Introduction: Welcome to the first lesson of foundations of Blockchain. This course aims teach the areas of blockchain to everyone regardless of their background. There will be a variety of sources and videos all maintained in a central place as we recognize that people learn in different ways. In this lesson you will introduced briefly as to what blockchain is and why it is used.

Learning Outcomes:

* Get a basic understanding of the concept of blockchain
* To discover when it was originated.
* To understand why blockchain technology is used.

What?

To put it simply, a blockchain is a special type of database. A blockchain differs from traditional databases in the way that data is stored. As the name suggests, A blockchain collects information together in groups which can also be referred to as “blocks” and these blocks are linked to other stored blocks that help form a “chain” of data known as a “blockchain”.

The video below from simply explained provides a good overview of what blockchain technology is, be sure to watch it!

<https://www.youtube.com/watch?v=SSo_EIwHSd4&ab_channel=SimplyExplained>

When?

The origins of blockchain technology dates back to 1991 by two researchers named Stuart Haber and W.Scott Stornetta who shared a common goal of implementing a system where documents are timestamped and cannot be tampered with. However Blockchain technology didn’t gain its notoriety until the launch of Bitcoin in 2009, a digital currency that has amassed a market capitalization of over $1.06T at the time of writing. The introduction of bitcoin provided blockchain technology with its first real-world application.

Why use blockchain technology?

Blockchain technology possesses multiple features that justify why it should be adopted, for instance:

**Decentralization:** Blockchains are decentralized, which means that the blockchain is maintained and distributed amongst multiple nodes (computers) without the need of a central authority such as a bank. Therefore, an environment is created where no single person is exclusively in charge. By using blockchain, organizations can bring down the costs that are associated with using third party vendors.

**Immutability:**

The data that is stored on blockchains is immutable, meaning that once it gets recorded on the blockchain it cannot be changed or deleted. On a blockchain all of the data is timestamped, and date stamped so there is a permanent record. This enables consumers to utilize blockchain to track information over time, allowing for a secure and reliable audit of information. As opposed to using error-prone paper-file based systems or legacy computers which can be corrupted.

**Security:** Blockchain provides security through the previous two features mentioned. As the data is immutable and encrypted, blockchain mitigates the risks of fraud and unauthorized activity. Also, since blockchain is decentralized (spread across multiple computers) and not stored on one server, a single point of failure is removed. This in turn provides a greater resistance to malicious attacks from hackers.

Assignment

1. Read through the content provided by Euromoney regarding what a blockchain technology is
2. Watch this animated video from Simplilearn to reinforce what you have learned today.

Make up of Blockchain : How does it work?

What does a blockchain consists of?

A typical block contains the following properties:

1. Data
2. A hash
3. A hash of the previous block’s data.

These concepts are probably new to the most you but don’t worry they will be explained below:

Data : the type of data depends on what the blockchain is used for. In most cases the data corresponds to transactions, and a single block can contain hundreds of transactions. A simpl example of a transaction is Person A sending £500 to person B.

Hash: A hash is common concept used in cryptography. It is the value that is returned by a hash function. See here (https://en.wikipedia.org/wiki/Hash\_function) To put it simply, a hash is a unique combination of letters and numbers. It acts as a digital fingerprint for the data in a block, and is always unique for each block in the blockchain.

Hash of previous block: This property is what makes the blockchain. Each block contains a reference to the previous block’s hash thereby forming a “chain” of data. It is worth noting that by logic the first block will have no previous block so it will reference nothing. This is called the genesis block.

Hashes are important as they are one of the main reasons why blockchains are immutable. When a malicious attacker attempts to modify a transaction in a block this causes the hash of that block to change, which in turn causes the hash of the previous block to change, and so on until every block is invalid. This makes attempts of tampering evident to everyone involved in the network. Invalid blocks will never be validated unless the whole blockchain is re-written or participants of network are convinced that falsified data is true. Both instances have been impossible to achieve since blockchain technology was invented.

How does it work?

Now that we know what a blockchain consists of, lets discuss how it works. This process can be characterized in five steps:

1. **Transaction**: two parties agree to exchange a unit of value. This could be a digital currency or some other sort of asset. This in turn initiates the transaction
2. **Block**: The transaction is bundled together with other pending transactions to form a ‘block’. Then, the block is sent to all of the nodes (computers) participating in the blockchain network.
3. **Verification**: the participating nodes assess each transaction to determine whether they are valid based on agreed-upon rules. Upon a consensus being reached, the transactions are considered valid. Consensus algorithms are the mechanisms that help derive rules to determine the validity of a transaction, they will be discussed in a later lesson.
4. **The block is added to the existing blockchain**: After verification the block is added to the existing blockchain in an permanent way.
5. **Execution**: the unit of value moves from the account of the first party, to the account of the second party.

Consensus Protocols

This lesson will introduce you to what consensus protocols are, the role they play in blockchain technology, and the different types.

What are they?

A consensus protocol is simply a mechanism that allows all nodes in the blockchain network to reach a common agreement about the current state of the blockchain. They ensure that every new block that is added to the blockchain is a undisputed version of the truth agreed upon by all participants of the blockchain.

Why are they important?

As mentioned before, blockchains are decentralized in nature meaning that there is no central authority present to verify and validate transactions. Nonetheless, every transaction in the blockchain is secured, and verified. This is only made possible through the presence of consensus protocols. They supply blockchains with reliability and provide trust between unknown nodes in a decentralized environment.

How they work?

There are many implementations of consensus protocols across multiple different blockchains, therefore this section will supply you with the working examples of consensus algorithms and how they work.

Proof of Work: Proof of work is perhaps the most notable consensus algorithm as it is utilized by the bitcoin blockchain. The concept behind this protocol is to select a miner ( node) for the next block generation. Proof of work requires the participants of the network to devote a significant amount of computational power to solve a complex mathematical puzzle based on a leading number of zeros. On success, it results in a new block being added to the block chain and the winning miner is rewarded with bitcoin.

The video below provides a greater in-depth explanation of proof of work, so be sure to watch it!

**Proof of stake:**

Proof of stake was created as more sustainable, energy efficient alternative to proof of work. It relies on validators to secure the network. With proof of stake instead of the participants devoting computational power, they devote their tokens as collateral ( staking) with the hopes of being selected as a validator.

When a block of transactions is ready to be processed, the proof of stake protocol will randomly select a node to be a validator based on factors such as staking age ( the duration of time the participant has staked for) and the monetary value of the amount staked.

The chosen validator checks if the transactions in the block are accurate. If so they add the block to the blockchain and receive crypto rewards for their contribution. However, if a validator attempts to add a block with inaccurate information, they will lose some of the staked holdings as a punishment.

Proof of stake has gained a vast amount of popularity since the Ethereum blockchain switched from Proof of work, to proof of stake.

Types of Blockchain.

In blockchain technology, there are many different types of blockchains. These blockchains differ in aspects such as architecture and the way they are governed. This lesson will focus on two specific types of blockchains: Public and private, explaining what they are whilst highlighting the benefits and drawbacks of each approach.

Public blockchain (Permissionless):

A public blockchain network is permissionless in the sense that any one can join the network and have access to the ledger (record of transactions). It provides users from all around the world with the ability to interact with the blockchain and submit or read transactions to the network as long as they are connected. There are no restrictions when it comes to participation meaning that anyone can take part in the consensus process ( see previous lesson).

Public blockchains bring complete decentralization so there is no central authority responsible for maintaining the blockchain, maintenance is in the hands of the participants of the blockchain network.

Examples of public blockchains consists of Bitcoin, Ethereum and Litecoin

Private blockchains (permissioned):

Private blockchains, are permissioned blockchains meaning that users are not allowed to freely join the network and read or write to the ledger. These types of blockchains are controlled by a single organization meaning there is a central authority. These central authorities determine who can be a node and participate in the consensus process.

Private blockchains are only partially decentralized because public access to these blockchains are restricted. Examples of private blockchains consist of Ripple and Hyperledger.

Advantages and disadvantages of the different types of blockchain

Public Blockchain (Permissionless)

Benefits:

Maximum Security: public blockchains are designed to operate with maximum security. Often , shared networks are victims of online hacking attacks, which is why public blockchains work hard to maintain a high standard of security protocols. An example of this is bitcoin’s proof of work consensus algorithm. Proof of work is so secure that to this day the bitcoin network has never been hacked.

Anonymous nature: with public blockchains, the participants are not required to reveal their real name or identity to participate. Because of this, it is not possible to track down a user’s identity based on their activities on the network.

Transparency: all participants of a public blockchain can see each and every transaction at any moment of time because they each have a copy of the ledger. This eliminates the chances of any discrepancies and mitigates the risk of corruption within the network.

Drawbacks:

Speed: public blockchains like bitcoin are extremely slow, only managing to process seven transactions per second. If we compare this to Visa which can process 24,000 transactions per second, we can see the inefficiency. Public blockchains are slow because it takes time for the network to reach consensus ( ten minutes for proof of work). In this case, the security of public blockchains are traded off for speed.

Scalability: Due to the slow processing of transactions, public blockchains face concerns over scalability. As things are now, public blockchains are not able to compete with traditional systems. The slow transaction speed introduces a bottleneck into the network as it scales.

Anonymity: The anonymous nature of public blockchains are easily as much as a drawback than it is as a benefit. Due to participants having no fear of their identity being revealed, public blockchain can be used to harbor criminal activity.

Private Blockchain (Permissioned)

Benefits:

**Speed:** Opposite to public blockchains, a big advantage of private blockchain is speed. This is because private blockchains have far fewer participants as not everyone can join freely, meaning it takes less time for the network to reach a consensus. In comparison to public blockchains, private blockchains are more efficient in terms of the amount of transactions processed per second. Private blockchains can process thousands of transactions per second whilst public blockchains like bitcoin merely process seven transactions per second.

**Scalability**: Private blockchains also are much more scalable. This is because only a few nodes are authorized and responsible for managing data, therefore the network can process more transactions making it much more competitive with traditional systems. Due to private blockchains being centralized, the decision making is much faster, therefore the chances of a bottleneck being introduced into the network as it scales is significantly reduced.

Drawbacks

Security: As private blockchains contain fewer nodes that public blockchains, it is a lot easier for an untrustworthy individual to gain control of the network. Private blockchains are at a greater risk to hacking and data manipulation.

Centralization : Although centralization leads to faster decision making, it is also one of the biggest disadvantages for private blockchains. Blockchain was built to avoid centralization but private blockchains inherently become centralized as the single organization must build and maintain the private network.

Lack of Trust: The trustworthiness of private blockchains depends heavily on the credibility of legitimate nodes. As these nodes are responsible for verifying and validating transactions. In addition private blockchains are not transparent meaning that the validity of records also cannot be independently verified.

Conclusion – What is the better choice?

In terms of what type of blockchain is better, it is dependent on the purpose as both types each have their benefits and drawbacks. For instance Public blockchains are better suited for serving large communities due to the transparency which in turn fosters more trust. However it is held back by both speed and scalability.

Private blockchains may be better suited to the corporate world and financial institutions especially if they have an idea of what data will be stored on it. This way it is an advantage to know exactly who has access to what. However as a result trust and security is compromised.

The takeaway is that blockchain technology is consistently improving and bringing new innovations to the world. So much that there is an option to have a mixture of public and private blockchains where the participants of the network can benefit from the best of both worlds. (Hybrid Blockchain)

Cryptocurrencies:

Introduction: In this following lesson you will learn all about cryptocurrency.

What are cryptocurrencies?

Cryptocurrencies are cryptographically secured digital representations of value that can be transferred, stored, and traded electronically. In short, a cryptocurrency is a digital currency that can be traded and used to pay for things. Because cryptocurrencies are secured by various cryptographic techniques it makes them nearly impossible to counterfeit or double-spend.

How do they work?

The difference between cryptocurrencies and digital cash is that they are not controlled centrally, instead they operate on an open network. Transactions are conducted peer to peer without the need of a third party such as a bank. This is possible as they utilize blockchain technology, where a public record is kept of all transactions.

How many cryptocurrencies are there?

As of 2021, there are nearly over 6000 cryptocurrencies. A number likely to increase as new cryptocurrencies are introduced each and every day. The largest cryptocurrency to this date is Bitcoin which was first created in 200W9 by Satoshi Nakamoto. Bitcoin has amassed a market cap of $1.15T and is trading at a value of $60,000 per token at the time of writing.

Below you can find a range of cryptocurrencies, each ranked in order by their market cap.

Why use cryptocurrencies?

Cryptocurrencies benefit from most of the advantages that blockchain technology provides. In particular they allow for the transfer of funds directly between two parties without the need for a trusted third party such as a bank or credit card company. Instead, transfers are secured by the use of public and private keys (cryptography). This means that fund transfers are completed with minimal processing fees, allowing the users to avoid the steep fees charged by financial institutions. Transactions in crypto-currencies are also lighting fast regardless of the distance between the two participants; a user can be sending crypto to someone half way across the world and it will be completed it the same amount of time as if the recipient was in the same domestic country. Due to these properties cryptocurrencies become the optimal solution for transactions.

What are the risks of using cryptocurrencies?

As the privacy and security for cryptocurrencies transactions are high, its hard for the government to track down users. Bitcoin has been used as a vessel to perform illegal activities such as buying drugs or weapons off the black market, or to launder money.

Also, although cryptocurrencies are very secure, exchanges ( where cryptocurrencies are held to buy from the general public.) are not as secure. This makes them susceptible to malicious attacks from hackers that can steal cryptocurrencies from user accounts. For instance, Bitfinex was an exchange that was subject to a hack that resulted in thousands of bitcoin stolen, that resulted in damages of $760 million.

Applications of Blockchain Technology

Introduction: This will be the last lesson on the foundations of blockchain course. In this lesson we will go over the real world applications of blockchain technology to shed light on the endless capabilities that blockchain technology can achieve once utilized.

Blockchain in the Financial industry:

The financial services industry is riddled with costly problems consisting from human error and corruption. From research, it is stated that the asset management industry could save a whopping $2.7 billion yearly by utilizing blockchain technology.

The applications of blockchain in the financial industry include recordkeeping, data management, security, privacy, and transaction processing.

Blockchain in Healthcare:

Healthcare is an industry where data protection, privacy and storage play a vital role. Blockchain can add many benefits in healthcare. It can be used to solve all these issues, providing data security and records of data sharing. This way healthcare organizations will benefit from greater patient treatment and higher quality data.

An real world example of blockchain implementation in health care is the Estonian eHealth foundation who announced a partnership for using a blockchain system to ensure the security of millions of medical records.

Blockchain for identification:

More than 1.1 billion people worldwide have no way of confirming their identity. Blockchain technology has the potential to provide a standardized network of identification information that can be stored securely and validated in a record time.

Companies like Microsoft are working on ways to integrate blockchain applications in a authenticator app which will give users full control of their digital identities. This could enable people in poverty-stricken regions with access to the financial system, healthcare and various other areas of industry.

Conclusion:

Blockchain technology applications such as these are only the beginning. There is no way of grasping the capabilities that future blockchain applications will bring as the possibilities are infinite. For this reason, many people are optimistic about the positive changes that blockchain technology can bring to the world.