The Permanent Record

BlockChain As a Consistent, Persistent Data Service

OverStory Ltd
info@overstory.co.uk

What is Blockchain and What Is It Useful For?

This presentation provides a high level introduction to blockchain and its concepts. It focuses on what it is and how it can be used, rather than the technical details of how it works. We aim to illustrate what blockchain is, and to show why blockchain is an important new technology with wide ranging implications across many fields.

"Predicting the future is easy. It's trying to figure out what's going on now that's hard."

- Fritz R S Dressler

About OverStory

OverStory is a UK-based technology consultancy that has assisted clients around the world by providing advice and bespoke IT solutions.

We specialise in modern, robust and elegant designs and implementations using the most appropriate technologies for the problem space.

Genesis of BlockChain

It Started With Bitcoin

In October 2008, a paper titled *Bitcoin: A Peer-to-Peer Electronic Cash System* was published on a cryptography mailing list by someone using the name Satoshi Nakamoto.

It is still unclear if Nakamoto is a real person or an alias, possibly for several people.

The Bitcoin paper and associated Open Source code laid out a system of cryptographically secured currency, “cryptocurrency”, that does not require a central authority (i.e. government, bank or other trusted party) for settlement.

Bitcoin solved two significant problems with electronic money:

1) The *double spending problem*
Occurs when there is a delay between spending and reconciling. Blockchain requires *consensus* to create new transactions, which forces a strict sequencing.

2) *Trustless networks*
A system that depends on trust of third parties is always subject to subversion and/or fraud.

By design, blockchain addresses both problems.

© 2017 OverStory Ltd | overstory.co.uk

A Shared Distributed Ledger

Bitcoin is a digital cryptocurrency. It uses cryptographic keys to encode exchanges of value.

What makes it unique is the globally distributed ledger. The records are distributed globally, and prevent conflicting updates (double spend). Each block in the chain is cryptographically locked to its neighbours. Tampering with a block breaks the chain.

No central authority, such as a bank or government, is needed to settle transactions because all needed information is on the chain.

The blockchain, as the name implies, is an ordered chain of transaction blocks. It's also a protocol for sharing and copying those blocks among cooperating network nodes.

Blockchain imposes an economic cost by requiring payment to add new transactions to the chain. This computationally intensive *mining* process makes it prohibitively expensive to cheat by tampering or creating fraudulent blocks.

It also means that the network can be *trustless*, where none of the nodes trust any of the others, but the chain still functions reliably.

© 2017 OverStory Ltd | overstory.co.uk

BlockChain Is Not Cryptocurrency

Bitcoin Needs Blockchain, But Not Vice Versa

The blockchain is an ordered sequence of data blocks that form an unbreakable chain. New blocks cannot be added without consensus from the nodes (each holding blockchain copies).

A block cannot be modified without re-computing all subsequent blocks - which is very expensive and would require collusion by a large percentage of nodes in the network.

Bitcoin exploits this to reconcile and record currency transfers in a way that all parties can agree and depend upon.

Although blockchain was invented to underpin Bitcoin, it can in theory be used to record any sort of information.

A shared, immutable, permanent public record system has myriad uses. Non-currency uses for blockchain technology is where much of the innovation is happening now.

Certification, property records, life events, logistics, livestock, fraud prevention, etc, are all candidates for blockchain-based solutions

The Blockchain Is Forever

Records written to the blockchain last forever. It is not possible to overwrite or tamper with completed blocks. Recorded transaction data can never be lost or refuted.

There are thousands of nodes in a blockchain network and each of them holds a complete copy of all blocks in the chain. Nodes can join or leave the network without compromising the integrity of the blockchain itself.

Adding transactions can be relatively slow (a few seconds to a few minutes), but queries of the blockchain are typically very fast.

The massive redundancy inherent in a blockchain network makes it very resilient and highly available. It's essentially indestructible.

Blockchain nodes get paid (in cryptocurrency) to create new blocks, so it's in their interest to always be available. Yet the network does not depend on any specific nodes. This yields a ubiquitous fabric of blockchain computing resources, always available, always improving.

© 2017 OverStory Ltd | overstory.co.uk

BlockChain Is a Shared Database

A Ledger Is A Database

A currency account is a simple database. It's essentially a table with rows, each of which contains a few columns. Relational databases are designed around this basic metaphor.

But the transactions in a blockchain ledger need not be limited to a few columns of numbers. They can be generalized to store arbitrary information.

Data stored in blockchain transactions enjoy all the benefits of monetary Bitcoin transactions.

Every blockchain transaction has a unique address, like a database primary key. With this address, the data can be retrieved by anyone with access to a blockchain node.

The blockchain database is massively distributed. It's also massively redundant. Any data successfully added to the blockchain will effectively last forever.

Data on the blockchain is irrefutable. All nodes have a copy of it. It cannot be deleted or changed. Ever.

© 2017 OverStory Ltd | overstory.co.uk

BlockChain Provides New Solutions

Bitcoin is Yesterday, Ethereum Is Tomorrow

The Bitcoin blockchain was the first. It was designed solely for the purpose of recording Bitcoin transactions.

Using the Bitcoin blockchain for other purposes is difficult due to those design limitations.

Other cryptocurrencies have been developed with their own blockchain variants, some of which are much better for storing other forms of data.

Each makes a different set of trade-offs.

The emergent dominant successor to the Bitcoin blockchain is *Ethereum*.

While Ethereum also has a cryptocurrency, Ether, its design emphasizes the blockchain rather than the currency aspects.

Ethereum is a sophisticated system that not only records data but also stores executable code, known as *smart contracts*.

Smart contracts up the game for blockchain, extending the distributed database to be a massively parallel compute engine.

© 2017 OverStory Ltd | overstory.co.uk

Ethereum Is Smart

Ethereum’s smart contracts enable a whole new class of applications.

Rather than simply storing a transaction record to show the result of an operation, the operation itself can be stored in the Ethereum blockchain.

This has many uses: i.e. validation that a transaction meets certain criteria (that a property description is valid, for example), enforce prerequisites (by checking that related past, or future, transactions have been recorded), calculating and paying commissions, etc.

Ethereum smart contracts can be so sophisticated that they constitute Democratic Autonomous Organizations (DAO).

A DAO can, conceivably, become a fully self-sustaining, independently functioning business (or government agency?) that can operate indefinitely with no human intervention.

It’s too soon to know if DAOs will become our new digital overlords, but smart contracts hold great promise (and perhaps a bit of danger).

BlockChain Solves Old Problems

Question Authorities

Blockchain can be applied almost anywhere that permanent, authoritative records are required. Traditionally these have been maintained by governmental agencies or other organizations that have been charged with a duty of public trust.

It's vital that there be a single source of truth for things like property deeds, birth/marriage/death certificates, business and professional licenses, educational qualifications, tax records, etc. It's also essential that these records never be lost or tampered with.

Placing these records on the blockchain assures:

- they will persist,
- they will not be changeable
- they will always remain public
- they will always be available.

Even if the responsible authority ceases to exist, due to natural disaster, political upheaval, war, famine, pestilence or whatever.

Such indestructible records can be invaluable in the aftermath of a disaster to establish ownership, settle disputes, identify victims, etc.

© 2017 OverStory Ltd | overstory.co.uk

BlockChain Creates New Opportunities

New Tricks For Old Dogs

Blockchain in general and Ethereum in particular not only offer new solutions to old problems, they also present opportunities for doing things that weren't possible before.

The blockchain is a massive, resilient, distributed, reliable database in the cloud that you can use for free. Although there is a cost for adding things to the chain, reading them is, for the most part, free.

For many applications this can be a tremendous saving in cost and complexity.

Because the blockchain is trustless, you can collaborate and do business with parties that you may not necessarily trust. With smart contracts it's easy, for example, to set up an escrow system that automates arm's length sales or exchanges.

Because the blockchain exists independently of any single person or organization, the information you you store there will persist indefinitely even after your business (and you) are gone.

You can make promises that the blockchain will keep for you.

© 2017 OverStory Ltd | overstory.co.uk

Blockchain is a thing. There’s more to it than a funny-money scheme. It’s real and it will affect your life. You should know about it.

Thank You

OverStory Ltd
info@overstory.co.uk
overstory.co.uk
@overstory