

JOHN PALFREYMAN

**BUSINESS
BLOCKCHAIN**

**UNLOCKING
TRANSFORMATIONAL
POTENTIAL**

CONTENTS

Contents.....	5
Foreword	6
User guide.....	12
1. Blockchain basics	13
2. Brief history of blockchain	23
3. Building blocks.....	31
4. Platform choices.....	49
5. First project	57
6. Business usage	91
7. Government blockchain	117
8. Security and privacy	133
9. Starting the journey.....	143
About the author.....	152
Credits.....	154

1. BLOCKCHAIN BASICS

Blockchain is a new method of recording transactions within a business network which adds efficiency and trust to the exchange of assets between network members.

There are five fundamental components of business blockchain. The shared ledger records who owns what; smart contracts determine when transactions occur; privacy services control who can see what and make transaction records tamperproof; consensus is the method used to determine if transactions are valid and business network connecting the different organisations.

When applied to the right business use case blockchain can save time, increase efficiencies, reduce risk and increase trust.

When asking the simple question “what is blockchain?” one is often confronted with a barrage of technical gobbledygook and seldom given a concise, business explanation of the technology, how it works and its key benefits. I address this by explaining blockchain in clear terms that can be understood by a business practitioner wishing to find out how this new technology can change their organisation for the better.

I will focus on blockchain used by businesses, where the technology is applied across a business network where the participants are known. I will touch upon cryptocurrencies, but only to explain the difference between them and blockchain for business.

I will strive to avoid technical jargon and too much detail and where possible give pointers should the reader wish to understand the underpinning technology to the next level of detail.

1.1 WHAT IS BLOCKCHAIN?

Businesses always work together in a network with other businesses, banks and government departments. Ownership of assets – tangible (e.g. a car, a house) or intangible (bonds, intellectual property) pass across the business network in return for payments and governed by contracts.

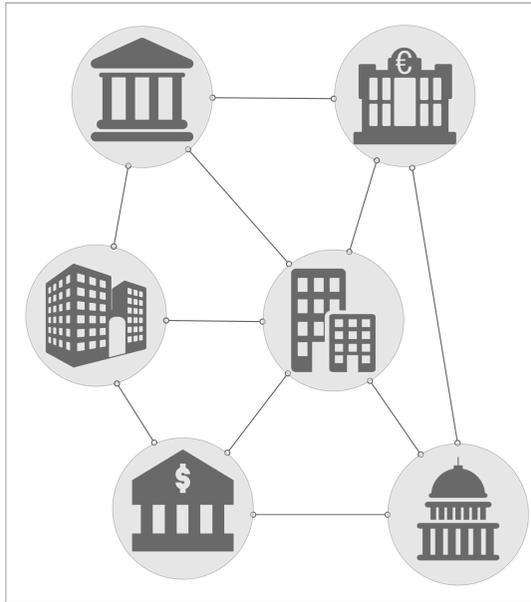


Figure 1: Businesses operate in a network

Each network participant keeps their own ledger (or book of record) – recording all assets they own and any changes to those assets.

Although well tried and tested, this process is very inefficient, vulnerable to fraud or cyber attack and is often piling cost on cost. In particular, the need for separately managed ledgers to all be updated correctly across the business network often leads to disputes and costly reconciliation. It's far from fit for the needs of the twenty first century!

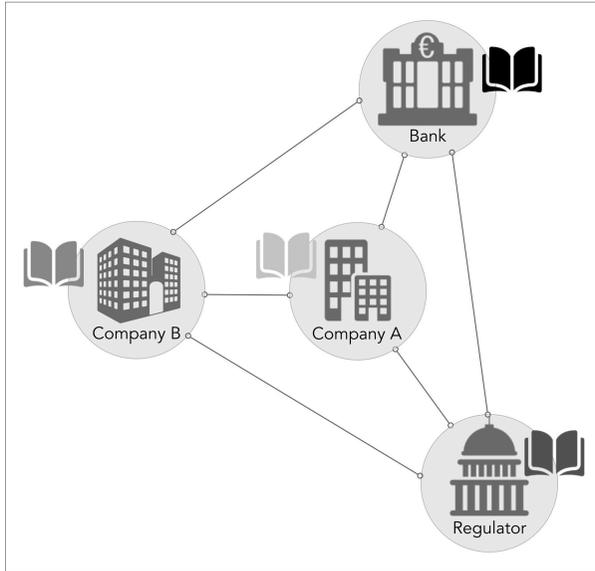


Figure 2: Traditionally, each business has their own ledger

Blockchain gives participants the ability to share a ledger which is updated every time a transaction occurs. Privacy services (rendered with cryptography) ensure that business network members see only the parts of the record that are relevant to them, and that transactions are secure, authenticated and verifiable.¹

¹https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf

Blockchain also allows the (smart) contract for asset transfer to be embedded in the shared ledger to govern the execution of the transaction. Business network participants agree how transactions are verified through a process called "consensus". Regulator oversight, compliance and audit can be part of the same network.

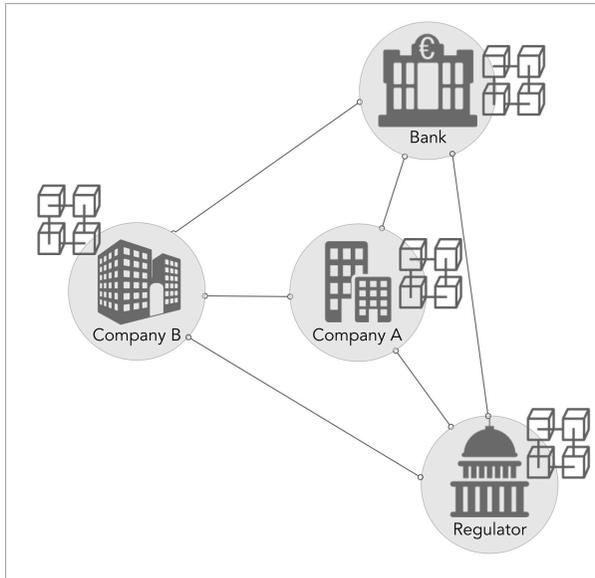


Figure 3: Blockchain enabled business network

The first application of blockchain technology was to underpin the bitcoin cryptocurrency. This leads to much confusion between bitcoin and blockchain, which could prevent organisations realising the full benefits from business blockchain. I will detail the relationship between blockchain and bitcoin in Chapter 3.

1.2 HOW DOES IT WORK?

“How does blockchain work?” is an interesting question. For a business user, one could counter with “why do you want to know?”. The internet is used extensively for business, but few business users are interested in how it works. I’m pretty sure that this will be the same for blockchain once the technology matures.

If we strip away all the technical stuff, it’s pretty straightforward. Suppose our business network consists of Peter, Susan and George who share a vehicle ownership ledger, recording who owns which vehicle. Peter has decided to transfer ownership of his car to Susan when she pays him £500. Once the money is received, Peter tells George and Susan that he wants to make this transfer, and if they are in agreement the ownership change is written into the ledger in a way that it cannot be changed and all copies of the ledger are updated. If they are not in agreement, the money is returned to Susan. Privacy services ensure that Peter and Susan can see full details of this transaction, whilst George sees only that the transaction has occurred, but does not have access to the full details.

The technical building blocks that make this possible are outlined in Table 4.

Blockchain feature	Technology
Trusted agreement of a transaction (ownership change).	Consensus algorithm, details are highly dependent on the use case.
Once money is received, car ownership transfers.	Smart contracts will specify the conditions for asset movement.
Transaction cannot be changed once written to ledger.	Privacy services - specifically cryptography - used to "lock" the transactions details once written.
Ledger is shared between parties in business network.	Peer to peer replication technologies, first used in file sharing.
Control over who can see transaction details.	Again privacy services - specifically cryptography - used to control visibility of transactions on ledger.

Table 4: Technology building blocks

This leads to the five key components of a business blockchain:

1. **Shared ledger** - recording who owns what.
2. **Privacy services** - making transactions tamper proof and controlling access.
3. **Smart contracts** - determining when a transaction occurs.
4. **Consensus** - the method used to determine that a transaction is valid.
5. The **business network** - connecting the different organisations.

I will explain each of these in Chapter 3, and provide details of how each is rendered with underpinning technologies.

1.3 BLOCKCHAIN BENEFITS

Sometimes misunderstood and often exaggerated, real business benefits can accrue when blockchain is used correctly. There are four fundamental benefits from blockchain usage, as listed in Table 5. These benefits are realised in different ways depending on the business usage of blockchain.

Blockchain benefit	How is benefit realised?
Saves time, through near instantaneous transactions.	Complex, multi-party transactions can be agreed between relevant parties and executed efficiently.
Increases efficiencies, by removal of costly overheads and intermediaries.	Appropriate access to shared ledger granted to members of the business network.
Reduces risk of tampering, fraud and successful cyber attack.	The ledger is distributed to members of the business network, thus increasing resilience.
Increases trust across business network.	Business network members share business processes and tamper proof records of asset ownership on the shared ledger.

Table 5: Blockchain benefits

I will explore the business usage of blockchain in Chapter 6 by describing how the emerging technology can improve the transfer of different asset types around a business network.

A foretaste of this is in Table 6, which lists example business usage for each blockchain benefit. Through the book such business usage is referred to as a “use case”.

Blockchain benefit	Example business usage
Saves time, through near instantaneous transactions.	Complex letters of credit governing international trade replaced by shared ledger of asset ownership and location, with smart contracts governing payment.
Increases efficiencies, by removal of costly overheads and intermediaries.	Internal and external audit granted controlled access to the shared ledger reducing cost of audit, whilst improving reliability of result.
Reduces risk of tampering, fraud and successful cyber attack.	Shared ledger of asset ownership, location and authenticity removes risk of counterfeit goods in a supply chain.
Increases trust across business network.	Dispute resolution by maintaining a trusted record of asset status with a complete audit trail of changes.

Table 6: Realising blockchain benefits

1.4 CONCLUDING REMARKS

This first chapter in the book is by design the shortest. By focussing on the core components, key benefits and a few quick examples of business usage, I hope it has given you a taste of business blockchain which I will develop further in the rest of the book. After giving a little historical background, I will “unpack” business blockchain, giving details of the core components and how they work together to realise this business benefit.

These realisable business benefits are critical for a meaningful blockchain project. I plan to make them clearer through the book with comprehensive illustration and explanation of how they are realised in practice in Chapter 6.

1.5 REFLECTIVE QUESTIONS

1. What are the three most important organisations in your business network?
2. What are the main assets that you transfer?
3. What asset transfers take the most time, and / or are the most inefficient?
4. What’s the current level of trust across your business network?
5. What personal experience / opinion do you have with bitcoin?

To read the rest of Business Blockchain, please visit <http://bit.ly/BizBCBook> or search “palfreyman blockchain” on your local Amazon site.