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:	Name:
Ms. Geethu P C M.Tech, MISTE	Col MP Induchudan, M.E., FITE
Signature:	Signature: .....
Date: March 26, 2014	Date: March 26, 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, 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 M.Tech, MISTE 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;

- Cardholder-initiated transactions, using a payment card such as a credit or debit card
- Direct deposit payment initiated by the payer
- Direct debit payments, sometimes called electronic checks, for which a business debits the consumer's bank accounts for payment for goods or services
- Electronic bill payment in online banking, which may be delivered by EFT or paper check
- Transactions involving stored value of electronic money, possibly in a private currency
- Electronic Benefit Transfer

EFTs include direct-debit transactions, wire transfers, direct deposits, ATM withdrawals and online bill pay services. Transactions are processed through the Automated Clearing House (ACH) network, the secure transfer system of the Federal Reserve that connects all U.S. banks, credit unions and other financial institutions.

For example, when you use your debit card to make a purchase at a store or online, the transaction is processed using an EFT system. The transaction is very similar to an ATM withdrawal, with near- instantaneous payment to the merchant and deduction from your checking account.

Direct deposit is another form of an electronic funds transfer. In this case, funds from your employers bank account are transferred electronically to your bank account, with no need for paper-based payment systems.

The increased use of EFTs for online bill payments, purchases and pay processes is leading to a paper- free banking system, where a large number of invoices and payments take place over digital networks. EFT systems play a large role in this future, with fast, secure transactions guaranteeing a seamless transfer of funds within institutions or across banking networks.

EFT transactions, also known as an online transaction or PIN-debit transaction, also offer an alternative to signature debit transactions, which take place through one of the major credit card processing systems, such as Visa, MasterCard or Discover, and can cost as much as 3% of the total purchase price. EFT processing, on the other hand, only charges an average of 1% for debit card transactions.

Chapter 3

Existing System

The first crypto currency to begin trading was Bitcoin in 2009. Since then, numerous crypto currencies have been created. Fundamentally, crypto currencies are specifications regarding the use of currency which seek to incorporate principles of cryptography to implement a distributed, decentralized and secure information economy. When comparing crypto currencies to fiat money, the most notable difference is in how no group or individual may accelerate, stunt or in any other way significantly abuse the production of money. Instead, only a certain amount of crypto currency is produced by the entire crypto currency system collectively, at a rate which is bounded by a value both prior defined and publicly known.

In centralized economic systems such as the Federal Reserve System governments regulate the value of currency by simply printing units of fiat money or demanding additions to digital banking ledgers, however governments cannot produce units of crypto currency and as such governments cannot provide backing for firms, banks or corporate entities which hold asset value measured in a decentralized crypto currency. The underlying technical system upon which all crypto currencies are now based was created by the anonymous group or individual known as Satoshi Nakamoto for the purpose of creating an economy within which the practice of fractional reserve banking would be fundamentally impossible.

Hundreds of crypto currency specifications now exist, most are similar to and derived from the first fully implemented crypto currency protocol, Bitcoin. Within crypto currency systems, the safety, integrity, and balance of all ledgers is ensured by a swarm of mutually distrustful parties, referred to as miners, who are, for the most part, general members of the public, actively protecting the network by maintaining a high hash-rate difficulty for their chance at receiving a randomly distributed small fee. Subverting the underlying security of a crypto currency is mathematically possible, but the cost may be unfeasibly high.

Most crypto currencies are designed to gradually introduce new units of currency, placing an ultimate cap on the total amount of currency that will ever be in circulation. This is done both to mimic the scarcity (and value) of precious metals and to avoid hyperinflation. As a result, such crypto currencies tend to experience hyper deflation as they grow in popularity and the amount of the currency in circulation approaches this finite cap. Compared with ordinary currencies held by financial institutions or kept as cash on hand, crypto currencies are less susceptible to seizure by law enforcement. Existing crypto currencies are all pseudonymous, though additions such as Zerocoin and its distributed laundry feature have been suggested, which would allow for anonymity.

Chapter 4

Proposed System

Bitcoin is a form of digital currency, created and held electronically. No one controls it. Bitcoin arent printed, like dollars or euros theyre produced by lots of people running computers all around the world, using software that solves mathematical problems. Its the first example of a growing category of money known as cryptocurrency.

Bitcoin can be used to buy things electronically. In that sense, its like conventional dollars, euros, or yen, which are also traded digitally.

However, bit coins most important characteristic, and the thing that makes it different to conventional money, is that it is decentralized. No single institution controls the Bitcoin network. This puts some people at ease, because it means that a large bank cant control their money.

This currency isnt physically printed in the shadows by a central bank, unaccountable to the population, and making its own rules. Those banks can simply produce more money to cover the national debt, thus devaluing their currency.

Instead, Bitcoin is created digitally, by a community of people that anyone can join. Bitcoin are mined, using computing power in a distributed network. This network also processes transactions made with the virtual currency, effectively making Bitcoin its own payment network.

Bitcoin has several important features that set it apart from normal fiat currencies.

1. Its decentralized

   The Bitcoin network isnt controlled by one central authority. Every machine that mines bitcoin and processes transactions makes up a part of the network, and the machines work together. That means that, in theory, one central authority cant tinker with monetary policy and cause a meltdown or simply

decide to take peoples Bitcoin away from them, as the Central European Bank decided to do in Cyprus in early 2013. And if some part of the network goes offline for some reason, the money keeps on flowing.

2. It's easy to setup

   Conventional banks make you jump through hoops simply to open a bank account. Setting up merchant accounts for payment is another Kafkaesque task, beset by bureaucracy. However, you can set up a Bitcoin address in seconds, no questions asked, and with no fees payable.

3. It's anonymous

   Well, kind of. Users can hold multiple Bitcoin addresses, and they arent linked to names, addresses, or other personally identifying information.

4. It's completely transparent

   Bitcoin stores details of every single transaction that ever happened in the network in a huge version of a general ledger, called the block chain. The block chain tells all. If you have a publicly used bitcoin address, anyone can tell how many Bitcoin are stored at that address. They just dont know that its yours. There are measures that people can take to make their activities more opaque on the bitcoin network, though, such as not using the same Bitcoin addresses consistently, and not transferring lots of bitcoin to a single address.

5. Transaction fees are miniscule

   Your bank may charge you a 10 fee for international transfers. Bitcoin doesnt.

6. It's fast

   You can send money anywhere and it will arrive minutes later, as soon as the bitcoin network processes the payment.

7. It's non-repudiable

   When your bitcoins are sent, theres no getting them back, unless the recipient returns them to you. Theyre gone forever.

Chapter 5

Bitcoin: A Peer-to-Peer Electronic Cash System

5.1 Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyersA solution is proposed to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any

cooperating group of attacker nodes.

5.2 Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

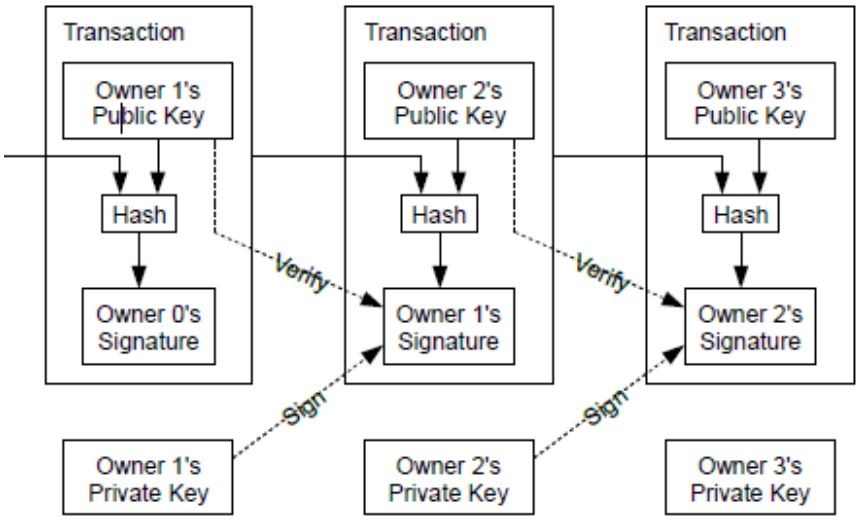

Figure 5.1: Transaction

The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank. We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly

announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

5.3 Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

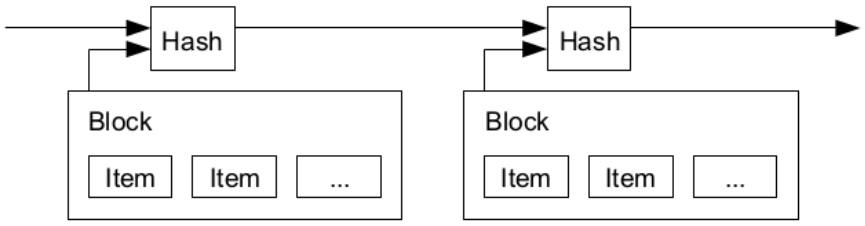

Figure 5.2: Timestamp Chain

5.4 Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash, rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.

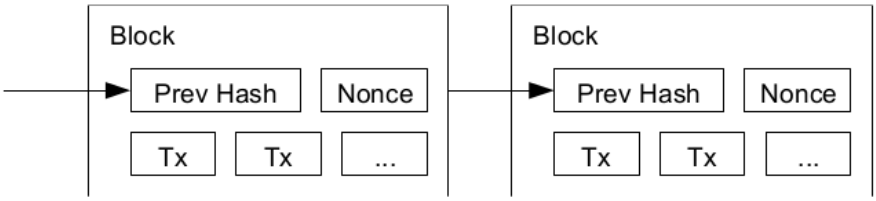

Figure 5.3: Block Chain

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5.5 Network

The steps to run the network are as follows:

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.

6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof- of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

5.6 Incentive

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

5.7 Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without

breaking the block's hash, transactions are hashed in a Merkle Tree, with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.

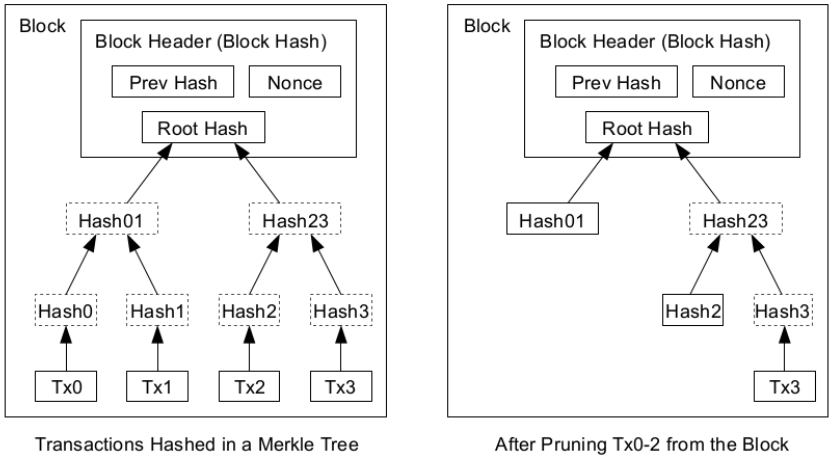

Figure 5.4: Transactions hashed in a Merkle Tree and pruning

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

5.8 Simplified Payment Verification

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.

As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to

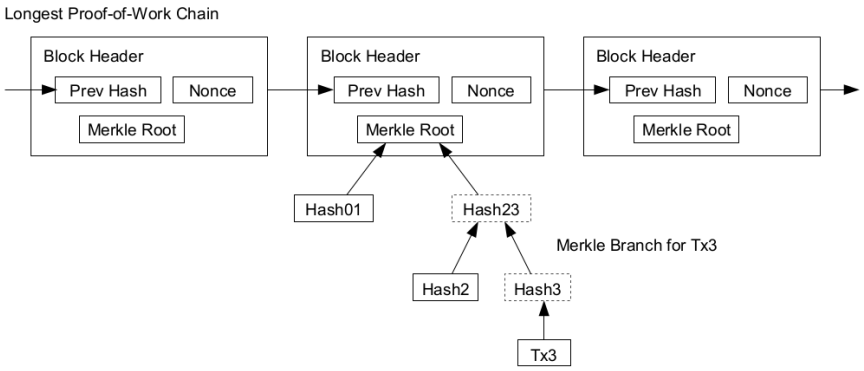

Figure 5.5: Proof-of-Work Chain

overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

5.9 Combining and Splitting Value

Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined,transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.

It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

5.10 Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public

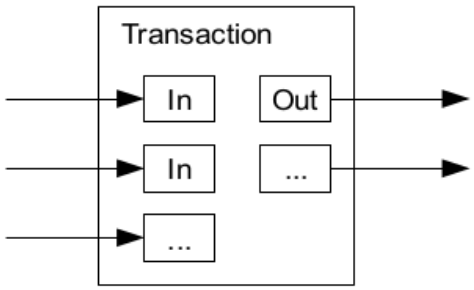

Figure 5.6: Inputs and Outputs in a transaction

keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

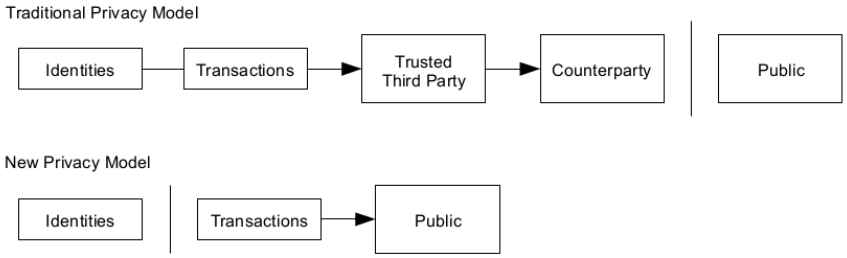

Figure 5.7: Privacy Models

As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

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)