https://docs.google.com/document/d/1PGlbhx2yJF_fmaBOzR_PwfT4Z9zr__PIeV0iTZX8yi0/edit

Subject E. Blockchain and innovations. Cross-industry potential. Our decentralized future.

1. Blockchain and Latest Developments. - evolution of blockchain

Blockchain has now been around for just over a decade and is one of the most innovative and fastest growing industries. It is crucial to keep up with the latest developments as they provide meaningful solutions to problems that could not be dealt with in this way before.

Public, Private, and Hybrid Blockchains

Amongst the most recent iterations of the technology is something known as a hybrid blockchain. This is a blockchain combining elements from both public and private blockchains. So to understand it we need to know the difference and what each of these elements entails.

A public blockchain which is the most common topic of conversation in the industry is, as suggested, open to anyone. Everyone is equal and there are no restrictions on the participation of individuals. Anyone can read the blockchains, make transactions, mint transactions, verify the network, run a node, or anything else as long as the protocol is followed. The most known examples of public blockchain are Bitcoin and Ethereum.

Meanwhile, in a private blockchain parties have limited access. This is most commonly used within companies. For example, a company can choose to use a blockchain as a software solution for storing data immutably. Within the company, a manager would control permissions and give different employees. For example, they can give access to the managers to write data and only allow workers to read data. Furthermore, this data can either be shown or hidden from the public and customers.

A hybrid blockchain strives to take the best of both worlds and combine public and private features for the particular use case of the blockchain. Hybrid blockchain architecture is flexible and customizable just like any other blockchain. Ideally, the goal is for the blockchain to have both controlled access and freedom at the same time. To simplify, a hybrid blockchain has the features of a public blockchain while allowing access to trusted parties only. This means that whoever is in charge of the blockchain may grant access to individuals, but the system is anonymous, transparent, and secure after this gateway. An example of a hybrid blockchain worth looking into is DragonChain.

NFTs

With the recent hype you have likely heard about NFTs, so let's try to understand them. NFT stands for non-fungible token. Fungible since it is uncommon, means "replaceable by an identical item". As suggested by the name, this means that an NFT is unique, whereas other tokens are interchangeable. This gives NFTs many use cases. One of the most promising solutions that NFTs provide is digital ownership. Thanks to the security and immutability of blockchain technology, it is a much better way of organizing ownership of cars, houses, art, and anything else.

Hyperledger, Azure, R3, Amazon Managed Blockchain

As a fast-growing industry, it is important to lower the barrier for entry so that new people of all skill and creativity levels can be quickly brought up to speed. In association with this are organizations such as hyperledger that provide building blocks in the form of code solutions. They are an open-source project hosted by the Linux foundation. This is of course not the only organization that has seen this opportunity. Azure by Microsoft, Amazon-managed Blockchain, and R3 all provide software solutions and similar services. Hyperledger also provides educational materials in the blockchain industry.

Synthetix

Synthetix is a DeFi platform built on Ethereum that has made significant moves in incorporating the more complex areas of traditional finance into the blockchain world. To understand what it does, we need to understand what derivatives are and what they are useful for. Derivatives are defined as assets that derive their value based on the value of another asset. In traditional finance, these can be found as contracts, for example, options or futures contracts. The value of these contracts is calculated through a formula that uses the value of another asset such as shares in a company as a variable. Synthetic assets (or synths) are the blockchain equivalent of derivatives. They tokenize the relationship between the underlying asset and the derivative product. The Synthetix platform allows anyone to mint synthetic assets on the blockchain whereas in traditional finance this can only be done by licensed institutions. Of course, since this is all on the blockchain, the synths can be exchanged anonymously and without a middleman. There are of course other platforms that provide similar services to Synthetix such as UMA, Perpetual Protocol, and Mirror.

2. Blockchain and Web 3.0. IPFS.

You may have heard of the concept of web 3.0, but what does this refer to? Each version of the web is a disruption, starting back in the 1990s when the internet first came into existence and started becoming more publicly accessible. This was distinguished by the static websites that offered no interaction. Most websites were a file. While the transition between web 1.0 and web

2.0 cannot be pinpointed, one of the main features that define web 2.0 is the use of databases to host websites rather than using a file. This means that the websites can be updated in real-time. It also allows for users to post comments. This change progressed in the 2000s as more features and tech got developed, including server-side scripting, in-browser text editing, and more, which also provided the basis for forums and social media.

Blockchain is a distinctive change between web 2.0 and web 3.0. While web 3.0 is not widespread, it is being worked on actively. For both web 2.0 and 3.0, there are no exact definitions, but the core idea for web 3.0 is that the internet will be taken back by the people. It will become peer-to-peer rather than run on company servers. Data will not be stored on servers but on immutable, secure, decentralized blockchains. The internet will be permissionless as these blockchains will be public and companies will not have the power to restrict anyone's rights to read or write. Another key feature constituting a major part of web 3.0 is the integration of AI and IoT. This will be discussed in detail further into this course. Web 3.0 is the web of intelligence, where the interactions will not only be between people and software, but also between software and software.

The next major change between the current web and web 3.0 is the underlying file system. The manner in which files will be stored and accessed will be completely different since servers will not function as they do now. Currently, the web is based on DNS and the HTTP protocol. The way the web works now is that every device has an IP address. HTTP is a server-client protocol which means that your device asks a server for information via its IP and it sends that data to your IP. The change will be in the fact that there will no longer be designated servers. Instead, each device (including your own) will serve both as a client and a server which is the basis for peer-to-peer networks. The most likely protocol/ software solution that will replace HTTP is called IPFS. In place of providing content based on where it is located, IPFS uses content addressing to know what is in the content based on its address. The address is, therefore, representative of the content rather than its storage address.

There are many advantages that IPFS provides over HTTP. Firstly, IPFS is more secure. SSL is a protocol for establishing authenticated and encrypted connections between networked computers which is no longer necessary with IPFS. IPFS also keeps all versions of a file as well as the file. The data will be distributed in many places so it is less likely to get lost whereas a server that is not backed up can suffer physical damage and make the data irretrievable. The data can be moved without changing the address which will make it much easier to locate and keep track of. IPFS is also much faster than HTTP. It is transport-layer agnostic, which means it can work over any transport layer (from TCP to Bluetooth).

3. The challenge of interoperability.

Interoperability is one of the most prevailing challenges in the blockchain world. Taking into account all of the information, we can see how important it is. Currently, there are over 800 blockchains and they are all their own separate networks. It is incredibly difficult and inefficient to migrate data or value between chains. The safest way to do so as of right now is to use a centralized exchange and give them tokens on one network, sell them, buy other tokens, and then withdraw them on a different network. WBTC is even an exchange specifically designed to put BTC on ETH.

Of course, for people to have the decentralized freedom we want, all of these public blockchains need to be connected so everyone can take advantage of all of the services and solutions they provide. A very obvious example is wanting to migrate BTC onto ETH so that you can use your BTC to farm yield. This will not be a trustworthy process if a centralized exchange needs to be involved every time.

It makes sense to want interoperability due to the different strengths and weaknesses of different chains. For example, if you want full access to DeFi, you may want to keep assets on Ethereum, if you want cheap transactions, you may want to use another network, if you want fast execution you may want a different network, liquidity is also an important factor, the list goes on. So far it has also been one of the biggest challenges to tackle. The biggest hack in crypto is currently PolyNetwork, where $600 million were taken by a hacker. PolyNetwork is a cross-chain DEX. This means that trying to take on interoperability has been the most expensive and difficult thing to achieve in blockchain until now.

Solutions are being worked on with full force. Chainlink is developing CCIP (Cross-Chain Interoperability Protocol), Polkadot and Cosmos are also projects that are focused on interoperability, and there are bridges that attempt to connect chains such as Clover which is between Polkadot and Ethereum.

4. The challenge of scalability.

Another almost equally important challenge that has come to light with the most recent explosion in the popularity of crypto is scalability. The best example of this is Ethereum. To do the most basic transaction on Ethereum in 2020 it cost 0.50USD. In 2021, however, the cost of a transaction did not drop below 5.00USD for 7 months, reaching highs of 70USD and averaging 20USD for the span of Q1 and Q2. These transactions do not include smart contracts which are even more expensive and slow to run. The rise in cost is due to the number of transactions being processed and the architecture of how transactions are chosen to be minted in the blockchain. All of this means that when there are more people actively using the network, it becomes much more expensive to make transactions.

This is of course a massive problem if we want the entire world to participate. The market cap of the entire industry is only 1 trillion USD when compared to the 7.5 trillion USD that are the 5 biggest tech companies. Even with such a small user base it is already impractical for users so think about how bad it could get when we witness global adoption (the ultimate goal for the industry). To provide the best user experience and allow people to use the tech that is being provided, it is important to solve the problem of scalability.

There are already solutions being developed to combat this. There are 2 ways to implement scaling solutions, namely on-chain, and off-chain. On-chain means that the Ethereum layer 1 protocol will have to be altered for these solutions to come into play. The on-chain solution that is being looked at the most to lower transaction fees. The idea is to split the Ethereum database horizontally, creating new chains (or shards). This will lighten the load so that different validators can process different transactions rather than trying to squeeze all of the transactions into one place at the same time.

As for off-chain solutions, there are many creative ways to do this, some of which rely on layer 1 for security while others don't. One type of scaling solution is called a rollup. They are on layer 2 but sit parallel to the main Ethereum chain. What they do is "roll-up" transactions, in other words, thousands of transactions can be put into one rollup block. This is then sent to mainnet as CALLDATA, which is much cheaper than layer 1 storage and computation. This will result in a 100x improvement. There are different methods of doing this - namely, optimistic rollups and ZK-rollups. These rollups will also benefit if sharding is implemented.

The next off-chain scaling solution is called a state channel. Let's say you want to play a game against an opponent. You open a state channel. Every move either player makes is recorded off-chain as a transaction. This also allows for the chronology of the moves to be maintained. Once the game finishes, the channel closes and the "final state" is signed by both players. It is then sent as one transaction, hence reducing congestion on the network and the participants only need to pay 1 fee.

The next way to reduce traffic on mainnet is called a plasmachain. This is like a separate chain but it is anchored to mainnet. It is essentially a copy of mainnet. An example of this is Polygon (previously Matic). These are also sometimes referred to as child chains. There is no limit to how many can be created.

The final scaling solution is different in that it does not use Ethereum for immutability. This solution is called a sidechain. By creating a new chain, all of its characteristics can be altered for it to serve a specific purpose. This chain is a copy of Ethereum, even if block times and other parameters are different, which means it is fully EVM compatible. It is connected with a two-way bridge to mainnet. Since it is a copy of Ethereum, the benefit is you can deploy identical code.

5. Potential and limitations a decade from the beginning.

However exciting a technology it is, Blockchain is not a solution to every problem that presents itself. While there are new ideas in the industry every day, for now it still remains that blockchain has very specific use cases where it is of any benefit over traditional systems. Currently a lot of the benefits still owe it to the infrastructure and philosophy of the technology - being public, trustless, immutable. In the short time blockchain has existed, it has not yet been developed to the extent of previous technology and can therefore not match the performance. For this reason it is critical to understand when blockchain is a relevant solution and when it may be less effective.

The first factor to consider is who will be accessing the data. If only one entity will need to read the data, a spreadsheet is a much more simple solution which is more cost effective, easier to use, takes less time, energy, and storage. If the data is shared, however, it may be good to consider blockchain.

The same goes for writing data. If only one person needs to write data, even if more people need to read it, you do not need a blockchain, but can stick to solutions such as databases.

Of course, the data in a blockchain is immutable, so if you need to alter it at some point in the future, a blockchain is certainly not relevant.

Furthermore, storing sensitive information in a blockchain is a terrible idea. If you want a place to store passwords or client information, an encrypted database is a go-to.

Now that these basic things have been mentioned, it is also important to consider the context of the data. Blockchains are particularly useful when there is a conflict of interest. If there is no conflict, there is no need for a blockchain. This is when participants are fighting over who has control of the data. As we know, on a blockchain no one has control, which is why it is a good solution in this scenario.

Just like fighting over power in a conflict of interest, another issue that can be faced is a lack of trust. If you need to ensure trust in the data to someone who has any reason not to trust you, a blockchain is a relevant solution.

Blockchain is also only useful when it is important to make data tamperproof and immutable. Due to its limitations, it is not worth implementing unless it is necessary.

Another advantage blockchain has over any other technology is that it can be used to remove intermediaries.

Finally, blockchain is useful for proving authority or ownership or identity. By linking ownership to your private key through, for example an NFT, it is easy to show that you are indeed who you say you are.

So all of these factors are exclusive benefits to blockchain that other technologies cannot offer, but there are always reasons why it may not be the perfect solution in a given situation. If you need flexibility in your data or frequently update the manner in which it is stored (structure) or want to add fields, it will be much more difficult to do if using a blockchain.

Another issue is the size of data. If you want to store large files, blockchain is definitely not for you since the nodes in the network need to update and this can be incredibly slow when dealing with a lot of data.

Blockchain also has certain hardware requirements - you need multiple nodes for the system to be of any benefit, and it may take some computational power to run. Data is also redundent so if any node has a problem it will not affect the network, meaning that you need possibly double the storage of a regular database.

Finally, if your data requires updating or changing at all, blockchain is not for you. As explained, once a block with data is added to the chain, it cannot be changed at all at a later date.

6. Interaction with other innovative industries/technologies:

There are currently 3 main technological industries that are growing at an astonishing speed. These are Blockchain, Artificial Intelligence, and the Internet of Things. When these 3 technologies are combined, we will have so many possibilities. This is what the future will most likely look like.

Blockchain and the IoT

In the current state of the internet, there is a problem with identity fraud. An outside party provides your online identification. SSI (Self-sovereign identity) allows people to be in control of their own identity through blockchain. This is because instead of using an account belonging to a company to show credentials, your private key is all you will need, and no one has that except you! More interestingly, however, is that this may be more relevant to commercial uses such as identifying objects.

These objects are known as the Internet of Things. IoT is a network of internet-connected physical devices. While they can be almost anything, the main attributes of these devices is that they have sensors which can be used for collecting all kinds of data. Their sensors allow them to communicate with their environment while software provides the tools necessary for processing this information. Finally, all of the devices connect together allowing for a deeper understand of occurrences. This network already had more than 22 billion devices connected in 2018 and is continuing to grow rapidly with the recent change of energy source preference from gas to electricity.

Consumer applications of IoT include but are not limited to smart home automation; Devices such as lights, security systems, air conditioning, TVs, etc. Wearable electronics - which can collect and analyze information about your body and transmit it if needed. Remote health monitoring for those in need - emergency notifications and real-time health analytics.

Enterprise applications are the automation of: transportation, manufacturing of products, agriculture, energy grid, etc.

Essentially, IoT is the information layer.

Blockchain and AI

As a separate technology, we have AI. AI can be used to analyse, interpret, and find meaning in the mass of data collected by the device sensors. It will be able to identify patterns that no human or computer currently can. Artificial intelligence is about teaching computers how to perform tasks that would usually need human input as machines do not yet have the ability to consider the consequences of decisions. “AI is whatever hasn’t been done by computers yet” (Larry Tesler’s Theorem). Once AI finds a solution to a problem, it is no longer considered AI but instead becomes a part of everyday computing.

Once combined, AI will be able to make decisions upon which the devices in the IoT will act. Blockchain is the glue that allows for AI and IoT to work together, securely storing all of the transactions and settling payments. It also allows for smart contracts to exist which enable automatic execution and enforcement of contracts under given conditions. Digital ownership and custom financial instruments will also be relevant.

Taking all of this together, we have the IoT collecting massive quantities of data in a cost-effective way, AI analyzing this data to find meaningful patterns otherwise not identifiable by humans or computers, and finally blockchain immutably and securely recording all of the transactions and storing them with no single point of failure (centralized server or company record), allowing autonomous systems to interact with each other.

Blockchain in other industries

While blockchain can be combined with other technology to unlock endless possibilities, it will also disrupt other industries by itself. Blockchain technology is not limited to the public blockchain industry - it will change how many industries operate and provide opportunities that were previously not possible.

One of the good things about decentralization is that it motivates collaboration. Without a big company making decisions, people are pushed to be creative and find their own solutions. Since it is difficult to do anything meaningful alone, this naturally allows for small groups with aligned goals to form.

Through smart contracts anything is possible! Blockchain lowers the barrier to entry in many well-established industries by disrupting the infrastructure. Previously only lisences companies had the ability to offer leveraged assets. As discussed in the section about synthetic assets, blockchain changes this.

One of the industries blockchain will revolutionize is real estate - blockchain will do to real estate investing what the internet did to stock investing. Through tokenization, a property can be owned by multiple entities. As said previously, this lowers the barrier to entry. This would allow anyone to invest any amount (even really small quantities) into any available property and reap proportional rewards.

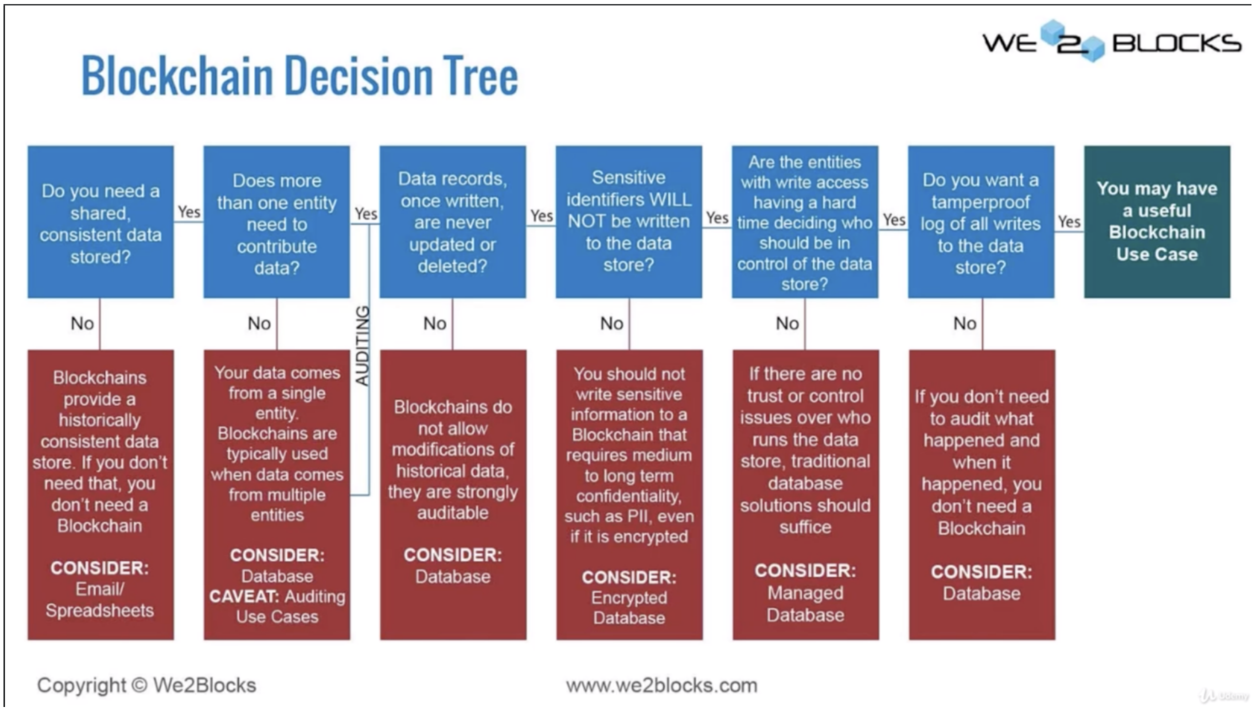
This is also good for sellers. A further benefit is that this makes markets much more liquid, allowing for faster and cheaper transactions that benefit both sides since there is no commission to be paid to an intermediary.

Tokenization is also good for capital raising. Not only in real estate, but in other industries too. If someone has a business idea and they need capital, tokens can be sold the same way shares work in a company, providing the investor with governing power as well as dividends.

7. Our decentralized future.

All of these technologies sound promising in delivering the next generation of the internet. The internet is upgrading from the internet of information to the internet of value. With it individuals will have equal opportunity to use services since their identity will not be a factor. Everyone will have more freedom as the technology will provide solutions to complex problems that were previously only accessible to lisenced or wealthy corporations. Crowd funding will be easier, the world will be peer to peer, hence more efficient without intermediaries. There will be no controlling authorities such as companies that have a monopoly on services and own your data. You will have control over your own online property and identity. Transactions will be transparent and anonymous. Content will be accessible through a more efficient system, and businesses will provide more value in the increasingly competitive markets rather than markup price because they can. Many industries will be revolutionized. Agricultural providers will receive what they deserve rather than accept the unfair prices. The origin of products and resources will be traceable resulting in improved ethics and trust. The infrastructure of the internet will be more convenient for the user as they will not rely on servers that powerful people running large companies can control. As technology continues to evolve there will be endless possibilities that can not be predicted. That is why it is important to try and understand how everything works and stay up to date with new ideas.

For part 5



Blockchain Decision Tree

WE2BLOCKS

Do you need a shared, consistent data stored?

Yes

No

Blockchains provide a historically consistent data store. If you don't need that, you don't need a Blockchain

CONSIDER: Email/ Spreadsheets

Does more than one entity need to contribute data?

Yes

No

Your data comes from a single entity. Blockchains are typically used when data comes from multiple entities

CONSIDER: Database
CAVEAT: Auditing Use Cases

AUDITING

Data records, once written, are never updated or deleted?

Yes

No

Blockchains do not allow modifications of historical data, they are strongly auditable

CONSIDER: Database

Sensitive identifiers WILL NOT be written to the data store?

Yes

No

You should not write sensitive information to a Blockchain that requires medium to long term confidentiality, such as PII, even if it is encrypted

CONSIDER: Encrypted Database

Are the entities with write access having a hard time deciding who should be in control of the data store?

Yes

No

If there are no trust or control issues over who runs the data store, traditional database solutions should suffice

CONSIDER: Managed Database

Do you want a tamperproof log of all writes to the data store?

Yes

No

If you don't need to audit what happened and when it happened, you don't need a Blockchain

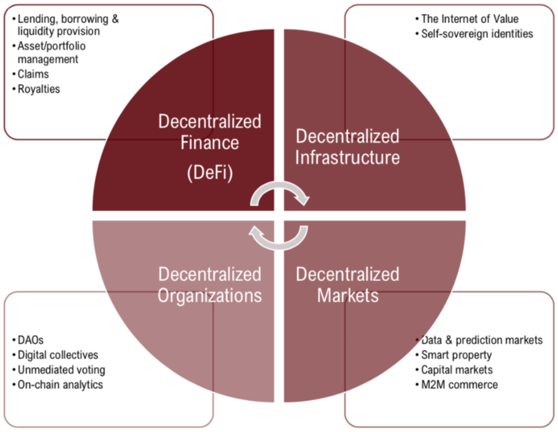
CONSIDER: Database

You may have a useful Blockchain Use Case

www.we2blocks.com

Some examples of the ‘exciting stuff’

Native blockchain applications



Decentralized Finance (DeFi)

- Lending, borrowing & liquidity provision
- Asset/portfolio management
- Claims
- Royalties

Decentralized Infrastructure

- The Internet of Value
- Self-sovereign identities

Decentralized Organizations

- DAOs
- Digital collectives
- Unmediated voting
- On-chain analytics

Decentralized Markets

- Data & prediction markets
- Smart property
- Capital markets
- M2M commerce