Tiana Laurence

INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

THE MANY FACES OF BLOCKCHAIN TECHNOLOGY IN THE 21ST CENTURY

Van Haren
PUBLISHING

INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

Other publications by Van Haren Publishing

Van Haren Publishing (VHP) specializes in titles on Best Practices, methods and standards within four domains:

- IT and IT Management
- Architecture (Enterprise and IT)
- Business Management and
- Project Management

Van Haren Publishing is also publishing on behalf of leading organizations and companies: ASLBiSL Foundation, BRMI, CA, Centre Henri Tudor, Gaming Works, IACCM, IAOP, IFDC, Innovation Value Institute, IPMA-NL, ITSqc, NAF, KNVI, PMI-NL, PON, The Open Group, The SOX Institute.

Topics are (per domain):

IT and IT Management

ABC of ICT
ASL®
CATS CM®
CMMI®
COBIT®
e-CF
ISO/IEC 20000
ISO/IEC 27001/27002
ISPL
IT4IT®
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
SABSA
SAF
SIAM™
TRIM
VeriSM™

Enterprise Architecture

ArchiMate®
GEA®
Novius Architectuur Methode
TOGAF®

Business Management

BABOK® Guide
BiSL® and BiSL® Next
BRMBOK™
BTF
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
OPBOK
SixSigma
SOX
SqEME®

Project Management

A4-Projectmanagement
DSDM/Atern
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP®
P3O®
PMBOK® Guide
Praxis®
PRINCE2®

For the latest information on VHP publications, visit our website: www.vanharen.net.

Introduction to blockchain technology

The many faces of blockchain technology in the 21st century

Tiana Laurence

Van Haren
PUBLISHING

Colophon

Title:	Introduction to blockchain technology
Subtitle:	The many faces of blockchain technology in the 21st century
Author:	Tiana Laurence
Reviewers:	Atul Anand (Global MBA, SP Jain: Strategic Management, IIMC) Stefan Macica (Slovakia) Rita Pilon (EXIN) Scott Robinson (founder of Plug and Play FinTech) Mikulas Zalai (Slovakia)
Text editor:	Steve Newton
Publisher:	Van Haren Publishing, ’s-Hertogenbosch, www.vanharen.net
ISBN Hard copy:	978 94 018 0499 8
ISBN eBook pdf:	978 94 018 0501 8
ISBN eBook EPUB:	978 94 018 0504 9
Edition:	First edition, first impression, October 2019
Layout and DTP:	Coco Bookmedia, Amersfoort – NL
Copyright:	© Van Haren Publishing, 2019

This publication was produced with the utmost care and attention. Nevertheless, the text may contain errors. The publisher and the authors are not liable for any errors and/or inaccuracies in this text.

Preface

Dear reader,

You have heard buzz words like “bitcoin”, “blockchain”, and “cryptocurrency”. They are everywhere. Companies and governments have started to use blockchain technology in earnest and will increasingly do so for the foreseeable future. It is time to take an in-depth look at blockchain technology, and how you can take advantage of its potential.

This book is perfect for you if you are looking to expand your knowledge of blockchain technology but are not a programmer. It is about software but not written for technical experts. It assumes that you have little to no knowledge of the subject and will explain topics as simply as possible, while not obscuring details that may affect you. The book will give you insight into the critical differences in blockchain software and will provide you with a basic understanding of how and why they work.

After reading this volume, you will be able to speak with confidence on the topic, know key differences in technology, and why they are relevant to you, your company, and your industry. You will also have critical insight into blockchain software’s inherent limitations and shortcomings.

The popularization of blockchain has shrouded the sector into the realm of alchemy. Attaching the words “tokenization” and “blockchain” have spontaneously transformed the mundane into the magical. This book will demystify the topic and cut through the hype. You will understand the changes that are happening and uncover any pretense.

In this book, each chapter ends with review questions to help you better understand the core of the chapter.

I hope you will enjoy this book.

Kind regards,

Tiana Laurence

Contents

1 Introduction to Blockchain Technology

Blockchain has become an omnipresent term that encompasses a social promise and a new technology. Originally proposed as a solution for Bitcoin's cryptocurrency record keeping system, blockchains are now used to store the records of all types of applications.

Blockchain means something more in many people's minds. The promise many associate with blockchain applications is that they will collapse all centralized systems. Centralized systems are everywhere people need to trust a counterparty and don't have the resources themselves to do so independently.

An easy way to identify a place where blockchain technology may be applied is to look for areas where a middleman is needed to facilitate trust. Trust is essential for things such as the transfer of money, voting, land records, IP rights, and identity. Blockchain software can be programmed to take the place of the middleman by becoming the trusted record keeping system.

In this chapter, you will learn the basics of blockchain software. This includes the vital concepts that govern most blockchains, economic models, and network structures. It will help you lay a strong foundation for understanding how the technology works and what it is capable of doing.

1.1 Key blockchain concepts

Blockchain technology has come a long way since the initial vision published by Satoshi Nakamoto in the Bitcoin white paper in 2008. Buzz words like "bitcoin", "blockchain", and "cryptocurrency" are everywhere. Companies and governments have started to use blockchain technology in earnest and will increasingly do so for the foreseeable future.

Since its initial conception, blockchain has encompassed both a social promise and new technology. Originally proposed as a solution for Bitcoin's cryptocurrency record-keeping system, blockchains are now used to store the records of all types of applications.

Core services you may depend on every day such as the transfer of money, payments, voting, land records, IP rights, and identity all rely on intermediaries. Blockchain software has begun taking the place of these antiquated systems. The software becomes the trusted record-keeping systems, and the rules programed into the software become the intermediaries.

It is important to note that blockchains can be used for more than just recording the transfer of value between two parties. The primary benefits of cryptographic identity, historical and chronological provenance, and the transparency of the networks complete history work exceptionally well for many industries that require two parties to trust each other.

Pigeonholing blockchain technology solely for financial transactions is a very limited perspective. Before you can fully grasp the potential applications of blockchains as part of a technology stack, it's important to understand how the technology works. In the following section you will learn about the key concepts that make blockchain technology revolutionary.

What is a blockchain?

Blockchain technology structure was first described in the Bitcoin white paper as a peer-to-peer distributed time-stamp server. The author, Satoshi Nakamoto (possibly a fictitious name), wanted to create a peer-to-peer electronic cash system that did not need a network of banks to operate. Satoshi described "blocks" and "chains" as a way of organizing and securing records, such that once entries had been made into a shared database, they could be proved mathematically correct and to have remained unchanged.

Satoshi's description of blocks are groups of transactions that have occurred over a period of time. A transaction, in the case of Bitcoin, represents the transfer of some cryptocurrency, known as bitcoin, from one user to another.

For example, Sally sends you a bitcoin, you receive it, and the transfer of the bitcoin between the two of you is recorded as a "transaction". Bob, Joe, Mark, and Tammy send each other bitcoins at the same time. All of these transactions are bundled into a block and are recorded in the Bitcoin blockchain.

Blockchains have a special way of recording the transfer of bitcoins from one party to another. The transactions are time-stamped and signed by the sender of the bitcoin. So, in the example above, Sally signs the transfer of bitcoin to you. Sally's signature for the transfer of bitcoin is not an ink and paper kind. Sally signs electronically or rather cryptographically, with what is called a private key. What this means is that the blockchain software can tell she and no one else has the authority to transfer that bitcoin.

Once Sally's transaction with you has been recorded in the block with all the other bitcoin transfers, the block is sealed and linked to the other blocks of transactions. Blocks are sealed and linked by hashes. Hashes are created through a cryptographic hash function.

How hash functions are used in blockchains is very clever but simple. All the data that make up a block of transactions are processed. The output of this mathematical process is a string of numbers and letters of a fixed-size, for Bitcoin it is 32 bytes. If the input does not change, the hash function will always result in the same output string. Hash functions are a covenant way in computer science to prove data has not changed.

Once a hash has been generated from a block, the fixed string of numbers and letters is recorded in the next new block of transactions. Recording the hash of the previous block of transactions links one block to another chronologically. Removing a block, or even a single

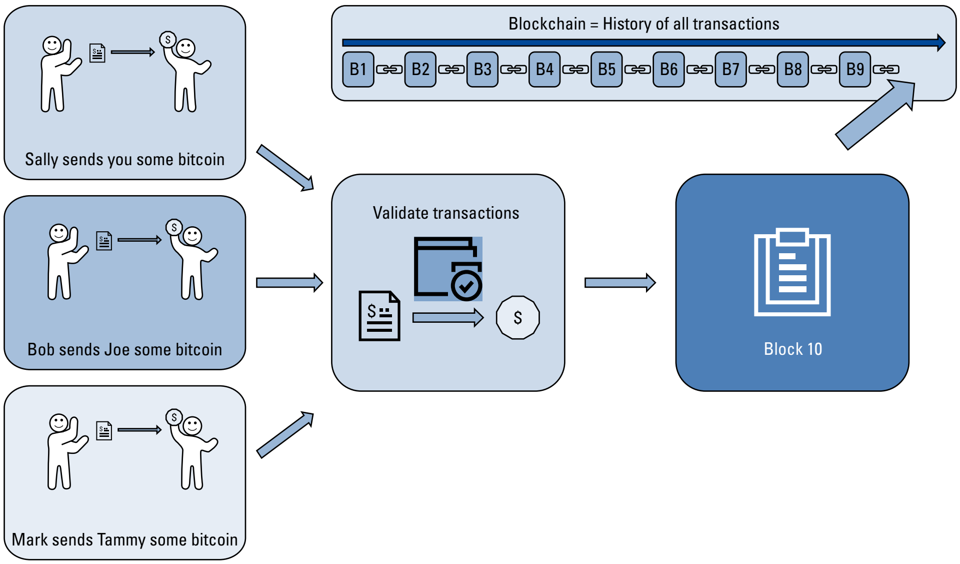
Sally sends you some bitcoin
Bob sends Joe some bitcoin
Mark sends Tammy some bitcoin
Validate transactions
Block 10
Blockchain = History of all transactions
B1
B2
B3
B4
B5
B6
B7
B8
B9

Figure 1 What is a blockchain?

transaction, from within a block would break the record and would instantly be noticeable to everyone, as your fixed string of 32 characters would not match their fixed string. See figure 2.

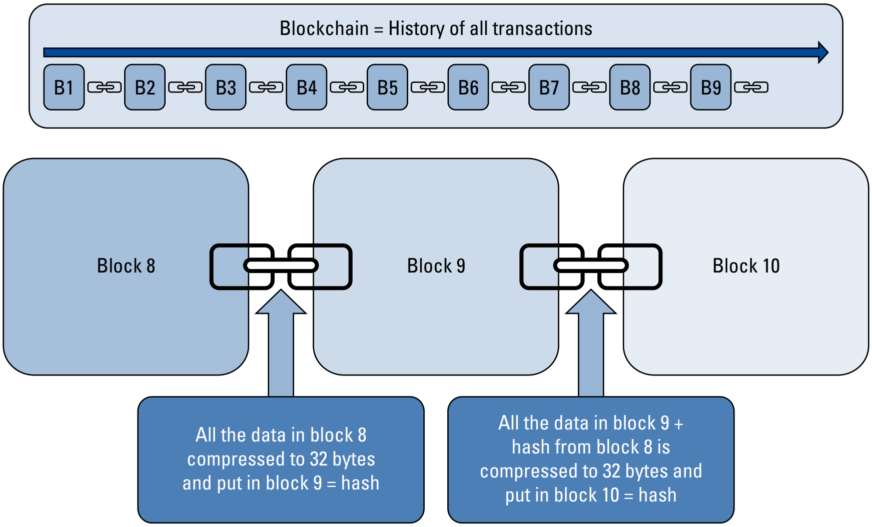
Blockchain = History of all transactions
B1
B2
B3
B4
B5
B6
B7
B8
B9
Block 8
Block 9
Block 10
All the data in block 8 compressed to 32 bytes and put in block 9 = hash
All the data in block 9 + hash from block 8 is compressed to 32 bytes and put in block 10 = hash

Figure 2 Hash function in blocks of transactions.

Satoshi's goal was to prevent Sally from sending the same bitcoin to you and someone else and thus defrauding the network. The "block" and "chain" of blockchain technology is a clever way of structuring and recording transaction data chronologically. It keeps track of "who" owns "what" and "when".

The Bitcoin white paper incorporated an incentive program for participants to process new transactions and to keep an unaltered record of every past transaction. In Bitcoin, this incentive system is called mining, and the incentive given to the miners is the cryptocurrency bitcoin, see figure 3.

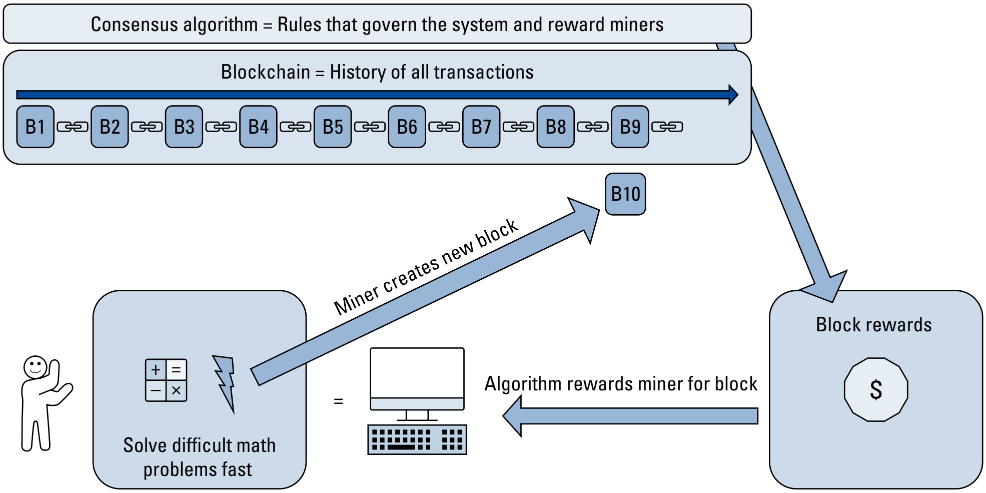
Consensus algorithm = Rules that govern the system and reward miners
Blockchain = History of all transactions
B1
B2
B3
B4
B5
B6
B7
B8
B9
B10
Miner creates new block
Block rewards
$
+ =
– ×
Solve difficult math problems fast
=
Algorithm rewards miner for block

Figure 3 The concept of mining.

Satoshi understood that if a single person or entity had master editing power over the records, then the transaction could be altered, defeating the purpose. If the record was broken, then it may be possible for Sally to send you and Bob the same bitcoin.

Satoshi, possibly inspired by the financial crisis of 2008, wanted to stop fraudulent transactions without needing a third party to aggregate records and provide trust that everyone would operate in good faith. Satoshi proposed that the aggregation of records could be done with software via a peer-to-peer distributed time-stamp server and trust could be established through cryptographically-provable mathematics. This system of record keeping is what you now known as a blockchain.

What are nodes?

When a computer connects to a blockchain network, the computer becomes a *node*. A node runs the blockchain software for the network and keeps the network healthy by engaging in the transfer of information. Anyone can run a node on a public network like Bitcoin. Nodes broadcast bitcoin transactions to other nodes throughout the network. However, not all nodes are the same.

There are several classifications of nodes depending on the level of participation and the type of blockchain network. Every network has different roles available. For example, when you run a node that has a complete history of the network's transactions and verifies all of the rules of the system, it is called a *full node*. Full nodes download every block, and then they check each transaction and block to make sure they are compliant with the rules of the network. The network's rules are called its *consensus system*. See figure 4.

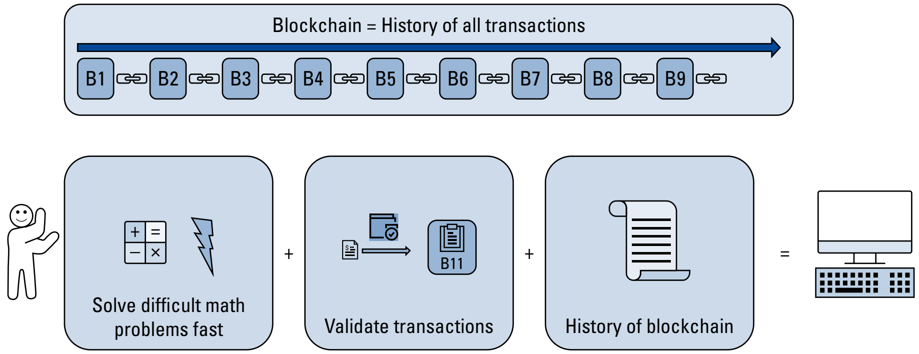
Blockchain = History of all transactions
B1
B2
B3
B4
B5
B6
B7
B8
B9
Solve difficult math problems fast
+
B11
Validate transactions
+
History of blockchain
=

Figure 4 What is a node?

Every blockchain has unique consensus rules. These rules cover things like the number of cryptocurrency units rewarded to miners and how transactions and blocks are formatted. When a full node finds a transaction or block that breaks the consensus rules, the node rejects the transaction or the block. Each full node works independently.

Operating a full node can be resource-intensive. It requires downloading every transaction for the full history of that blockchain. Full nodes need all new transaction records. They keep all *block headers*. Block headers identify a unique block and contain a hash of the previous block. All of this data adds up and takes up a lot of room. The Bitcoin blockchain is hundreds of gigabytes in size and growing every day.

However, there is a way to connect to a blockchain, without committing as many resources to the network. This is called a *lightweight node* or *client*. Lightweight nodes verify transactions by piggybacking on the work of full nodes. They only download the headers of all blocks and then check transactions utilizing a system called Simplified Payment Verification (SPV). As you may remember, the block headers contain hashes that prove that each block is in order and has all its transactions.

Operating a lightweight node may seem appealing. However, they are vulnerable to being tricked by bad actors. Because the SVP method is only checking the blockchain header, the lightweight node may accept transactions or blocks that are not valid. If you think you have received some bitcoin for example, but in reality you have not, this could cause financial issues. Full nodes provide the highest protection from fraud related to the transfer of cryptocurrency.

Another common way to connect to a blockchain network is to mine. A *miner* is a type of node that is adding transactions to new blocks. Miners compete to win the right to create a new complete block by solving a complex mathematical problem. Each miner will write their answer in the block header and if they are correct, they are then rewarded with cryptocurrency. The problem that miners are trying to solve is to guess a number that, when combined with the hashed transaction data from the block, returns an answer that is within a specific range called a "nonce". For Bitcoin, a nonce is a number between 0 and 4,294,967,296.

The first miner to get a hash within the desired range broadcasts the winning number to the rest of the network. All the other miners promptly stop their work on that block and start guessing the nonce for the next block. At that point the competition for the next new block begins.

Miners opt into the ruleset by accepting the software upgrades. The network has available upgrades that users elect to adopt by updating their software. You can think of the upgrades as software patches. The upgrades are only as good as the acceptance and use by the miners. There are three critical distinctions in blockchain nodes that are worth understanding as these affect the assumptions that are made around fairness, censorship, and permanence of data.

Public blockchain nodes

Public blockchains are open to anyone in the world to participate in the functions of the network, only limited by their access to the internet, hardware, and electricity. This means that you can be a miner earning cryptocurrency as your secure blocks, a full node checking transactions, or a lightweight node sending and receiving messages on the network. There are no gating mechanisms, no one to ask permission and no licensing fee. The software is held in an open license such as the Apache or MIT license. Prominent examples of this type of network include Bitcoin and Ethereum.

Permissioned blockchain nodes

Permissioned blockchains are private networks that utilize some blockchain technology but not all. Most don't incorporate any kind of mining and so do not have a native cryptocurrency. This means that there are no disinterested third parties securing blocks, the blocks and transactions are all processed by known participants. The participants all have a vested interest in the integrity of the records. Often these networks are built by for-profit companies and are operated by consortiums such as R3.

Nodes on a Corda network

R3 (www.r3cev.com) built a consortium with more than 100 of the world's leading banks and insurance companies. They work to streamline redundant business processes by integrating blockchain technology.

Corda is the blockchain protocol behind R3. It is a distributed ledger platform, often referred to as "DLT" (distributed ledger technology). Breaking down the jargon, a "ledger" is a general term for describing records used to account for something and "distributed" means that the record is kept in more than one location. It is designed specifically to manage and synchronize financial agreements between regulated financial institutions.

The R3 platform works very differently from public blockchains. There is no mining, and the transmission of data is not public in the same sense as it is on platforms such as Ethereum or Bitcoin. Unlike public blockchains that broadcast their transactions to the whole network, transactions execute in parallel on different nodes. Each node is unaware of the other's transactions. The history of each network is on a need-to-know basis and cannot be viewed by the public.

Key features of Corda include the following:

- Controlled access to the network;
- Observer node for regulators;
- Transactions are validated only by the parties involved;
- Compatible with multiple consensus mechanisms;
- No mining and no cryptocurrency.

Nodes on a Hyperledger Fabric network

Nodes on Hyperledger Fabric (see also: https://www.hyperledger.org/projects/fabric) are called Peers and Orderers. Unlike public blockchains that have nodes validating transactions or mining, the nodes on Fabric host the ledger's data and make sure it's in order. The data they host may include smart contracts, orderers, policies, channels, applications, organizations, identities, and membership. Another important distinction is that a Fabric peer can host more than one blockchain ledger. This feature allows for flexible architecture in the design of your private blockchain system.

Blockchain applications connect with peers on Fabric through APIs, application programming interfaces. The APIs allow you to invoke Fabric smart contracts in order to create transactions. Once you have submitted your transaction, they will be ordered and committed to Fabric. This does not just happen right away. The transaction must get approval from enough peers before the ledger is changed. It is possible to have two or more peers agree to cooperate privately. In Fabric this is called a *channel*. In the channel, the peers agree to collaborate to share and manage identical copies of the ledger associated with their channel.

Otherwise, when you submit a transaction, there is a three-phase process. This process ensures all peers keep their ledgers consistent with each other, see figure 5. This is where orderer peers are important. Their job is to ensure that every peer's ledger is kept consistent. Single peers cannot update the ledger by themselves.

- Phase 1: an update to the ledger is requested by a blockchain application. Peers will endorse the transaction. Once a transaction has gained enough endorsements, the transaction will move to phase 2.

- Phase 2: the endorsed transactions are collected together and packaged into blocks. The orderer is crucial to this process. Peer audit by an orderer ensures this is done correctly.

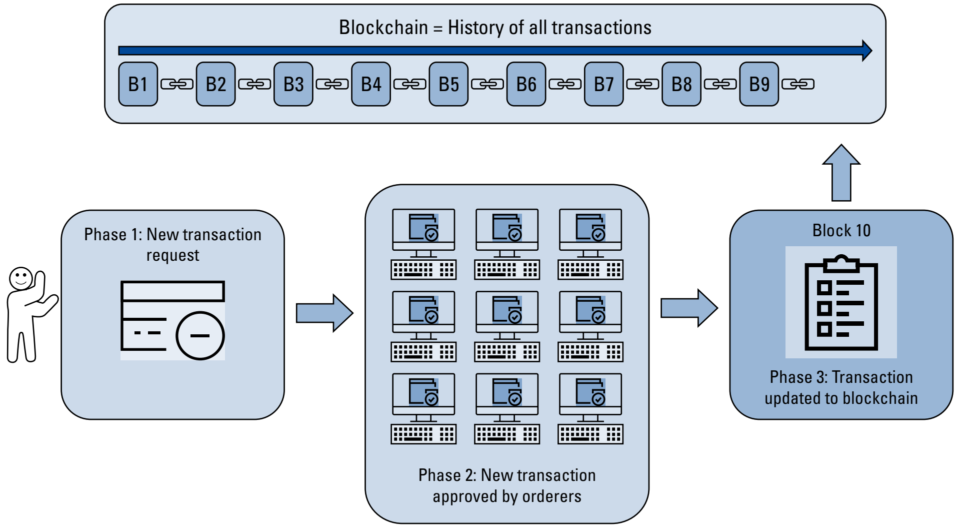
Blockchain = History of all transactions
B1
B2
B3
B4
B5
B6
B7
B8
B9
Phase 1: New transaction request
Phase 2: New transaction approved by orderers
Block 10
Phase 3: Transaction updated to blockchain

Figure 5 The Fabric three-phase process.

- Phase 3: the new block that was created is broadcast back to every peer so that they can update their blockchain record. Each transaction in the new block is then validated by the peer before being applied to its copy of the ledger.

Federated blockchain nodes

Federated blockchain nodes can exist in both public blockchains and private blockchains. Federation is when the system, or rather the user of a system, elect nodes to process transactions. Designating a few nodes to do most of the work of maintaining the blockchain records has its advantages and disadvantages.

One of the main reasons why systems choose this type of architecture is because it can reduce the raw cost of processing transactions and it can increase the speed at which the blockchain is updated and transactions are cleared.

However, there are some very good reasons to not have federated nodes. Blockchains are often judged to be less resilient to corruption when they have fewer nodes operating and securing the network. It is more feasible to take over a handful of computers and their operators then it is the ten thousand or more nodes that operate at any given time on the Bitcoin network.

Here are a few examples of blockchain networks that operate with some form of federation or designated nodes.

Factom is a public blockchain that has two classes of federated nodes, see figure 6. Half of these are processing transactions whilst the other half watch to make sure that the nodes processing the transactions are accurate and not censoring transactions. Users of the system elect nodes to be Federated Factom nodes. Factom does not use mining but does have