TITAN
CONSULTING
INSIGHTS

BITCOIN, BLOCKCHAIN, & CRYPTOCURRENCY SERIES:

OVERVIEW AND INTRODUCTION

by Keith Johnson, Practice Manager

As SAP specialists, our expertise lies in optimizing enterprise solutions, but the rising significance of Bitcoin and Blockchain technology has captured our attention. In this three-part series our goal is to simplify Bitcoin for readers of all backgrounds. In part one, we start with the basics, building a foundation for understanding this groundbreaking technology. By stepping beyond SAP, we aim to offer a public service – providing clear and easy-to-understand insights into one of today's most transformative innovations. Let's dive into the basics of Bitcoin.

— Warren Norris, Managing Partner

Welcome to Bitcoin, Blockchain, and Cryptocurrency. If you're new to all this, don't worry, this is for beginners. We're going to use casual, simple language to help you go from not knowing what these terms mean to understanding how they work. We will start by breaking down the basics; like how Bitcoin works, why it's decentralized, and why it was created in the first place. We'll also look at some exciting opportunities in the crypto world later in this series.

At the core of everything is blockchain technology, which is what makes cryptocurrency tick. We'll explain what it is, why it's so powerful, and how it's changing industries beyond just crypto. Our goal is to make the world of cryptocurrency easier to understand and give you the confidence to explore it yourself. By the end of this paper, you'll not only understand blockchain and how it works, but also how other areas like crypto wallets and cryptography play a role in supporting blockchain technology. **Whether you're interested in learning about the technology, looking for ways to invest in it, or just curious about its impact, this series is for you.**

Before we get into the technology behind cryptocurrency, let's take a step back to see where it all started - Bitcoin, the very first cryptocurrency.

How Bitcoin Got Its Start:

Bitcoin was created by someone (or maybe a group) going by the name Satoshi Nakamoto. That's about all we know – whether it's a real person, a pseudonym, or a group of people is still a mystery.

Nakamoto is credited with creating both Bitcoin and the blockchain technology behind it, and made it available to everyone, allowing developers around the world to help build the Bitcoin network. This approach is called open sourcing, and it allows the source code to be shared freely for anyone to review, modify, or improve. Today, volunteer developers play a crucial role in maintaining and improving the Bitcoin network. Because Bitcoin's code is open-source, it's constantly reviewed by the global developer community. This decentralized model helps ensure Bitcoin remains secure and trustworthy, with no single entity controlling its direction. We'll take a closer look at the decentralized model in a later section.

This system was designed to let people transfer the new currency, Bitcoin, between each other using a blockchain-based program. Operating outside the control of any central authority, it allows anyone to set up their own Bitcoin node – currently around 15,000 – to help process transactions. In return, those running nodes are rewarded with transaction fees and newly minted Bitcoins.

Blockchains:

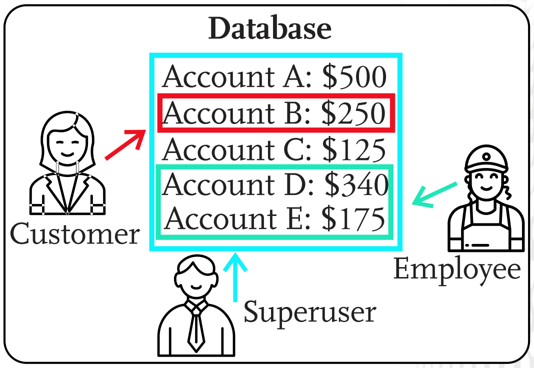
Blockchain is a buzzword that gets tossed around a lot, but for many it's unclear what it means, so let's clear that up. A blockchain is basically a digital ledger that records transactions – imagine it as a list where new information can be added, but nothing can be changed or deleted once it's in the ledger. When you make a transaction on a blockchain, it doesn't go straight to the recipient. Instead, it's grouped with other transactions, and they are all processed at once. This group is called a "block," and on the network a new block is added every 10 minutes.

Once a block is processed, it's added to the ledger in order, from the first block to the latest one. The most recent block connects to all the previous ones, forming a chain – hence the term "blockchain."

The contents of a block are pretty simple – an account number and associated data. For blockchain to be useful, that data needs to represent something in the real world, something tangible and valuable. So, blockchains are really just a digital records management system. But there are some important differences between regular databases (where most of the world's data is stored) and blockchains. Let's explore those differences first, and then we'll look at the benefits they bring.

Traditional Database vs. Blockchain Database:

In a regular database, like the one used by an online shopping platform to manage orders, there are different types of users. You might have customers who can only see and interact with their own order history, while employees can access and manage multiple orders. Then, there's usually a superuser with the ability to edit or manage every piece of data in the system.



In a regular database, you can add, delete, or edit data, which can lead to problems. For example, a hacker with superuser access could create fake records or change real ones. Or a software bug might cause unintended changes. This has happened to major companies across industries, including financial, healthcare, retail, and e-commerce, often taking months to correct.

In a blockchain database, data can only be added, not changed or deleted. **What are the advantages of blockchains over regular databases?** Here are a few:

- In a blockchain, only the owner can make transactions, so you have full control over your information. No one else can change it unless they get your credentials.
- In a regular database, other users have permission to your account, so if they don't like your transaction, they can stop it. For example, if you wanted to send money to someone flagged as high-risk, the database owner could block the transaction. With blockchain, the owner is the only one in control, so no one can stop the transaction. However, blockchain transactions are one-way, so if you send money to the wrong person, it can't be reversed – there's no third party to fix the mistake.

Crypto Mining and Cryptography:

Crypto mining and Cryptography work hand-in-hand, but they do different things. Cryptography is about securing transactions and making sure data is safe, private, and impossible to mess with. Crypto mining, on the other hand, is the process of solving tough cryptographic puzzles to verify transactions and add them to the blockchain. Miners do this work, and in return, they get rewarded with new Bitcoins. So, Cryptography keeps things secure, while mining helps keep everything running smoothly. Let's look closer at these two technologies.

As we mentioned in the "How Bitcoin Got Its Start" section, running a Bitcoin node is called Bitcoin Mining, and the people who operate these nodes are known as Miners. Each node in the Bitcoin network constantly shares information with all the others, and several times a day all the nodes come to an agreement on one approved version of the Bitcoin blockchain.

This ensures that the nodes on the network are always using the same version of the blockchain. This process is known as the Consensus Mechanism. Simply put, the Consensus Mechanism keeps the blockchain in sync across all the nodes. Let's get back to Bitcoin mining. When Bitcoin first started, Bitcoin mining could be done on a home computer, but those days are long behind us now.

Bitcoin miners face a complex puzzle that involves finding a specific Hash, a unique string of characters that serves as a digital fingerprint for a block of transactions. To solve the puzzle, miners repeatedly guess different values (called "nonces") and run them through a hashing algorithm. When they find a Nonce that produces the correct Hash, they get to add the new block to the blockchain and are paid for their efforts. This process requires significant computing power and plays a key role in securing the Bitcoin network. We'll go into more detail about how hashing works when we cover Cryptography.

To really understand how Bitcoin transactions and ownership transfers are secured, we need to dive into the technology that makes it all possible – Cryptography.

A Bitcoin transaction is similar to a deed of trust or a release of lien on a house, in that it represents a transfer of ownership. When you buy a house, the deed of trust shows your ownership, with a trustee holding it as collateral for the loan. A release of lien confirms that any prior claims, like a mortgage, have been removed. In the same way, a Bitcoin transaction doesn't involve physically transferring the Bitcoin, it's just an update on the blockchain ledger that shifts ownership from one person to another. The Bitcoin network acts like the legal system, verifying and recording the transfer, much like how your county clerk will record a deed of trust or release of lien on your property.

Cryptography is the science behind secure communication, ensuring that only the sender and the intended recipient can understand the contents of a message. One of the key techniques in cryptography is called hashing.

Hashing takes information and turns it into a unique, unreadable string of characters, which can't be interpreted by humans or used by any system other than the one it's meant for. This unreadable string is called a "hash." Here's an example of what hashes look like.

Input		Hash
Hi, my name is Johnny	→	dc37dc223e8b19a0e17770fe62db9a27d
The entire lyrics of Hotel California	→	f7b130bba79d26112173ca61105a3e5e

Unless you can decode a hash back into its original information, it's impossible to know what kind of information or how much data it represents. This makes hashing a secure way to send sensitive information, as it can't be easily compromised.

Like mentioned earlier, in Bitcoin mining, each new block is hashed, generating a unique number assigned to that block called a Nonce. To process transactions and add the block to the blockchain, Bitcoin miners compete to guess the correct Nonce using powerful computer systems running mining software. Once a miner guesses the correct Nonce, the block is added to the blockchain, and the miner is rewarded with Bitcoin. Then the process starts over.

Crypto Wallets:

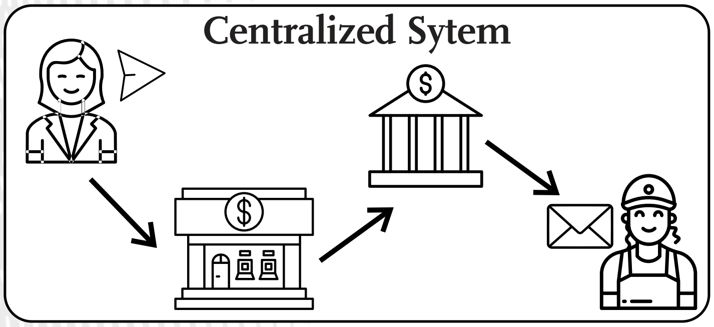
A Bitcoin or Crypto Wallet doesn't actually store your Bitcoins. Instead, your Bitcoin balance is just a number saved in a system. What your wallet actually contains are your private keys, which are needed to access and send your Bitcoin. When you send Bitcoin to someone, your wallet uses your private key to sign the transaction, letting the Bitcoin network know that you're the one making the transfer. So, if you lose access to your wallet – like forgetting your password – you haven't lost the Bitcoins themselves, just your ability to access them.

Many people have lost their Bitcoins because they've forgotten or misplaced their private keys. Without the private key, there's no way to access or recover the Bitcoins in that wallet. Since Bitcoin transactions are decentralized and not controlled by any bank or central authority, there's no way to reset or recover a lost private key.

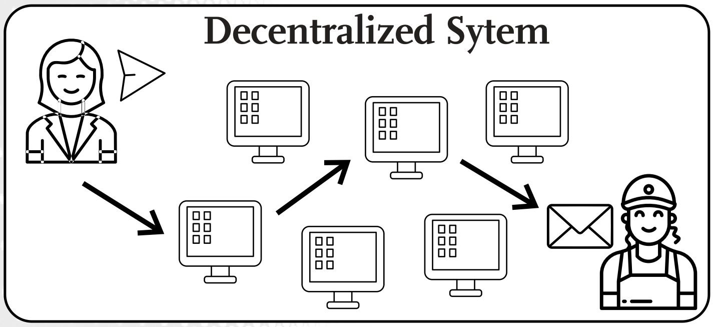
This lack of central authority is a key part of what makes Bitcoin unique, and it's directly tied to the concept of decentralization - our next topic. Let's take a closer look at what decentralization really means and how it plays a critical role in the Bitcoin network.

Decentralization:

We've come full circle to revisit decentralization, which we touched on at the beginning of this paper. Blockchain transactions happen directly between the sender and receiver, with no middleman involved, making them unstoppable. This is possible because blockchains are decentralized – a term that gets thrown around a lot, but not everyone fully understands. To get a better grasp of what that means, let's start by looking at a centralized system. For example, when you buy something through an online store, the payment request is sent to the company's payment processor, which then communicates with your bank or credit card provider to approve the transaction. Once everything checks out, the payment is processed, and the seller receives their funds. In a centralized system, the payment can be blocked at either bank because there's a central authority controlling everything.



In a decentralized system, things work a bit differently. There's no single processing authority between the sender and the receiver. Instead, there are multiple processing points, known as nodes. As the transfer happens, it moves between these different nodes, and each transaction uses different nodes.



One of the biggest perks of a decentralized system is that it removes the risk of a single point of failure. Each time a transfer happens, it goes through different nodes depending on which one is the most efficient at that moment.

Let's Summarize:

To put it simply, Bitcoin runs on a decentralized system powered by blockchain technology. This setup allows for secure and transparent transactions without needing a middleman. Users store their private keys in crypto wallets, giving them full control to send and receive Bitcoin directly. Behind the scenes, cryptography (especially hashing) keeps everything secure, while Bitcoin mining, done with powerful computers, validates transactions and adds new blocks to the blockchain. All these pieces work together to make Bitcoin and other cryptocurrencies stand out as a unique and resilient alternative to traditional financial systems.

Next Steps:

Follow along as we continue to explore the various aspects of cryptocurrency and what it means for investors, individuals, and the business world. For more information about us or to learn how Titan Consulting can equip your business to reach its full potential, visit our website at titanconsulting.net.