's name. RSS feeds enable the publishers to syndicate data automatically. A standard XML file format controls compatibility with many different machines. RSS feeds also benefit users who want to receive timely updates from favourite websites or data from many sites. When we subscribe to a website, RSS removes the need for user to manually check the website for any new content. Instead, their browser constantly monitors the site and informs the user of any updates. The browser can also be allowed to automatically download the new data for the user. Software termed as "RSS reader", "aggregator", or "feed reader", which can be web, desktop, or mobiledevice-based, presents RSS feed data to the users. Users now subscribe to feeds either by entering a feed's URI into the reader or by clicking on the browser's feed icon. The RSS reader checks the user's feeds regularly for new information and can automatically download it, if that function is enabled. The reader also provides a user interface. We have created a website that is web page which is running under decentralized server where bitcoin cryptography and bittorrent network is used.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1675 - 1680
RECEIVED : 29.02.2017 PUBLISHED : 15.03.2017
March 15, 2017

6. WORK FLOW DIAGRAM:



CONCLUSION:

The website is working under the decentralized architecture.so that all the users in the network can act as uploaders and downloaders who are linked with the network nodes. confidential data can be transmitted over the secure network by using bitcoin cryptography. The BitTorrent protocol can be used to reduce the server traffic and network impact of distributing large files. Multi node data handling is maintained P2P is adopted for data sharing among peers, for reducing traffic among peers while data transaction, bittorent network is used. In this the data can be visualized in various formats. Pictorial representation of datasets makes the people to understand easily and quickly. In this paper, The concept of data visualization in decentralized sever with high security can be achieved.

REFERENCES:

[1]VitalikButerin. Satoshidice sold for $12.4 million, Jul 2013. Bitcoin Magazine.

[2] Christian Cachin and Jan Camenisch. Optimistic fair secure computation. In MihirBellare, editor, Advances in Cryptology – CRYPTO 2000, volume 1880 of Lecture Notes in Computer Science, pages 93– 111. Springer, August 2000. Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Compact e-cash. In Ronald Cramer, editor, Advances in Cryptology – EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science, pages 302–321. Springer, May 2005.

[3]K. Kant, R. Iyer and V. Tewari. A framework for classifying peer-to-peer technologies. Cluster Computing and Grid 2nd IEEE.2002.
http://doi.ieeecomputersociety.org/10.1109/CCGRID.2002.1017163

[4] Andrew Kantor. Despite reports, Grokster decision is a win for file sharing. http://www.usatoday.com/tech/columnist/andrewkantor/2005-07-01-groksterdecision_x.htm

[5] David Karger, Eric Lehman, Tom Leighton, Matthew Levine, Daniel Lewin and RinaPanigrahy. Consistent Hashing and Random Trees: Distributed Caching Protocols for Relieving Hot Spots on the World Wide Web. http://portal.acm.org/citation.cfm?doid=258533.258660

[6]LegalTorrents.com. http://www.legaltorrents.com/

[7]PetarMaymounkov and David Mazi‘eres. Kademlia: A Peer-to-peer InformationSystem Based on the XOR Metric. http://www.cs.rice.edu/Conferences/IPTPS02/109.pdf

[8]Chris Meredith. The story tit-for-tat. 1998. http://www.abc.net.au/science/slab/tittat/story.htm

[9] Iqbal Mohomed. Understanding BitTorrent.
http://www.cs.toronto.edu/~walex/mpvc/UnderstandingBitTorrent.ppt

[10]NextGenTel. http://www.nextgentel.no

[11] Opera. Press release: Faster, more efficient downloads in Opera technical preview with BitTorrent. http://www.opera.com/pressreleases/en/2005/07/07/

[12]Opera. Torrents. http://www.opera.com/download/torrents/

[13]Gilles Brassard, David Chaum, and Claude Crepeau. Minimum disclosure proofs of knowledge. Journal of Computer and System Sciences, 37(2):156 – 189, 1988.

[14]VitalikButerin. The bitcoin gambling diaspora, Aug 2013. Bitcoin Magazine.

VitalikButerin. Satoshidice sold for $12.4 million, Jul 2013. Bitcoin Magazine.

[15]Christian Cachin and Jan Camenisch. Optimistic fair secure computation. In MihirBellare, editor, Advances in Cryptology – CRYPTO 2000, volume 1880 of Lecture Notes in Computer Science, pages 93–111. Springer, August 2000.

[16] Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Compact e-cash. In Ronald Cramer, editor, Advances in Cryptology – EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science, pages 302–321. Springer, May 2005.

[17]David Chaum. Blind signature system. In David Chaum, editor, Advances in Cryptology – CRYPTO’83, page 153. Plenum Press, New York, USA, 1983.

[18] Richard Cleve. Limits on the security of coin flips when half the processors are faulty. In Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing, STOC ’86, pages 364–369, New York, NY, USA, 1986. ACM.

[19] Amos Beimel, Yehuda Lindell, EranOmri, and IlanOrlov. 1/p-Secure multiparty computation without honest majority and the best of both worlds. In Phillip Rogaway, editor, Advances in Cryptology – CRYPTO 2011, volume 6841 of Lecture Notes in Computer Science, pages 277–296. Springer, August 2011.

[20] Assaf Ben-David, Noam Nisan, and Benny Pinkas. FairplayMP: a system for secure multi-party computation. In PengNing, Paul F. Syverson, and SomeshJha, editors, ACM CCS 08: 15th Conference on Computer and Communications Security, pages 257–266. ACM Press, October 2008.
[7] IddoBentov and RanjitKumaresan. http://eprint.iacr.org/.