UNIVERSITY of NICOSIA

Session 6

Blockchain Types

DFIN 511: Introduction to Digital Currencies

Objectives

- Introduce the different types of blockchains.
- Take a closer look at Ethereum and smart contracts.
- Summarise various private, permissioned, consortium, and / or hybrid blockchain projects.

While this course mainly focuses on Bitcoin and popular cryptocurrencies, this week we will look at various blockchain projects being built for purposes other than permissionless, censorship resistant digital cash.

Next week, we will going into alternative uses of the currency and summarise some of the several hundreds of cryptocurrencies that have also emerged. We will cover the properties of altcoins, stablecoins and security tokens.

Disclaimer: As usual, the inclusion of any particular blockchain project or organisation is for educational purposes only. This should not be construed as an endorsement or investment advice.

Agenda

1. Properties of the Bitcoin Blockchain
2. Blockchain Types
3. Open, Public and Permissionless Blockchains
4. Ethereum Blockchain and Smart Contracts
5. Open, Public and Permissioned Blockchains (Ripple)
6. Enterprise, Hybrid, 'Blockchain Inspired' (Quorum, R3, Hyperledger, EEA)
7. How many Blockchains are there?
8. Conclusions
9. Further Reading

Session 6: Blockchain Types

1. Properties of the Bitcoin Blockchain

Properties of the Bitcoin Blockchain

The Bitcoin network is:

- **Public**: the code and all transactions recorded in the Bitcoin network are publicly verifiable and available to all the operators in the network.
- **Open**: anyone can join or leave the network, validate transactions and mine new coins.
- **Peer-to-peer**: transactions are sent from one party to another without the need for a centralised authority or intermediary to authorise them.
- **Distributed**: storage and validation of the blockchain is performed across a wide variety of independent network participants.
- **Secure**: as long as more than 50% of nodes are honest.
- **Reliable**: since there is no single trusted third party, network uptime is maintained 24/7, every day of the week, all year round.

Properties of the Bitcoin Blockchain

The Bitcoin network is:

- **Immutable**: erasing or rewriting blockchain history becomes more computationally infeasible as time passes, due to the energy intensive requirement of proof-of-work.
- **Permissionless**: no need for credentials, IDs or authorization to join the network.
- **Borderless**: the network operates across geograhical boundaries, accessible practically anywhere with an internet or satellite connection
- **Censorship resistant**: no one has the power to block the transfer of funds based on the type, origin, or destination of any transaction, as long as it is valid according to consensus rules.
- **Neutral**: the Bitcoin network is agnostic to accounts, people and reasons, for sending and receiving Bitcoins wherever, whenever and to whoever.

Session 6: Blockchain Types

2. Blockchain Types

Main types of Blockchain

Table 1. The main types of blockchain segmented by permission model

			READ	WRITE	COMMIT	EXAMPLE
Blockchain types	OPEN	Public permissionless	Open to anyone	Anyone	Anyone	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Supply Chain ledger for retail brand viewable by public
	CLOSED	Consortium	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
		Private permissioned ("enterprise")	Fully private or restricted to limited set of authorised nodes	Network operator only	Network operator only	External bank ledger shared between parent company and subsidiaries

Source: Hileman and Rauchs, 2017

https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-09-27-ccaf-globalbchain.pdf

Main types of Consensus Algorithms

Consensus algorithms may vary across a range of characteristics: **performance**, **transaction speed**, **scalability**, **settlement finality**, **governance**, **privacy/confidentiality**, **compliance**, and **safeguards*** against unexpected issues. Some characteristics will be more / less important (or even undesired) according to the needs and goals of developers and users. Prioritising certain characteristics over others may involve trade-offs or second layer solutions like the Lightning Network (see Week 5 material).

Ex. Satoshi set Bitcoin's average block time for 10 minutes, at the cost of transaction speed but to the advantage of less wasted work.

Consensus Algorithm	Participants must...	Decentralization
Proof-of-Work (PoW)	Invest in specialised hardware, energy resources (though neither are required for non-mining full nodes)	Most tested; full decentralization possible, depending on distribution / access to energy resources and hardware manufacturing capability
Proof-of-Stake (PoS)	Invest in and stake significant amounts of the native cryptocurrency	Full decentralization only possible with equal distribution of stake / wealth
Delegated Proof-of-Stake (DPoS)	Similar to PoS, but also has a voting mechanism for delegates who make consensus decisions	Less tested in practice, but arguably easier to decentralize than PoS

https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-09-27-ccaf-globalbchain.pdf https://101blockchains.com/consensus-algorithms-blockchain/

Session 6: Blockchain Types

3. Open, Public and Permissionless Blockchains

Open, Public and Permissionless Blockchains

Characteristics of open, public and permissionless blockchains (similar to what we have previously explained about the Bitcoin blockchain):

- Anyone can join or leave the network, validate transactions or mine new coins.
- Anyone can maintain a copy of the entire blockchain and operate as a full node.
- All recorded transactions are publicly verifiable and available to all the operators.
- There is no need for credentials, IDs, or authorization to join the network.
- The only requirement to join the network is to download the software.
- There is no need for network operators to know or trust each other personally.

Open, Public and Permissionless Blockchains

- In the last decade, the most well known examples of open, public, and permissionless blockchains include Bitcoin (2009), Litecoin (2011), Monero (2014), and Ethereum (2015). We will explore Ethereum more in the next section.
- These public and permissionless networks have their own native currency / asset: bitcoin for the Bitcoin blockchain, ether for the Ethereum blockchain, etc.
- Since these distributed network participants need to reach consensus to update the state of the chain, on-chain transactions can be slow.
- While most of these blockchains has used proof-of-work (see Week 3 material) or similar variants for their consensus process, other mechanisms such as proof-of-stake continue to be explored.

Source: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

Session 6: Blockchain Types

4. Ethereum Blockchain and Smart Contracts

Ethereum Blockchain

- **Ethereum** is an open, public and permissionless platform, like Bitcoin.
- Ethereum was proposed in late 2013 by Vitalik Buterin. After a pre-sale to fund development in 2014, the network went live on July 30, 2015.
- It was described as "a revolutionary new platform" for **decentralized applications**, supporting anything from voting, to financial exchanges, to smart property. Ethereum features:
  - A standardized foundation platform (i.e. the enhanced programming abstractions, protocol and network)
  - An object-oriented programming language called Solidity to facilitate the creation of distributed/decentralized applications and "smart contracts" by anyone. Besides validation and distributed storage enhanced by Bitcoin, Ethereum also enhances processing of data and logic.
  - Its own native currency / asset called ether, which can be tracked on the blockchain and is used more as a computational fuel than a scarce currency.

Source: https://etherscan.io/stat/supply

Ethereum Blockchain

- With Ethereum's genesis block in 2015, 72 million ether were generated. The supply surpassed 100 million units in June 2018, and is currently over 117 million. Unlike bitcoin, which has a capped total supply of 21 million, the ether supply remains uncapped.
- Ethereum's market capitalization exceeded $200 billion in February 2021, and is approaching $500 billion in October 2021.
- Ethereum block time is presently roughly 13 seconds but can vary.
- Ethereum nodes must validate and process more information rather than just payments. Until June 2020, Ethereum's block size averaged less than 30 kilobytes. It currently exceeds 70 kilobytes.

Source: https://etherscan.io/stat/supply https://etherscan.io/chart/blocktime https://etherscan.io/chart/blocksize https://thenextweb.com/hardfork/2018/06/11/ethereums-total-supply/

Ethereum Major Releases

- 30 July 2015: Frontier. The first series of releases, following the mining of Ethereum's genesis block, were accessible only via the command line.
- 15 Mar 2016: Homestead Introduced new codes in Solidity (the programming language), allowed users to build more on the platform and introduced MIST: a full node wallet used to hold and transact ETH, write and deploy smart contracts.
- 20 July 2016: An unplanned release following the DAO attack. The Decentralized Autonomous Organization (DAO) was a decentralized investment fund which was hacked and $50 million worth of ETH was stolen by an unknown hacker. Following a disagreement about whether to rollback the chain to return the stolen funds, a hard fork occurred, resulting in two networks: the original chain without the rollback, known as **Ethereum Classic (ETC)**, and the chain with the rollback, **Ethereum (ETH)**, which was supported by the majority of the community and core developers.

Source: https://consensys.net/blog/blockchain-explained/a-short-history-of-ethereum/

Ethereum Major Releases and Moving Forward

- 16 Oct 2017: "Metropolis" was the third release, divided into two steps: Byzantium and Constantinople, implemented on 28 Feb 2017. This stage aimed to reduce the complexity of the Ethereum Virtual Machine (EMV) and provide flexibility for smart contract developers; zk-SNARKs and ring signatures are added.
- 08 Dec 2019: 'Istanbul' upgraded Ethereum's data storage process, mining protocol, and code execution.

The last phase is Serenity or Ethereum 2.0. The upgrade is expected to see a number of drastic developments, such as transition from proof-of-work to a proof-of-stake consensus algorithm, realization of a new scalability paradigm called sharding, and the introduction of a more efficient Ethereum Virtual Machine capable of executing high-performance smart contracts. Researcher Danny Ryan has formulated five overarching design goals for Ethereum 2.0: decentralization, resilience, security, simplicity and longevity. (More about proof-of-stake and sharding in week 7).

Serenity will be introduced in 5 phases: a) Phase 0: Beacon Chain (officially released on Dec. 1st of 2020), b) Phase 1: Sharding, c) Phase 1.5: Merging Ethereum PoW Blockchain With New PoS Blockchain, d) Phase 2: Implementation of the new operating model, and e) Stage zero: the launch.

Source: https://consensys.net/blog/blockchain-explained/a-short-history-of-ethereum/ https://cointelegraph.com/news/istanbul-to-berlin-ethereum-milestones-on-the-road-to-serenity

Smart Contracts

- Ethereum is based on the concept of self-executing **smart contracts.**
- A **smart contract**, in the context of Ethereum, consists of "immutable computer programs that run deterministically... as part of the Ethereum network protocol, i.e., on the decentralized Ethereum world computer." (Mastering Ethereum)
- A smart contract is "an account containing code that executes whenever it receives a transaction from another account" and other specific conditions are met.

Smart Contracts: Advantages and Challenges

Smart contracts may provide several advantages, for instance:

- Automatically enforce power equality of all parties involved.
- Protect an individual's rights by enforcing reasonable expectations for the signee.
- Eliminate the possibility of any signatory defaulting on their obligations.

But challenges also exist:

- Legality and whether a smart contracts is admissible at Court is questionable.
- They are still difficult to understand by a non-programmer. (*Ricardian contracts, intended to be both human and machine-readable, were proposed by Ian Grigg in 1994.*)
- Deploying smart contracts remains challenging in cases where human judgment is required (i.e. interpret the conditions and circumstances of a car accident).
- Any bug in the code of smart contracts might be exploited and result in a loss of funds.

Learn More: See on our further reading list at the end of the presentation for more on smart contracts.

https://medium.com/lumiwallet/bitcoin-smart-contracts-b3ae6a4b3041 https://komodoplatform.com/limitations-of-smart-contract-platforms/

Smart Contracts and the 'Oracle Problem'

- In order for some smart contracts to execute, they must rely on data coming from external / off-chain sources. They are unable to retrieve such data on their own, therefore we need some kind of a 'gateway' between the real world and smart contracts.
- In mythology we had 'oracles' as 'gateways' between the real world and the Gods.
- In the world of smart contracts, 'oracle' refers to a small group of nodes with the power to input off-chain data such as temperatures, commodity prices, foreign exchange (FX) rates, flight or train delays.
- An example would be bonds or other financial instruments, which use smart contracts to automatically pay interim interest payments (i.e. quarterly or semi-annual) and principal upon maturity. Smart contracts can also determine the value of the interest payments by pulling in data regarding currency exchange rates.

Source: https://legal-tech-blog.de/the-problem-of-blockchain-oracles-interview-with-alexander-egberts https://create.smartcontract.com/#/contracts/3575b07de7a520c49605549e9bce20ec

Smart Contracts and the 'Oracle Problem'

- Reaching consensus regarding such data among all nodes is important, since they all must agree on the same information in order to create a new block, in a deterministic, tamper-proof and reliable manner.
- Relying on oracle service providers is still challenging and under development (risks involve preventing single point of failure, leaking sensitive information, using various oracles to compare and cross check the authenticity of the collected data and prevent malicious actors from feeding false data, in order to profit from an incorrect execution of the smart contract).
- Oraclize is a promising project trying to address these challenges. http://www.oraclize.it/

Session 6: Blockchain Types

5. Open, Public and Permissioned Blockchains

Open, Public and Permissioned Blockchains

Characteristics of Open, Public and Permissioned Blockchains:

- In a permissioned blockchain, **not anyone** can join the network.
- **Permission is provided** to certain identifiable participants to join the network.
- This requirement adds an **additional level of security** in the absence of robust consensus mechanisms based on a distributed network of honest nodes.
- Participants are known to each other and are trusted parties.

Source: https://www.investopedia.com/terms/p/permissioned-blockchains.asp

Permissioned Blockchains

- Permissioned blockchains **may also define the role** of each participant:
  - Who can operate a node.
  - Who can validate new transactions.
  - Which parts of the network and blockchain the participant can access / have influence over.
  - Who can introduce changes to the system.

Source: https://www.investopedia.com/terms/p/permissioned-blockchains.asp

Permissioned Blockchains

Ripple

- Ripple was released by Ripple Labs Inc in 2012, focusing on intra-bank applications. The native, centrally issued token XRP had a total market capitalization of $11.6 billion as of 11 Oct 2020.
- Ripple uses a HashTree instead of a blockchain, and consensus is determined by a selected number of participants known as the 'Unique Node List.' Only votes from these nodes are used to validate transactions.
- In December of 2020, the U.S. Securities and Exchange Commission (SEC) sued Ripple Labs, their CEO Brad Garlinghouse, and co-founder Chris Larsen for the sale of XRP as an unregistered security. It has since been delisted by several exchanges. The case is still ongoing.

https://www.sec.gov/news/press-release/2020-338

Source: https://coinmarketcap.com/currencies/xrp/ https://bitcoinmagazine.com/guides/what-ripple https://en.wikipedia.org/wiki/Ripple_(payment_protocol)

Session 6: Blockchain Types

6. Enterprise, Hybrid, 'Blockchain-Inspired'

Consortium (Private) Blockchains

- Consortium blockchains are used by organizations or businesses wishing to process private transactions within a permissioned group of known participants, between organizations and geographic locations.
- Examples include:
  - Hyperledger, an umbrella project of the Linux Foundation Blockchain Initiative.
  - Corda, a self-described "blockchain inspired" distributed ledger from R3.
  - Quorum, a permissioned copy of Ethereum by JPMorgan (acquired by ConsenSys).

- The Enterprise Ethereum Alliance (EEA) is a consortium which aims at creating a standard version of the Ethereum software for enterprise applications, such as tracking financial contracts. It includes over 450 enterprise business members such as Microsoft, JPMorgan Chase, Santander, Accenture, ING, Intel and Cisco. In Oct 2018, EEA and Hyperledger announced that they would be working together.

Source: https://www.investopedia.com/terms/p/permissioned-blockchains.asp

Hybrid Blockchains

- Hybrid blockchains combine elements from public and private blockchains.
- Examples include:
  - **Dragonchain**, focused on interoperability in a multi-chain network of blockchains. There are 359 million DRGN coins in circulation, out of a total supply of 434 million. As of 28 October 2021, the market capitalisation is $53.6 million.

Other

- IOTA Tangle is a Directed Acyclic Graph (DAG), a type of distributed ledger - not a blockchain.

Source: https://dragonchain.com/blog/differences-between-public-privat https://www.iota.org/

Session 6: Blockchain Types

7. How many Blockchains are there?

How many Blockchains are there?

- As of May 2019, it was estimated that there are over 800 blockchains, but the number is growing rapidly.
- Aside from those already mentioned, here are some other notable examples:
  - Liquid Network (federated sidechain)
  - Stellar
  - NEO
  - EOS
  - Dash
  - Tron
  - Polkadot

https://blog.bitdegree.org/did-you-know-there-are-861-blockchains-c60e1720fad5

Session 6: Blockchain Types

9. Conclusions

How many Blockchains are there?

- Blockchains may be used to support organizations in multiple ways, rather than just serve as a peer-to-peer payment mechanism.
- Blockchains have presently evolved from the ‘internet of money’ to the ‘internet of value’.
- Aside of Bitcoin and Ethereum which are Open, Public and Permissionless, other types of blockchains exist such as Permissioned, Private/Closed, Consortium, Enterprise and even Hybrid blockchains.
- Each blockchain can serve different purposes, obey different rules, and employ different protocols.
- Each blockchain has its advantages and disadvantages.

https://blog.bitdegree.org/did-you-know-there-are-861-blockchains-c60e1720fad5

Session 6: Blockchain Types

10. Further Reading

Further Reading

On public and private blockchains :

- https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
- https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

More on Ethereum and smart contract platforms:

- https://ieeexplore.ieee.org/document/8751309
- https://support.exodus.io/article/108-what-is-an-erc20-token
- https://blockgeeks.com/guides/ethereum-metropolis/
- https://blog.zeppelin.solutions/the-hitchhikers-guide-to-smart-contracts-in-ethereum-848f08001f05
- https://github.com/ethereum/wiki/wiki/Sharding-FAQs
- https://www.investopedia.com/terms/u/uncle-block-cryptocurrency.asp
- https://hackernoon.com/2019-blockchain-layer-2-solution-review-d00385147396

More on Ethereum 2.0:

- The Eth2 upgrades | ethereum.org
- Ethereum 2.0 is coming - Here's what you NEED to know (boxmining.com)

Tip: Clicking while pressing Ctrl key opens a new tab in Chrome browser on non-Apple devices

Further Reading

Run a Ripple Validator

https://developers.ripple.com/run-a-rippled-validator.html

EEA

- https://cointelegraph.com/news/enterprise-ethereum-alliance-and-hyperledger-enter-formal-association-agreement
- https://cointelegraph.com/news/enterprise-ethereum-alliance-publishes-on-blockchain-uses-in-telecoms
- https://cointelegraph.com/news/austrian-capital-vienna-develops-reward-token-for-citizens-in-partnership-with-university

Corda and the Distributed Ledger Technology

- https://tpbit.blogspot.gr/2017/01/corda-and-distributed-ledger-technology.html

Tip: Clicking while pressing Cltl key opens a new tab in Chrome browser on non-Apple devices

Further Reading

Hyperledger & Walmart Case Study

- https://www.hyperledger.org/resources/publications/walmart-case-study

Hyperledger Fabric Functionalities

- https://hyperledger-fabric.readthedocs.io/en/release-1.2/functionalities.html

Four International Banks Complete Commercial Paper Transaction on R3's Corda Platform

- https://cointelegraph.com/news/four-international-banks-complete-commercial-paper-transaction-on-r3s-corda-platform

SWIFT Integrates With R3'S Corda Settler In DLT Trial

- https://www.investinblockchain.com/swift-integrates-r3-corda-settler-dlt-trial/

Ripple

- https://cryptonews.com/news/this-is-why-ripple-removed-xrapid-xvia-and-xcurrent-from-the-4817.htm
- https://cointelegraph.com/news/ripple-ceo-our-transparency-has-opened-us-up-to-attack
- https://www.ripple.com/ripplenet

Tip: Clicking while pressing Ctrl key opens a new tab in Chrome browser on non-Apple devices

Further Reading

Ethereum-based decentralized applications

- https://www.stateofthedapps.com/

Smart Contracts Switch “I agree” to “I negotiate”, Andreas Vlachos

- https://www.linkedin.com/pulse/smart-contracts-switch-i-agree-negotiate-andreas-vlachos

Deloitte 2019 Global Blockchain Survey

- https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf

Tip: Clicking while pressing CItl key opens a new tab in Chrome browser on non-Apple devices

UNIVERSITY of NICOSIA

Questions?

Contact Us:

Twitter: **@mscdigital**
Course Support: **digitalcurrency@unic.ac.cy**
IT & Live Session Support: **dl.it@unic.ac.cy**